Délibération SAN-2022-022 du 30 novembre 2022

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Etat juridique : En vigueur

Date de publication sur Légifrance : Jeudi 08 décembre 2022

Délibération de la formation restreinte n°SAN-2022-022 du 30 novembre 2022 concernant la société X

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Monsieur Alexandre LINDEN, président, Madame Christine MAUGÜÉ, Monsieur Alain DRU et Monsieur Bertrand du MARAIS, membres ;

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

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 le code des postes et 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 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° 2019-188C du 26 septembre 2019 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 les sociétés […] et […] ou pour leur 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 17 décembre 2020 ;

Vu le rapport de Monsieur François PELLEGRINI, commissaire rapporteur, notifié à la société […] le 21 avril 2022 ;

Vu les observations écrites versées par la société […] le 2 juin 2022 ;

Vu la réponse du rapporteur à ces observations notifiée à la société […] le 13 juillet 2022 ;

Vu les nouvelles observations écrites versées par la société […] le 26 août 2022, ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 29 septembre 2022 :

- Monsieur François PELLEGRINI, commissaire, entendu en son rapport ;

En qualité de représentants de la société […] :

- […] ;

- […] ;

- […] ;

- […] ;

- […] ;

- […] ;

- […] ;

- […].

En qualité de représentants de la société […], joints par visioconférence :

- […] ;

- […].

La société […] ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La société […] (ci-après la société), dont le siège social est situé […], est une filiale du groupe […] qui est un opérateur de télécommunication fixe. Créée en 1999, la société compte environ 179 salariés.

2. Pour l'année 2020, la société a réalisé un chiffre d'affaires d'environ […] euros, pour un résultat net d'environ […] euros. En 2021, la société dénombrait environ […] d'abonnés, […].

3. Entre le mois d'octobre 2018 et le mois de novembre 2019, la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission) a été saisie de 41 plaintes à l'encontre de la société. Parmi ces plaintes, 10 ont été examinées dans le cadre de la présente procédure de sanction. Les plaignants faisaient notamment état de difficultés rencontrées dans l'exercice de leurs droits d'accès ou d'effacement. Certaines de ces saisines étaient également relatives à la sécurité des données à caractère personnel des clients de la société.

4. Le 8 février 2019, la société a procédé auprès de la CNIL à une notification de violation de données à caractère personnel puis, le 22 février 2019 à une notification complémentaire. Elles indiquaient qu'environ 4 100 […] avaient été remises en circulation sans que leur reconditionnement ne soit effectif, c'est-à-dire sans que les données du précédent abonné ne soient effacées du disque dur de la […].

5. Deux missions de contrôle sur place, dans les locaux de la société […] puis de la société […], ont été effectués les 21 et 22 janvier 2020.

6. Les procès-verbaux n° 2019-188/1 et n° 2019-188/2, dressés par la délégation le jour des contrôles, ont été notifiés à la société le 23 janvier 2020. À cette occasion, des demandes de complément d'information et de documents supplémentaires ont été adressées à la société. La direction juridique du groupe […] y a répondu par courriels des 3 et 10 février 2020.

7. Un contrôle sur pièces a également été effectué auprès des sociétés […] et […] le 3 juin 2020. La direction juridique du groupe […] y a répondu par courriel du 29 juin 2020.

8. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 17 décembre 2020, désigné Monsieur François PELLEGRINI en qualité de rapporteur sur le fondement de l'article 22 de la loi du 6 janvier 1978 modifiée.

9. Une demande de complément d'information a enfin été adressée à la société par courrier du 16 mars 2022. La direction juridique du groupe […] y a répondu par courrier du 31 mars 2022.

10. Le rapporteur a, le 21 avril 2022, fait notifier à la société un rapport détaillant les manquements au RGPD qu'il estimait constitués en l'espèce.

11. Ce rapport proposait à la formation restreinte de prononcer une amende administrative et une injonction de mettre en conformité le traitement avec les dispositions de l'article L.34-5 du code des postes et des télécommunications électroniques (CPCE) et des articles 7-1, 15, 17, 32 et 33 du RGPD, assortie d'une astreinte par jour de retard à l'issue d'un délai de trois mois suivant la notification de la délibération de la formation restreinte. Il proposait également que cette décision soit rendue publique, mais qu'il ne soit plus possible d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

12. Le 2 juin 2022, la société a produit ses observations en réponse au rapport de sanction.

13. Le 13 juillet 2022, le rapporteur a adressé sa réponse aux observations de la société.

14. Le 26 août 2022, la société a produit de nouvelles observations en réponse à celles du rapporteur.

15. Le 5 septembre 2022, le rapporteur a informé la société et le président de la formation restreinte de la clôture de l'instruction. Le même jour, le président de la formation restreinte a adressé une convocation à la séance de la formation restreinte du 29 septembre 2022.

16. Le 14 septembre 2022, la société a produit une attestation de son prestataire, la société […], relative à la fourniture de numéros de téléphone et d'adresse électroniques destinés à une campagne de prospection commerciale sur la période du 2 au 6 décembre 2019.

17. Le 21 septembre 2022, le président de la formation restreinte a avisé la société du report de la clôture de l'instruction au lundi 26 septembre 2022 et lui a demandé d'avertir la société […] afin qu'un de ses représentants puisse assister à la séance de la formation restreinte.

18. La société […] et le rapporteur ont présenté des observations orales lors de la séance de la formation restreinte.

19. Monsieur […] et Monsieur […], dont l'audition a été estimée utile, ont été entendus en application de l'article 42 du décret n° 2019-536 du 29 mai 2019.

II. Motifs de la décision

A. Sur le manquement à l'obligation de recueillir le consentement de la personne concernée par une opération de prospection directe au moyen de courrier électronique et de SMS

20. Aux termes de l'article L.34-5 du CPCE :

Est interdite la prospection directe au moyen de système automatisé de communications électroniques […], d'un télécopieur ou de courriers électroniques utilisant les coordonnées d'une personne physique […] qui n'a pas exprimé préalablement son consentement à recevoir des prospections directes par ce moyen. Pour l'application du présent article, on entend par consentement toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe. […] .

21. Aux termes de l'article 4, paragraphe 11, du RGPD :

Aux fins du présent règlement, on entend par […] consentement de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement .

22. Aux termes de l'article 7, paragraphe 1, du RGPD :

Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant .

23. Le rapporteur pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant des articles L. 34-5 du CPCE et 7, paragraphe 1, du RGPD, tel qu'éclairé par les dispositions de l'article 4, paragraphe 11, du RGPD, se fonde sur le fait que la société […], qui réalise des opérations de prospection commerciale par voie électronique via une base de données à caractère personnel collectées par son prestataire, la société […], n'est pas en mesure d'apporter la preuve d'un consentement univoque, spécifique, libre et informé des prospects avant que ceux-ci aient été démarchés lors d'une campagne de prospection commerciale par voie électronique (courriel et SMS) en décembre 2019. Pour considérer le manquement comme étant constitué, le rapporteur s'est appuyé sur les éléments recueillis à l'occasion des opérations de contrôle sur place (procès-verbaux n° 2019-188/1 et n° 2019-188/2) ainsi que sur des pièces complémentaires transmises à l'issue de ces vérifications, notamment un document indiquant que la société a obtenu en décembre 2019 auprès de ce partenaire des fichiers de prospects pour effectuer une compagne de prospection

commerciale par SMS et par email et que cette unique campagne […] n'a été faite qu'en décembre 2019 et n'a pas été poursuivie en 2020 .

24. En défense, la société soutient qu'elle a effectivement envisagé de réaliser une campagne de prospection par SMS et courrier électronique auprès de personnes non abonnées et a signé un devis avec son partenaire […] [la société […]] à cet effet . Elle indique cependant qu'elle s'est mal exprimée dans le document produit en pièce et qu'aucun manquement ne peut lui être reproché car cette campagne a été annulée avant même d'être lancée . Elle ajoute que l'une des raisons pour lesquelles cette campagne n'a pas été réalisée est que celle-ci devait permettre originellement de promouvoir les services de […] liés à la fibre optique. Du fait d'une pénurie, entre octobre 2019 et janvier 2020, des équipements utilisateurs nécessaires à l'installation de la fibre optique […], […] n'a finalement pas souhaité promouvoir des services dont elle n'aurait pu assurer la livraison . Lors de la séance de la formation restreinte, la société a réitéré ces éléments.

25. La formation restreinte relève que le document sur lequel se fonde le rapporteur comporte des éléments erronés et que la société a apporté des explications convaincantes sur les circonstances dans lesquelles l'erreur s'est produite.

26. Dans ces conditions, la formation restreinte considère qu'il n'est pas établi que la campagne de prospection commerciale électronique dont il est fait état ait été réalisée et que les éléments du débat ne permettent pas de conclure à l'existence d'un manquement aux obligations résultant de l'article L. 34-5 du CPCE et de l'article 7-1 du RGPD.

B. Sur les manquements en lien avec l'exercice des droits

27. Aux termes de l'article 12 du RGPD :

1. Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. […].

2. […].

3. Le responsable du traitement fournit à la personne concernée des informations sur les mesures prises à la suite d'une demande formulée en application des articles 15 à 22, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes. Le responsable du traitement informe la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande. Lorsque la personne concernée présente sa demande sous une forme électronique, les informations sont fournies par voie électronique lorsque cela est possible, à moins que la personne concernée ne demande qu'il en soit autrement.

4. Si le responsable du traitement ne donne pas suite à la demande formulée par la personne concernée, il informe celle-ci sans tarder et au plus tard dans un délai d'un mois à compter de la réception de la demande des motifs de son inaction et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel. […]
.

28. Aux termes de l'article 15 du RGPD :

1. La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi que les informations suivantes :

[…]

g) lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source.

[…]

3. Le responsable du traitement fournit une copie des données à caractère personnel faisant l'objet d'un traitement. […].

4. Le droit d'obtenir une copie visé au paragraphe 3 ne porte pas atteinte aux droits et libertés d'autrui.

29. Aux termes de l'article 17 du RGPD :

1. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :

a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ; […].

1. Sur le manquement à l'obligation de respecter le droit d'accès

30. Le rapporteur, pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant de l'article 15 du RGPD en matière de droit d'accès, se fonde sur cinq saisines de la CNIL, émanant de Messieurs […] (plainte n° 19009149), […] (plainte n° 19005208), […] (plainte n° 19014037), […] (plainte n° 19015831) et […] (plainte n° 19016618). Dans le cadre de ces plaintes, les personnes faisaient état de difficultés rencontrées dans l'exercice de ce droit, alors même que leurs demandes avaient bien été réceptionnées.

31. Le rapporteur indique que ces cinq saisines concernent notamment l'accès aux données à caractère personnel et, sur ces cinq saisines, quatre concernent plus particulièrement l'obtention d'une information sur la source d'où proviennent leurs données.

32. Le rapporteur observe qu'il ressort des constats effectués lors de la procédure de contrôle ou des éléments communiqués ultérieurement que la société n'a pas donné suite dans les délais prescrits aux demandes précitées d'exercice des droits d'accès des plaignants ou qu'elle leur a apporté une réponse incomplète s'agissant de la source de leurs données.

33. En défense, la société fait valoir, s'agissant de l'absence de réponse apportée dans les délais, que les procédures mises en œuvre n'ont pas été respectées en raison d'erreurs humaines isolées. Elle fait également valoir que le nombre réduit de plaintes relevés dans le rapport (2) doit être comparé aux nombres de demandes qu'elle traite par an (environ 600). Enfin, la société indique que ces saisines sont antérieures à la mise en place d'un nouvel outil de ticketing qu'elle utilise depuis juin 2019, qui a permis d'apporter des améliorations à la procédure de traitement des demandes d'exercice de droit. Dès lors, elle considère que ces dysfonctionnements ponctuels sont à présent résolus.

34. S'agissant des demandes d'informations sur la source des données, la société considère que, conformément aux dispositions du considérant 63 du RGPD et de l'article 15-4 du RGPD, elle n'est pas tenue d'y répondre dès lors qu'elle serait conduite à révéler une information relevant du secret des affaires (l'identité du courtier en données lui ayant fourni les données). Elle soutient qu'en réalité, l'information qui est recherchée par les requérants est l'identité de la source primaire qui est à l'origine de la collecte des données du demandeur. Elle indique avoir fait évoluer ses procédures au cours de la procédure de sanction puisqu'elle sollicite désormais ses courtiers en données afin qu'ils lui transmettent l'identité de la source primaire à l'origine de cette collecte, information que la société transmet à son tour aux demandeurs.

35. La formation restreinte relève, s'agissant de l'absence de réponse apportée dans les délais, qu'il résulte de l'article 12 du RGPD que lorsqu'une demande d'exercice de droit lui est adressée, le responsable de traitement doit fournir à la personne concernée des informations sur les mesures prises pour répondre à sa demande dans les meilleurs délais et en tout état de cause dans un délai d'un mois. La formation restreinte rappelle également que lorsque le responsable de traitement ne détient plus tout ou partie des données sur la personne qui exerce son droit d'accès (par exemple, les données ont été supprimées ou l'organisme ne dispose d'aucune donnée sur la personne), il doit néanmoins répondre au demandeur dans un délai maximal d'un mois.

36. S'agissant des informations à fournir sur la source des données au titre de l'article 15 du RGPD, la formation restreinte relève d'abord qu'il ressort des articles précités que la limitation du droit d'accès par les droits et libertés d'autrui qui incluent le secret des affaires, s'applique uniquement à l'article 15-4 du RGPD, relatif aux personnes demandant une copie de leurs données, et non à l'article 15-1 du RGPD, relatif aux personnes demandant des informations à un responsable de traitement qui procède au traitement de leurs données. En l'espèce, la formation restreinte note que les plaignants ne sollicitent pas de la société l'obtention d'une copie de leurs données ou l'accès à ces données, mais seulement une information quant à la source d'où proviennent leurs données. La formation restreinte estime dès lors que l'article 15-4 du RGPD est inapplicable. Elle considère en tout état de cause que l'article 15-1 du RGPD ne pourrait être limité que dans les conditions prévues par l'article 23 du RGPD, ce qui n'est pas le cas en l'espèce.

37. Ensuite, la formation restreinte relève que tout traitement de données à caractère personnel doit être conforme aux principes énoncés à l'article 5, paragraphe 1, a), du RGPD qui prévoit que les données à caractère personnel doivent être traitées de manière transparente au regard de la personne concernée. Elle souligne qu'il ressort des lignes directrices sur la transparence du groupe de travail de l'Article 29 devenu Comité européen de protection des données, que la source d'où proviennent les données à caractère personnel s'entend comme la source spécifique aux données ou, à défaut, la nature des sources (c'est-à-dire les sources publiques et privées) et les types d'organismes, d'entreprises et de secteurs . La formation restreinte considère que le droit d'accès de la personne concernée constitue une garantie fondamentale de la transparence des modalités de traitement des données. Elle en déduit que le responsable de traitement doit par principe communiquer la source spécifique relative aux données et que la limitation du droit d'accès aux indications de la nature des sources, des types d'organismes, d'entreprises et de secteurs ne peut intervenir que lorsqu'il ne détient pas cette

information, l'identification de la source spécifique des données à caractère personnel de la personne concernée étant impossible.

38. La formation restreinte relève également que le droit d'accès – l'article 15 du RGPD étant éclairé par le considérant 63 - a pour objectif de permettre à la personne concernée de prendre connaissance du traitement de ses données et d'en vérifier la licéité. L'exercice de ce droit suppose donc que les informations fournies soient les plus précises possibles.

39. La formation restreinte estime que le refus de communiquer l'identité du courtier en données à partir duquel les données de la personne concernée ont été obtenues, alors que la société dispose de cette information, et de limiter le droit d'accès à la source primaire de la collecte (c'est-à-dire le premier acteur de la chaîne à avoir collecté les données à caractère personnel de la personne concernée), qui n'était d'ailleurs pas fournie en l'espèce au moment du contrôle, revient à empêcher la personne concernée de pouvoir vérifier la licéité du traitement effectué par le responsable de traitement et, en particulier, la licéité des transmissions de données déjà effectuées. La formation restreinte considère, dès lors, que le droit de disposer de l'identité de la source des données est nécessaire pour permettre à la personne concernée de donner son consentement et d'exercer les droits qui lui sont conférés par le RGPD, en particulier le droit d'opposition, selon le type de prospection commerciale mise en œuvre par le responsable de traitement ayant obtenu les données auprès de courtiers.

40. La formation restreinte considère qu'un manquement aux obligations des articles 12 et 15 du RGPD est constitué pour l'ensemble des plaintes précitées dès lors que la société n'a pas traité les demandes d'accès qui lui ont été adressées dans le délai qui lui était imparti, laissant ainsi les personnes dans l'ignorance des données traitées par la société les concernant ou qu'elle leur a apporté une réponse incomplète s'agissant de la source de leurs données. En outre, la formation restreinte considère que la société n'a pas fourni, à la date de la clôture de l'instruction, d'éléments permettant d'attester d'une mise en conformité s'agissant spécifiquement du point relatif à la source des données.

2. Sur le manquement à l'obligation de respecter le droit d'effacement

41. Le rapporteur, pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant de l'article 17 du RGPD, se fonde sur deux saisines de la CNIL, émanant de Messieurs […] (plainte n° 19009870) et […] (plainte n° 19012463), dans le cadre desquelles les plaignants faisaient état de leurs difficultés dans l'exercice de leur droit d'effacement.

42. Le rapporteur indique que les intéressés ont demandé la suppression de leur compte de messagerie […].fr , via l'envoi, respectivement les 10 et 3 février 2019, d'un formulaire dédié à la suppression d'un compte principal […] accès gratuit sur lequel il est précisé que la suppression effective des comptes nécessite un délai de 48 heures après réception du courrier .

43. Le rapporteur observe qu'il ressort des constats effectués lors de la procédure de contrôle et des éléments communiqués ultérieurement que les plaignants n'ont pas obtenu de réponse à leurs demandes d'effacement formulées par lettre recommandée et que les mesures permettant de satisfaire leurs demandes d'effacement n'ont pas été mises en œuvre, dès lors que la base client SIEBEL contenait diverses données à caractère personnel propres aux plaignants, telles que leur identifiant de connexion, leur nom, prénom et adresse postale. En outre, le statut du compte de messagerie électronique […].fr de ces derniers était renseigné comme étant actif .

44. En défense, la société fait valoir que les demandes de suppression d'un compte […] accès gratuit ne sont pas des demandes d'effacement au sens du RGPD et ne sont encadrées par aucun délai légal […] mais s'assimilent à une demande de résiliation de contrat . La société en conclut qu'il serait totalement disproportionné de considérer que [ces demandes relèvent] de l'article 17 du RGPD et des délais posés par l'article 12.3 du RGPD . La société précise qu'elle est seulement tenue de respecter le principe de limitation de la conservation des données concernées, sans que cela impose la suppression immédiate de toutes les données concernées . Elle indique en ce sens avoir une obligation légale de conserver les données associées aux comptes de messagerie électronique pendant une durée de 1 an , conformément à l'article L. 34-1 du CPCE.

45. Sur ce point, la formation restreinte considère d'abord que les demandes des plaignants sont claires, en ce qu'il s'agissait pour chacun d'une demande de suppression générale d'un compte de messagerie électronique, adressée à la société par le formulaire dédié mis en œuvre par elle. Cette demande impliquait nécessairement la demande de l'effacement des données personnelles liées à l'utilisation du compte. La société ne peut donc se prévaloir du fait que cette demande de suppression n'aurait pas été claire et traitée en tant que demande d'effacement au sens du RGPD.

46. Ensuite, la formation restreinte considère qu'il ressort de l'article 12.3 du RGPD que le responsable de traitement doit fournir aux demandeurs des informations sur les mesures prises à la suite d'une demande formulée en application de l'article 17 du RGPD dans un délai maximal d'un mois, qui peut être prolongé d'une durée raisonnable dans certains cas. Or, elle relève que ce n'est que le 23 mai 2022 que la société a apporté une réponse aux plaignants, soit environ trois ans après que Messieurs […] et […]ont exercé leurs droits. Ce délai de réponse méconnaît l'article 12.3 du RGPD.

47. Enfin, la formation restreinte considère que si la demande d'effacement d'un compte de messagerie électronique n'implique pas nécessairement la suppression de l'ensemble des données relatives à ce compte (certaines données pouvant être conservées avec un statut d'archive intermédiaire), un manquement à l'article 17, paragraphe 1, a), du RGPD est en tout état de cause caractérisé en l'espèce dès lors que le statut du compte était actif et que la messagerie électronique était encore accessible aux personnes concernées plusieurs années après avoir effectué leurs demandes.

48. La formation restreinte considère qu'un manquement aux obligations qui découlent des articles 12 et 17 du RGPD est constitué dès lors qu'il incombait à la société de traiter la demande d'effacement des données à caractère personnel des plaignants dans les délais impartis.

49. Elle relève que, dans le cadre de la présente procédure, la société a justifié avoir pris des mesures pour se mettre en conformité avec les obligations découlant de l'article 17 du RGPD.

C. Sur le manquement à l'obligation d'assurer la sécurité des données à caractère personnel

50. Aux termes de l'article 32, paragraphe 1, du RGPD :

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) […] ;

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

c) […] ;

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 d'accès aux comptes clients

51. Le rapporteur, pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant de l'article 32 du RGPD, se fonde d'abord sur le fait que le mot de passe généré aléatoirement par la société lors de la création d'un compte utilisateur sur le site web de la société, lors d'une procédure de récupération ou lors d'un renouvellement du mot de passe, est d'une longueur de huit caractères et peut comporter uniquement un même type de caractères. Ensuite, le rapporteur relève que l'ensemble des mots de passe générés lors de la création d'un compte utilisateur sur le site web de la société était stocké en clair dans la base de données des abonnés de la société jusqu'au 23 janvier 2020. Enfin, le rapporteur relève que la délégation a été informée que le mot de passe qui est généré lors de la création d'un compte utilisateur sur le site web de la société est transmis par courrier électronique ou postal à l'utilisateur et indiqué en clair dans le corps du message. De même, le rapporteur relève qu'il ressort de trois saisines émanant de Messieurs […] (plainte n° 19018181), […] (plainte n° 18023964) et […] (plainte n° 19013170) que le mot de passe qui est associé au compte de messagerie électronique […].fr est transmis par courrier électronique ou postal à l'utilisateur et indiqué en clair dans le corps du message.

52. En défense, la société fait valoir qu'en tant que responsable de traitement, elle est libre de choisir les mesures de sécurité à mettre en place. Elle soutient en ce sens que les recommandations de la CNIL ou de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) citées dans le rapport n'ont aucun caractère impératif. Dès lors, la société considère qu'aucun manquement ne peut être retenu en l'absence d'une violation de données ayant affecté l'accès à l'espace abonné .

53. La société fait ensuite notamment valoir qu'à l'époque des opérations de contrôle, les abonnés étaient incités à modifier leur mot de passe sur leur espace abonné. Elle indique, en outre, que le mot de passe initial qu'elle a attribué présente un niveau de robustesse élevé et que l'espace abonné permet uniquement d'accéder à des informations basiques et non à des informations sensibles. Enfin, la société a annoncé avoir pris plusieurs mesures pour se mettre en conformité avec les obligations découlant de l'article 32 du RGPD s'agissant de la sécurité relative aux mots de passe via le renforcement de la robustesse des mots de passe générés ou créés par la société et le renouvellement obligatoire des mots de passe lors d'une procédure de récupération ou dès la première connexion. La société indique également avoir cessé de stocker en clair des mots de passe au sein de la base de données et d'avoir cessé de communiquer des mots de passe en clair (notamment, via l'arrêt de la transmission des mots de passe des nouveaux abonnés en clair par courriel, la création, par les nouveaux abonnés, de leur mot de passe, qui devra être conforme aux préconisations de la CNIL en la matière et la

suppression des formulaires au format papier devant être remplis puis adressés par voie postale pour obtenir la suppression d'un compte […] accès gratuit dans lequel la communication du mot de passe en clair était préalablement requise).

54. La formation restreinte considère qu'en l'espèce, la procédure d'authentification ainsi que les modalités de stockage et de transmission des mots de passe mises en œuvre par la société ne sont pas adaptées au regard du risque que ferait peser sur la personne concernée la captation de leur identifiant et de leur mot de passe par un tiers.

55. 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. La mise en place d'une politique d'authentification robuste constitue une mesure élémentaire de sécurité qui participe généralement au respect des obligations de l'article 32 du RGPD. Malgré le caractère non impératif de la délibération n° 2017-012 du 19 janvier 2017 ayant pour objet d'apporter des recommandations relatives aux mots de passe, du guide de la CNIL relatif à la sécurité des données à caractère personnel et de la note technique de l'ANSSI relative aux mots de passe cités dans le rapport, ces derniers exposent des précautions élémentaires de sécurité correspondant à l'état de l'art et constituent ainsi un éclairage pertinent pour apprécier la suffisance des mesures mises en place par un responsable de traitement.

56. En l'espèce, s'agissant de la procédure d'authentification, la formation restreinte considère que l'utilisation d'un mot de passe court ou simple sans imposer de catégories spécifiques de caractères et sans mesure de sécurité complémentaire, peut 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. Les mesures de blocage ont pour objectif de limiter ces types d'attaques.

57. La formation restreinte relève que la Commission recommande 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 satisfaire aux exigences de robustesse des mots de passe et assurer un niveau de sécurité suffisant, lorsque l'authentification repose, comme en l'espèce, sur un identifiant et un mot de passe, sans mise en place d'une mesure de sécurité complémentaire, le mot de passe doit comporter au minimum douze caractères et contenir au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial. Lorsque le mot de passe comporte huit caractères, contenant trois des quatre catégories de caractères (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux), il doit s'accompagner d'une mesure de sécurité complémentaire afin d'assurer un niveau de sécurité et de confidentialité suffisant.

58. La formation restreinte relève que la nécessité d'un mot de passe fort est également soulignée par l'ANSSI, qui précise 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 .

59. Par conséquent, en l'espèce, la formation restreinte considère qu'eu égard au volume et à la nature des données à caractère personnel pouvant être contenues dans les millions de comptes d'abonnés (notamment les nom, prénom, numéro de ligne fixe, numéro de téléphone mobile, adresse électronique et factures), l'imposition par cette dernière de mots de passe de connexion aux comptes des clients, composés uniquement de huit caractères, pouvant être d'une seule catégorie de caractères, sans mesure de sécurité complémentaire, ainsi que l'acceptation de leur renouvellement selon ces mêmes modalités, ne permet pas d'assurer la sécurité des données à caractère personnel traitées par la société ni d'empêcher que des tiers non autorisés aient accès aux données à caractère personnel des clients.

60. S'agissant de la procédure de stockage en clair des mots de passe, la formation restreinte constate que toute personne ayant accès à la base de données des clients de la société […] – qu'il s'agisse des administrateurs des systèmes d'information au sein de la société ou d'un attaquant en cas de compromission de celle-ci – pouvait directement collecter les identifiants et mots de passe en clair de chacun des abonnés et ainsi accéder aux informations contenues dans leurs comptes, puis éventuellement les modifier, tenter d'accéder à d'autres comptes de services au moyen de ces identifiants (les mêmes identifiants et mots de passe étant souvent utilisés sur plusieurs services) ou, encore, revendre ces derniers à d'autres attaquants.

61. S'agissant de la transmission du mot de passe en clair, le fait que ces éléments soient transmis en clair via un simple courrier électronique ou postal, les rend aisément et immédiatement utilisables par un tiers qui les intercepterait ou aurait un accès indu à la messagerie électronique de l'utilisateur, dès lors que ces mots de passe n'ont pas une durée limitée ou que leur modification n'est pas exigée lors de la première utilisation. Ce tiers pourrait alors, non seulement accéder à toutes les données à caractère personnel présentes dans le compte utilisateur […] de la personne concernée (nom,

prénom, numéro de téléphone […], adresse postale et adresse électronique) mais également télécharger ses factures et le relevé de ses consommations, procéder à la modification du mot de passe, de l'adresse de messagerie électronique ou encore des options du compte. Compte tenu de ces conséquences potentielles pour la protection des données à caractère personnel et de la vie privée des personnes, la formation restreinte considère que les mesures déployées pour garantir la sécurité des données en l'espèce sont insuffisantes.

62. La formation restreinte retient que des manquements aux obligations qui découlent de l'article 32 du RGPD sont ainsi constitués en raison de l'insuffisante robustesse des mots de passe ainsi que de leur stockage et transmission en clair aux abonnés de la société.

63. Elle relève que, dans le cadre de la présente procédure, la société a justifié avoir pris des mesures pour se mettre en conformité avec les obligations découlant de l'article 32 du RGPD.

2. Sur le reconditionnement des boîtiers […]

64. Le rapporteur, pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant de l'article 32 du RGPD, se fonde sur le fait que 4 137 boîtiers ont été remis en circulation sans que leur reconditionnement soit parfait , en raison notamment d'une erreur ayant conduit à la suppression d'une procédure (également appelée séquence de test) destinée à effacer les données stockées sur les disques durs de ces boîtiers […] .

65. En défense, la société fait valoir que l'obligation de sécurité prévue par l'article 32 du RGPD est une obligation de moyen, qui lui impose uniquement de mettre en œuvre des mesures de sécurité adaptées aux risques du traitement qu'elle effectue. Elle estime qu'en l'espèce, les mesures mises en œuvre étaient suffisantes, compte tenu du fait que cet incident résulte de deux erreurs humaines successives, qu'il existe un risque anecdotique que les […] soient détournées pour y stocker des données sensibles et que la circonstance qu'un seul abonné ait signalé ces faits conduit à ce qu'un seul accès effectif à la vie privée d'un ancien abonné se soit réalisé , ce qui reflète la probabilité limitée que ce risque se matérialise en pratique . La société considère en outre que la gravité de cet incident doit être nuancée compte tenu de la nature des données usuellement stockées sur les […] – qui se limitent principalement à l'enregistrement des programmes TV et marginalement au stockage de photos ou vidéos personnelles. Enfin, la société rappelle qu'à l'issue de la campagne visant à rappeler les boîtiers concernés, elle a adressé une […] de remplacement aux 322 abonnés n'ayant pas restitué leur […] et qu'en tout état de cause, celles-ci ont été désactivées en juillet 2022.

66. La formation restreinte considère tout d'abord que les mesures techniques et organisationnelles mises en œuvre n'étaient pas suffisantes au regard du risque de violation de données en l'espèce puisqu'aucun processus de levée d'alerte n'a été mis en œuvre pour contrôler la réalisation effective des séquences de tests incluant l'effacement des données. Cette défaillance a rendu possible l'accès, par des tiers non autorisés, en l'occurrence les nouveaux détenteurs des 4 137 boîtiers […] mal reconfigurés, aux données d'anciens abonnés qui auraient été stockées sur les disques durs de ces boîtiers. Ces données pouvaient être des photos, des vidéos personnelles ou l'enregistrement des programmes de télévision par l'utilisateur. La formation restreinte rappelle également que ce n'est pas la violation de données qui est en cause, mais l'insuffisance de mesures de sécurité qui a rendu possible la survenance d'une telle violation.

67. Ensuite, sur la probabilité limitée de réalisation du risque du fait de la réception d'un seul signalement par la société, la formation restreinte note que ce signalement est révélateur de l'insuffisance de mesures techniques et organisationnelles mises en œuvre, ce dernier ayant conduit à la découverte de l'incident.

68. En outre, sur la nature des données stockées dans les boîtiers […], la formation restreinte prend acte de ce que l'usage courant et principal des […] est l'enregistrement par l'utilisateur des programmes de télévision, mais considère que cet usage courant ne permet pas d'écarter la possibilité que certains des boîtiers […] mal reconditionnés contiennent des photos ou des vidéos personnelles, qui ont un caractère hautement personnel.

69. Enfin, la formation restreinte considère que le fait qu'une […] de remplacement ait été adressée aux 322 abonnés n'ayant pas restitué leurs anciens boîtiers ne permet pas d'écarter le risque que des ces derniers aient eu accès aux données d'anciens abonnés. En effet, à la date du 31 mars 2022 – soit plus de trois ans après le signalement de l'incident - la société indiquait que ce risque n'était toujours pas écarté puisque 322 [boîtiers] sont toujours utilisés par les abonnés sans que nous [la société] sachions si les données enregistrées sont celles de l'abonné antérieur ou de l'abonné qui l'utilise . En outre, seule la désactivation des 322 […] non restitués a permis d'écarter ce risque ; or cette désactivation a eu lieu en juillet 2022, soit plus de trois ans après le signalement de l'incident.

70. La formation restreinte considère qu'un manquement aux obligations qui découlent de l'article 32 du RGPD est constitué en raison de l'insuffisance des mesures techniques et organisationnelles du processus de reconditionnement des boîtiers […] pour assurer la sécurité des données à caractère personnel des abonnés de la société.

71. Elle relève que, dans le cadre de la présente procédure, la société a justifié avoir pris des mesures pour se mettre en conformité avec les obligations découlant de l'article 32 du RGPD.

D. Sur le manquement à l'obligation de documenter toute violation de données à caractère personnel

72. Aux termes de l'article 33, paragraphe 5, du RGPD :

Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.

73. Le rapporteur, pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant de l'article 33 du RGPD, fait valoir que la violation de données n'a pas été documentée conformément aux dispositions de l'article précité.

74. En défense, la société fait valoir que l'article 33 du RGPD n'impose pas de formalisme et que la documentation d'un incident de sécurité n'a pas obligatoirement à figurer dans un registre de violation de données. Elle considère que la documentation fournie à la suite du contrôle est conforme aux conditions de l'article précité et qu'elle n'est pas tenue d'y spécifier le résultat des mesures prises à savoir, comme le demande le rapporteur, le nombre de […] récupérées par […] après l'incident et la date de leur récupération .

75. La formation restreinte relève qu'à l'issue des deux jours de contrôle sur place, la société n'avait pas documenté la violation de données constituée par la remise en circulation de 4 137 boîtiers mal reconditionnés au sein d'un registre de violation de données. La documentation communiquée ultérieurement en réponse aux demandes de la délégation de contrôle ne permettait pas de savoir si l'ensemble des boîtiers […] dont le reconditionnement n'avait pas été effectif avaient été rapatriés et, le cas échéant, à quelle date. Or, la formation restreinte relève qu'il ressort du principe de responsabilité posé par le RGPD que le responsable de traitement doit suffisamment documenter ses pratiques pour être en mesure de démontrer sa conformité. En l'espèce, la formation restreinte considère que les éléments précités - à savoir si l'ensemble des boîtiers […] dont le reconditionnement n'avait pas été effectif avaient été rapatriés et, le cas échéant, à quelle date - font partie des informations devant être communiquées pour connaître les éléments factuels permettant d'apprécier l'effectivité de la mesure prise dans le traitement de la violation.

76. La formation restreinte considère qu'un manquement aux obligations qui découlent de l'article 33 du RGPD est constitué dès lors que la documentation établie à l'issue des deux jours de contrôle sur place et ultérieurement en réponse aux demandes de la délégation de la CNIL, ne permettait pas de prendre connaissance de l'ensemble des mesures prises pour remédier à la violation de données à caractère personnel et de ses effets.

77. Elle relève que, dans le cadre de la présente procédure, la société a justifié avoir pris des mesures pour se mettre en conformité avec les obligations découlant de l'article 33 du RGPD.

III. Sur les mesures correctrices et leur publicité

78. 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.

79. Aux termes de l'article 83 du RGPD :

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. , 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.

80. En premier lieu, sur le principe du prononcé d'une amende, la société soutient qu'une telle mesure n'est pas nécessaire et ne serait pas proportionnée au regard des faits qui lui sont reprochés.

81. 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, les mesures prises par le

responsable du traitement pour atténuer le dommage subi par les personnes concernées, le degré de coopération avec l'autorité de contrôle et les catégories de données à caractère personnel concernées par la violation.

82. La formation restreinte considère d'abord que la société a fait preuve d'une négligence certaine s'agissant de principes fondamentaux du RGPD puisque plusieurs manquements sont constitués, portant notamment sur les droits des personnes et la sécurité. La formation restreinte ajoute que trois manquements ont donné lieu à des plaintes.

83. La formation restreinte relève ensuite que la société est un acteur particulièrement important du secteur des fournisseurs d'accès à Internet puisqu'elle dénombrait, en 2021, environ 6,9 millions d'abonnés, ce qui la classait parmi les principaux fournisseurs d'accès à Internet en France. Elle dispose donc de ressources importantes lui permettant de traiter les questions de protection des données personnelles.

84. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative au regard des manquements constitués aux articles 12, 15, 17, 32 et 33 du RGPD.

85. En deuxième lieu, s'agissant du montant de l'amende, la formation restreinte rappelle que les amendes administratives doivent être à la fois dissuasives et proportionnées. En l'espèce, la formation restreinte considère que la société a méconnu ses obligations résultant des articles 12, 15, 17, 32 et 33 du RGPD, portant notamment sur les droits des personnes et sur des mesures élémentaires en lien avec la sécurité des données à caractère personnel. La formation restreinte ajoute que plusieurs manquements ont donné lieu à des plaintes, même si elle observe que les plaintes révélant l'existence de manquements apparaissent peu nombreuses – en effet, leur nombre, de dix, doit être rapporté au nombre d'abonnés s'élevant à environ 6,9 millions –de sorte que ces manquements ne peuvent être regardés comme ayant un caractère systémique.

86. La formation restreinte rappelle également que l'activité de la société et sa situation financière doivent être prises en compte pour la détermination de la sanction et notamment, en cas d'amende administrative, de son montant. Elle relève à ce titre que la société fait état d'un chiffre d'affaires de […] euros en 2020 pour un résultat net s'élevant à environ […] euros.

87. Dès lors, au vu de ces éléments, la formation restreinte considère que le prononcé d'une amende administrative de 300 000 (trois cent mille) euros apparaît justifié.

88. En troisième lieu, une injonction de mettre en conformité le traitement avec les dispositions de l'article L. 34-5 du CPCE et des articles 7-1, 15, 17, 32 et 33 du RGPD a été proposée par le rapporteur lors de la notification du rapport.

89. La société soutient que les actions qu'elle a mises en œuvre s'agissant de l'ensemble des manquements relevés doivent conduire à ne pas donner suite à la proposition d'injonction du rapporteur.

90. Comme indiqué précédemment, la formation restreinte relève que la société a pris des mesures de mise en conformité de ses traitements avec les dispositions des articles 17, 32 et 33 du RGPD. La formation restreinte considère cependant que la société n'a pas fourni, à la date de la clôture de l'instruction, d'éléments lui permettant d'attester d'une mise en conformité de ses traitements avec les dispositions de l'article 15 du RGPD, dans la mesure où elle entend fournir uniquement des informations relatives à l'identité de la source primaire de la collecte des données de la personne concernée (c'est-à-dire le premier acteur de la chaîne à avoir collecté les données à caractère personnel de la personne concernée). En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une injonction sur ce point.

91. En dernier lieu, s'agissant de la publicité de la décision de sanction, la société soutient qu'une telle mesure ne serait ni nécessaire ni proportionnée au regard des manquements allégués qu'elle réfute et de sa mise en conformité.

92. La formation restreinte considère que la publicité de la sanction se justifie au regard de la pluralité des manquements commis et de la nécessité de porter à la connaissance des personnes, et notamment des clients concernés, les défaillances liées aux traitements de données à caractère personnel mis en œuvre par la société. Elle estime par ailleurs que cette mesure permettra d'informer les personnes concernées de l'existence passée des manquements sanctionnés, dans la mesure notamment où ces faits ont fait l'objet de plusieurs plaintes.

PAR CES MOTIFS

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

• prononcer à l'encontre de la société […] une amende administrative d'un montant de 300 000 (trois cent mille) euros pour les manquements aux articles 12, 15, 17, 32 et 33 du RGPD ;

• prononcer à l'encontre de la société […] une injonction d'apporter une réponse exhaustive aux demandes de Messieurs […] (plainte n° 19014037), […] (plainte n° 19015831), […] (plainte n° 19016618) et […] (plainte n° 19005208) qui précise

l’identité du courtier en données à partir duquel elle a obtenu les données des personnes concernées ;

• assortir l’injonction d’une astreinte de 500 (cinq cent) euros par jour de retard à l’issue d’un délai d’un 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 ;

• 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’Etat dans un délai de deux mois à compter de sa notification.