Délibération SAN-2021-021 du 28 décembre 2021

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Date de publication sur Légifrance : Mardi 04 janvier 2022
Etat juridique : En vigueur

Délibération de la formation restreinte n°SAN-2021-021 du 28 décembre 2021 concernant la société X

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Monsieur Alexandre LINDEN, président, Monsieur Philippe-Pierre CABOURDIN, vice-président, Madame Anne DEBET, 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 ;
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 ces organismes ou pour le compte des sociétés [...] et [...] ;
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 2 août 2021 ;
Vu les observations écrites versées par la société [...] le 13 septembre 2021 ;
Vu la réponse du rapporteur à ces observations notifiées le 4 octobre 2021 à la société ;
Vu les nouvelles observations écrites versées par la société [...] le 22 octobre 2021, 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 4 novembre 2021 :
- Monsieur François PELLEGRINI, commissaire, entendu en son rapport ;

En qualité de représentants de la société [...] :
- […] ;
- […] ;
- […] ;
- […] ;
- […] ;
- […] ;
- […].

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 [...]. La société est un opérateur

de téléphonie mobile qui commercialise des téléphones et / ou des forfaits mobiles. Créée en […], elle compte environ […] salariés.

2. Pour l'année 2020, la société [...] a réalisé un chiffre d'affaires de […] euros, pour un résultat net de […] euros. Au 21 décembre 2020, la société dénombrait environ […] abonnés aux offres mobiles, […].

3. Entre le mois de décembre 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 19 plaintes à l'encontre de la société [...]. Les plaignants faisaient notamment état des difficultés rencontrées dans l'exercice de leurs droits d'accès ou d'opposition à recevoir des messages de prospection commerciale.

4. Pour les besoins de l'instruction des plaintes, deux opérations de contrôle sur place dans les locaux de la société [...] puis de la société [...] ont été effectuées en application de la décision n° 2019-188C du 26 septembre 2019 de la présidente de la CNIL. Ces missions ont été réalisées respectivement les 21 et 22 janvier 2020. En application de cette même décision, un contrôle sur pièces a également été effectué auprès des sociétés [...] et [...] le 3 juin 2020.

5. Ces missions avaient pour objet de vérifier le respect, par la société [...], de l'ensemble des dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après " le 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 ").

6. Au cours des deux premiers contrôles, la délégation de la CNIL s'est attachée à vérifier la gestion, par la société [...], des droits des personnes, et plus particulièrement la manière dont elle avait traité les demandes d'exercice des droits des personnes ayant saisi la Commission de plaintes. Ces contrôles avaient également pour but de vérifier les mesures de sécurité mises en place par la société pour protéger les données à caractère personnel qu'elle traite.

7. A l'issue de ces contrôles, les procès-verbaux n° 2019-188/1 et n° 2019-188/2 ont été notifiés à la société [...] par courrier daté du 23 janvier 2020. La société a transmis aux services de la Commission, par courriels des 3 et 10 février 2020, les pièces complémentaires sollicitées à l'issue de ces missions de contrôle.

8. Au regard des réponses apportées par la société, et en vue de préciser certains constats précédemment effectués, un nouveau contrôle sur pièces a été diligenté par la CNIL le 3 juin 2020, qui s'est traduit par l'envoi d'un questionnaire à la société [...].

9. La société a transmis aux services de la Commission, par courriel du 29 juin 2020, les pièces complémentaires et les informations sollicitées à l'occasion de ce contrôle.

10. 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 et en a informé la société par courrier du 23 décembre 2020.

11. À l'issue de son instruction, le rapporteur a, le 2 août 2021, fait notifier à la société [...] un rapport détaillant les manquements au RGPD qu'il estimait constitués en l'espèce. Le courrier de notification du rapport indiquait à la société qu'elle disposait d'un délai d'un mois pour communiquer ses observations écrites en application des dispositions de l'article 40 du décret n° 2019-536 du 29 mai 2019.

12. 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 15, 16, 21, 25 et 32 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, ainsi qu'une amende administrative. 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.

13. Le 13 septembre 2021, la société a produit ses observations en réponse au rapport de sanction.

14. Le 23 septembre 2021, le rapporteur a sollicité un délai pour répondre aux observations formulées par la société [...]. Par courrier du 24 septembre 2021, le président de la formation restreinte a avisé le rapporteur qu'il bénéficiait d'un délai supplémentaire de six jours pour produire ses observations. Par un courrier daté de ce même jour, la société a été avisée par le président de la formation restreinte qu'elle bénéficiait également d'un délai supplémentaire de six jours pour produire ses observations.

15. Par courrier du 4 octobre 2021, la réponse du rapporteur aux observations de la société lui a été adressée, accompagnée d'une convocation à la séance de la formation restreinte du 4 novembre 2021.

16. Le 22 octobre 2021, la société [...] a produit de nouvelles observations en réponse à celles du rapporteur.

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

II. Motifs de la décision
A. Sur la responsabilité de traitement de la société [...]
18. L'article 4, paragraphe 7 du RGPD prévoit que le responsable du traitement est " la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ".

19. Dans son rapport, le rapporteur souligne d'abord que la délégation a été informée lors du contrôle sur place du 21 janvier 2020 que " la société [...] est l'opérateur de radio télécommunication mobile du [...] et la société [...] est l'opérateur de télécommunication fixe du [...] " et que " chaque client est rattaché à la société [...] et / ou à la société [...] " en fonction de l'offre à laquelle il a souscrit. Le rapporteur relève ensuite que chacune des sociétés [...] et [...] " dispose de son propre système d'information dans lequel figurent [ses] clients " et que les " bases de prospects sont également réparties par société ", de sorte que les sociétés peuvent accéder aux bases de données qui leur sont propres. Une base de données commune est également utilisée par chacune des sociétés, pour son compte, afin d'effectuer de la prospection commerciale. Le rapporteur observe enfin que le registre de traitement transmis à la délégation de la CNIL indique que la société [...] se considère notamment responsable des traitements relatifs à la gestion des contrats souscrits auprès d'elle par ses abonnés et des traitements liés aux opérations de prospection commerciale qui sont réalisées auprès de ses clients et prospects pour son compte.

20. La formation restreinte relève que ces éléments n'ont pas été contestés par la société [...]. Elle considère qu'il résulte de ce qui précède que la société [...] doit être regardée comme responsable des traitements des données à caractère personnel de ses clients, mis en œuvre dans le cadre de l'exécution des contrats d'abonnement de téléphonie mobile, et des personnes qu'elle contacte à des fins de prospection commerciale, dans la mesure où elle détermine les finalités et les moyens de ces traitements.
B. Sur les griefs de la société en lien avec la procédure
21. La société estime que le rapporteur a manqué à son devoir de diligence en lui transmettant, plus de dix-huit mois après les opérations de contrôle et pendant les congés du mois d'août, le rapport proposant à la formation restreinte de retenir une sanction à son encontre. La société fait valoir, sur la base d'une moyenne qu'elle indique avoir établie à partir des décisions de la formation restreinte rendues entre 2018 et 2021 à l'issue d'un contrôle sur place, que le délai moyen de transmission de la procédure à la formation restreinte est d'environ treize mois et, qu'en l'espèce, ce délai a été porté à dix-huit mois. La société fait également valoir qu'elle n'a pas été mise en mesure de prendre connaissance, avant la réception du rapport, de deux plaintes sur lesquelles le rapporteur s'est fondé pour retenir à son encontre un manquement à son obligation d'assurer la sécurité du traitement. Enfin, la société s'étonne de ne pas avoir été au préalable mise en demeure de corriger les manquements à l'origine des faits litigieux, ce qui démontrerait la faible gravité des manquements allégués par le rapporteur, notamment s'agissant de ses procédures de sécurité.

22. En premier lieu, la formation restreinte relève que les textes applicables ne prévoient pas de limite au délai entre la conduite des contrôles et la transmission d'un rapport proposant une sanction. De plus, la présente procédure est intervenue pendant la crise sanitaire, qui a engendré un allongement des délais.

23. En deuxième lieu, s'agissant des deux saisines n° 19012802 et n° 19019490 pour lesquelles la société fait valoir qu'elle n'a pas été mise en mesure d'en prendre connaissance avant la réception du rapport, la formation restreinte rappelle que les textes applicables n'imposent pas une instruction préalable des plaintes avant la transmission d'un rapport proposant une sanction et n'empêchent pas le rapporteur de les porter à la connaissance du responsable de traitement au stade de son rapport, les plaintes étant à cette occasion versées à la procédure contradictoire. Enfin, l'article 50 du règlement intérieur de la CNIL impose uniquement que l'objet de la plainte soit " communiqué au responsable de traitement mis en cause […] afin que celui-ci fournisse toutes les explications utiles ", ce qui a été fait en l'espèce par le biais du rapport de sanction.

24. En troisième lieu, s'agissant de la transmission du rapport au mois d'août et de la nécessité, pour la société, d'y répondre pendant les vacances estivales, la formation restreinte observe que la société a bénéficié d'un délai d'environ six semaines pour produire ses premières observations, pour tenir compte de cette période, étant rappelé que l'article 40 du décret n° 2019-536 du 29 mai 2019 n'impose qu'un délai minimum d'un mois.

25. En dernier lieu, s'agissant du grief relatif à l'absence de mise en demeure préalable, la formation restreinte relève d'abord qu'il ressort des dispositions de l'article 20 de la loi " Informatique et Libertés " modifiée par la loi n° 2018-493 du 20 juin 2018 que l'autorité de contrôle dispose d'un ensemble de mesures correctrices, adaptées selon les caractéristiques propres à chaque cas, qui peuvent être combinées entre elles et être précédées ou non d'une mise en demeure. Les mesures correctrices peuvent être prises directement dans tous les cas.

26. La formation restreinte relève également que le Conseil constitutionnel (Cons. const., 12 juin 2018, n° 2018-765 DC) n'a pas émis de réserve s'agissant de la possibilité pour le président de la CNIL d'engager une procédure de sanction sans mise

en demeure préalable. Enfin, la formation restreinte rappelle que le Conseil d'État a jugé (CE, 9 octobre 2020, Société SERGIC, n° 433311) qu'il " résulte clairement [des dispositions de l'article 20 de la loi du 6 janvier 1978 modifiée], que le prononcé d'une sanction par la formation restreinte de la CNIL n'est pas subordonné à l'intervention préalable d'une mise en demeure du responsable du traitement ou de son sous-traitant par le président de la CNIL […] ".

27. En conséquence, la formation restreinte considère que la présente procédure et les différentes actions menées dans ce cadre n'ont pas porté atteinte aux droits de la défense de la société.

C. Sur la qualification des faits au regard du RGPD

1. Sur le manquement à l'obligation de respecter le droit d'accès des personnes aux données à caractère personnel les concernant

28. L'article 12, paragraphe 3, du RGPD prévoit que " 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 ". En outre, aux termes du paragraphe 4 de cet article " 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 ".

29. L'article 15, paragraphe 1, du RGPD prévoit le droit pour une personne 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 aux données à caractère personnel la concernant et notamment " lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source ". Aux termes de l'alinéa 3 du même article " le responsable du traitement fournit une copie des données à caractère personnel faisant l'objet d'un traitement ".

30. Le rapporteur se fonde sur trois saisines reçues par la CNIL, émanant de Messieurs […] (plainte n° 19018344), […] (plainte n° 19008608) et […] (plainte n° 19016049), dans le cadre desquelles les plaignants faisaient état des difficultés rencontrées dans l'exercice de leurs droits, pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant de l'article 15 du RGPD.

31. En défense, la société fait valoir qu'aucun manquement ne peut lui être reproché au titre de ces trois saisines. Elle indique qu'il s'agit de faits isolés, sur la base desquels l'existence d'un problème systémique ne saurait être déduite. Elle fait également valoir la différence entre le nombre réduit de plaintes relevées dans le rapport concernant l'exercice des droits (7) et le nombre de demandes d'exercice des droits traitées par la société par an (environ 600). Elle considère ainsi que les manquements allégués sont révélateurs d'erreurs humaines mais aucunement d'un " problème quant au fonctionnement même de la procédure " de [...]. Enfin, la société indique que les saisines litigieuses sont contemporaines de la date d'entrée en vigueur du RGPD et antérieures à la mise en place d'un nouvel outil de ticketing utilisé par [...], depuis juin 2019, qui a permis d'apporter des améliorations à la procédure de traitement des demandes d'exercice de droit de [...]. Dès lors, elle considère que ces dysfonctionnements ponctuels sont à présent résolus.

32. En premier lieu, s'agissant de la saisine n° 19008608 de mai 2019, Monsieur […] a saisi la CNIL, expliquant avoir demandé à la société [...], via l'adresse électronique dédiée aux demandes " Informatique et Libertés ", l'accès aux données le concernant qui seraient associées à son numéro de téléphone.

33. Le rapporteur observe qu'il ressort des éléments communiqués par la société à la suite des contrôles que, si la société indique bien avoir reçu la demande du plaignant, elle n'a en revanche " pas retrouvé de trace de réponse apportée au plaignant ". Le rapporteur considère donc que la société a manqué à son obligation de traiter la demande d'accès du plaignant.

34. En défense, la société explique tout d'abord qu'elle ne pouvait satisfaire à cette demande puisqu'elle ne disposait plus des données demandées. Elle précise en ce sens que Monsieur […] ayant résilié son contrat avec la société [...] quatre ans avant d'adresser sa demande d'accès, elle ne disposait plus que de l'information relative à l'existence d'une relation contractuelle jusqu'au 4 mars 2015. Suite à l'interrogation du rapporteur s'étonnant de l'absence de données à caractère personnel relatives au plaignant qui seraient conservées par la société en base d'archivage intermédiaire au titre de ses obligations légales ou comptables (données de facturation, gestion d'un éventuel contentieux, etc.), dans son second mémoire en défense, la société indique avoir retrouvé treize factures concernant le plaignant à l'issue d'une recherche dans sa base d'archivage et avoir adressé, par courriel du 14 octobre 2021, un complément de réponse au plaignant en lui fournissant ces éléments.

35. La formation restreinte rappelle d'abord qu'il ressort de l'article 12, paragraphe 4, du RGPD que lorsque le responsable de traitement ne détient plus de données sur la personne qui exerce son droit d'accès (par exemple si les données ont été supprimées), il doit néanmoins répondre au demandeur dans un délai maximal d'un mois pour le lui indiquer. Ainsi, la formation restreinte considère que la société aurait à tout le moins dû informer le plaignant que, selon elle, elle ne disposait plus d'information le concernant, mis à part celle relative à l'existence d'une relation contractuelle jusqu'au 4 mars 2015.

36. La formation restreinte relève ensuite que la société disposait d'autres données relatives au plaignant, en l'occurrence les treize factures conservées par la société dans sa base d'archivage intermédiaire, qui entrent dans le périmètre des données devant être communiquées au titre du droit d'accès. A cet égard, la formation restreinte rappelle que les personnes concernées doivent pouvoir avoir connaissance du fait que des données les concernant sont conservées et traitées par le responsable de traitement, y compris plusieurs années après la rupture de la relation contractuelle, comme c'est le cas en l'espèce. En effet, elle souligne que seule la communication de ces données permet aux personnes concernées de mesurer la nature et l'ampleur des traitements mis en œuvre par la société. En l'espèce, la formation restreinte relève que ce n'est qu'à compter de l'envoi du courriel du 14 octobre 2021 que la société a apporté une réponse exhaustive à la demande d'accès du plaignant, soit plus de deux ans après que Monsieur […] eut exercé ses droits, consécutivement à l'engagement de la procédure de sanction et la réception du rapport en réponse aux observations de la société datées du 4 octobre 2021.

37. Dans ces conditions, la formation restreinte considère qu'en ne donnant pas suite à la demande d'accès et en ne répondant pas au demandeur dans les délais prévus, la société a méconnu ses obligations découlant des articles 12 et 15 du RGPD.

38. Elle relève néanmoins que, dans le cadre de la procédure de sanction, la société a justifié avoir apporté une réponse au plaignant et, dès lors, avoir pris des mesures de mise en conformité avec les obligations du RGPD.

39. En deuxième lieu, s'agissant de la saisine n° 19016049 de septembre 2019, Monsieur […] a saisi la CNIL, expliquant avoir demandé à la société [...] de lui indiquer si elle détenait des données à caractère personnel le concernant. Dans l'affirmative, le plaignant souhaitait obtenir une copie de ses données et, plus particulièrement, la copie de l'enregistrement d'un appel qui aurait été passé par une personne ayant usurpé son identité ainsi que tout document qui aurait été envoyé à cette occasion.

40. Le rapporteur relève qu'il ressort des constats effectués dans le cadre de la procédure de contrôle que la société n'a pas apporté de réponse au plaignant, sans qu'elle ait été en mesure d'en justifier la raison. Il a également constaté que cette demande n'a pas été qualifiée comme une demande " Informatique et Libertés " mais comme une demande de " résiliation ". Le rapporteur considère donc que la société a manqué à son obligation d'indiquer au plaignant si des données à caractère personnel le concernant figuraient dans les traitements qu'elle met en œuvre et, le cas échéant, à son obligation de lui en adresser une copie.

41. En défense, la société fait valoir que cette demande n'a pas été adressée au service dédié aux demandes d'exercice des droits, de sorte qu'une erreur humaine a pu être commise dans sa qualification en tant que demande de résiliation et non en tant que demande de droit d'accès. Ensuite, la société explique qu'elle ne pouvait pas apporter une réponse favorable au plaignant dans la mesure où sa demande d'accès était relative aux données à caractère personnel d'un tiers. S'agissant des autres données détenues par la société, relatives au plaignant, elle indique y avoir répondu par courriel du 26 août 2021 en joignant une copie des données à caractère personnel le concernant qui sont enregistrées en base de données.

42. Sur le premier point portant sur l'adresse à laquelle le plaignant a envoyé sa demande, la formation restreinte considère que s'il n'est pas contesté que le plaignant n'a pas adressé sa demande à l'adresse courriel ou postale qui est identifiée par la société comme étant le canal dédié pour la transmission des demandes d'exercice des droits, il n'en demeure pas moins qu'il appartenait à la société, dès lors que cette demande a bien été reçue par cette dernière et qu'elle était claire en ses termes, de la traiter dans les délais prévus par le RGPD et de veiller à cet effet à ce qu'elle soit transmise aux services compétents. En effet, si la mise en œuvre de mesures organisationnelles pour faciliter l'exercice des droits des personnes est conforme aux exigences et à l'objectif poursuivi par le RGPD, cela ne saurait en revanche exonérer la société de son obligation de répondre aux demandes qui lui sont faites dès lors qu'elles ne lui seraient pas adressées par le canal qu'elle aura dédié à cet effet, a fortiori lorsque, comme c'est le cas en l'espèce, le contenu de la demande est clair.

43. Sur le second point en lien avec l'argument de la société selon lequel la demande d'accès portait sur des données d'un tiers, la formation restreinte relève que la demande du plaignant est, à titre principal, une demande générale de droit d'accès qui vise, à titre subsidiaire, la communication de données relatives à un appel téléphonique. Dès lors, si la formation restreinte peut entendre les éléments mis en avant par la société sur la nécessité de préserver les droits des tiers en lien avec la partie de la demande relative à l'appel téléphonique, elle considère en revanche que la société aurait en tout état de cause dû apporter une réponse à la demande générale de droit d'accès effectuée par le plaignant, ce qui n'a

pas été le cas avant le 26 août 2021, soit plus de deux ans après sa demande et après la notification à la société le 2 août 2021 du rapport proposant à la formation restreinte de prononcer une sanction.

44. Dans ces conditions, la formation restreinte considère qu'en ne donnant pas suite à la demande d'accès et en ne répondant pas au demandeur dans les délais prévus, la société a méconnu ses obligations découlant des articles 12 et 15 du RGPD.

45. Elle relève néanmoins que, dans le cadre de la procédure de sanction, la société a justifié avoir apporté une réponse au plaignant et dès lors, avoir pris des mesures de mise en conformité avec les obligations du RGPD.

46. En troisième lieu, s'agissant de la saisine n° 19018344 datée du mois d'octobre 2019, Monsieur […] a saisi la CNIL, expliquant avoir demandé à la société [...] l'accès aux données le concernant.

47. Le rapporteur relève que la société n'a pas apporté de réponse au plaignant.

48. En défense, la société explique qu'elle n'a jamais reçu la demande du plaignant et qu'elle ne pouvait donc pas y répondre.

49. Dans la mesure où il n'est pas établi que le plaignant ait régulièrement exercé ses droits, la formation restreinte estime qu'il n'y a pas lieu de retenir de manquement au regard de l'obligation de respecter le droit d'accès s'agissant de cette plainte.

50. En dernier lieu, s'agissant tout d'abord de l'argument selon lequel les faits reprochés à la société auraient un caractère isolé et ne constitueraient dès lors pas un manquement aux dispositions applicables, la formation restreinte considère que, si les plaintes reçues par la CNIL ne révèlent en effet pas l'existence d'un manquement structurel en matière de droit d'accès, il n'en demeure pas moins que la société a méconnu ses obligations dans le traitement des demandes de Messieurs […] et […], alors que celles-ci étaient clairement formulées. Ces faits constituent bien un manquement aux obligations découlant des articles 12 et 15 du RGPD.

51. S'agissant ensuite de l'argument selon lequel les manquements qui sont reprochés à la société sont contemporains de la date d'entrée en application du RGPD, la formation restreinte rappelle que la plupart des obligations en cause, relatives aux droits d'accès, de rectification d'opposition et à la sécurité, existaient avant l'entrée en application du RGPD et que la loi " Informatique et Libertés " permettait déjà de les sanctionner. La formation restreinte considère, dès lors, que la société ne saurait utilement exciper d'un changement du cadre juridique pour justifier l'absence de conformité au jour des contrôles.

52. S'agissant enfin des améliorations apportées par la société à sa procédure de gestion des droits, tout en soulignant le caractère opportun de leur adoption pour améliorer le traitement des demandes, la formation restreinte rappelle qu'elles sont sans incidence sur l'existence du manquement au jour des contrôles, qui a duré de nombreux mois, et auquel il n'a été mis fin qu'après l'engagement de la procédure de sanction.

53. Au vu de ce qui précède, la formation restreinte considère qu'un manquement aux obligations des articles 12 et 15 du RGPD est constitué pour les plaintes déposées par Messieurs […] et […], peu important qu'il n'ait pas revêtu un caractère structurel.

54. Elle relève néanmoins que, dans le cadre de la procédure de sanction, la société a justifié avoir pris des mesures de mise en conformité avec les obligations du RGPD en apportant une réponse aux plaignants.
2. Sur le manquement relatif au droit de rectification en application de l'article 16 du RGPD

55. L'article 16 du RGPD prévoit le droit pour une personne d'obtenir du responsable du traitement " la rectification des données à caractère personnel la concernant qui sont inexactes ".

56. Le rapporteur se fonde sur une saisine reçue par la CNIL, émanant de Madame […] (plainte n° 19017852 intervenue en octobre 2019) et dans le cadre de laquelle la plaignante faisait état de difficultés rencontrées dans l'exercice de son droit de rectification, pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant de l'article 16 du RGPD. Elle indiquait avoir demandé à la société la rectification de son adresse postale figurant sur les factures téléphoniques, rendue nécessaire à la suite d'une renumérotation de la voirie par la mairie.

57. Le rapporteur observe qu'il ressort des constats effectués lors du contrôle du 22 janvier 2020 que la demande de la plaignante, formée en septembre 2019, n'a pas été prise en compte dès lors que l'adresse postale objet de la demande de rectification qui figure sur la facture datée du 14 octobre 2019 de la plaignante est la même que celle qui figure sur la facture datée du 14 janvier 2020. Le rapporteur a donc considéré qu'entre le 14 octobre 2019 et le 14 janvier 2020, la demande de rectification de la plaignante n'a pas été prise en compte par la société [...], soit plusieurs semaines après avoir adressé sa demande.

58. En défense, la société fait valoir qu'un traitement plus rapide de la demande de Madame […] était impossible au regard des impératifs de lutte contre la fraude. Elle précise en effet que lorsqu'une personne est à la fois cliente des sociétés [...] (car détentrice d'une ligne fixe) et [...] (car détentrice d'une ligne mobile), comme c'est le cas de la plaignante, il faut d'abord que l'adresse postale relative à la ligne fixe soit modifiée auprès de la société [...]. Elle précise que cette modification ne peut avoir lieu qu'une fois que l'adresse physique d'installation de la ligne téléphonique a été modifiée au sein d'un outil nommé " SETIAR ", qui est administré par la société ORANGE S.A. La société précise que cet outil " permet d'assurer la correspondance parfaite entre un numéro de téléphone et l'adresse d'installation physique de la ligne téléphonique, afin d'éviter toute erreur au moment de réaliser une opération sur cette ligne ". La société indique que ces différentes démarches ne peuvent pas être réalisées dans de brefs délais et qu'elle a agi de manière diligente pour traiter cette demande. La société considère en tout état de cause avoir répondu à la demande de Madame […] en lui adressant un courrier, le 17 septembre 2019, soit quatre jours après avoir reçu sa demande, lui indiquant qu'elle pouvait modifier son adresse en ligne, directement depuis son espace abonné.

59. La formation restreinte relève que la nécessité pour Madame […] de modifier elle-même son adresse dans son espace abonné aurait dû lui être mieux expliquée. Lors de la séance, la société a toutefois bien expliqué la nécessité, dans le cadre de la lutte contre la fraude, de passer par l'outil " SETIAR ".

60. Dans ces conditions, la formation restreinte prend acte des éléments apportés par la société en défense et considère que, s'agissant de cette plainte, les éléments du débat ne permettent pas de conclure à l'existence d'un manquement commis par la société.

3. Sur le manquement relatif à l'obligation de respecter la demande d'opposition des personnes concernées
61. L'article 12, paragraphe 3, du RGPD prévoit que " 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 ". Enfin, aux termes du paragraphe 4 de cet article " 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 ".

62. L'article 21 du RGPD dispose que " lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection ".

63. Le rapporteur se fonde sur quatre saisines reçues par la CNIL, émanant de Madame […] (plainte n° 19008223) ainsi que de Messieurs […] (plainte n° 19016318) et […] (plaintes n° 17017795 et n° 19018125) et dans le cadre desquelles les plaignants faisaient état de leurs difficultés dans l'exercice de leurs droits, pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant de l'article 21 du RGPD.

64. En défense, la société fait valoir qu'aucun manquement ne peut lui être reproché au titre de ces quatre saisines, car elle a pris en compte les demandes des plaignants dans ses bases de données. Elle fait ensuite valoir, en synthèse et comme développé au point 31, que les manquements allégués, eu égard au faible nombre de plaintes visées dans le rapport, sont tout au plus révélateurs d'erreurs humaines et non d'un problème quant au fonctionnement de la procédure de traitement des demandes d'exercice des droits par la société, qui constituerait un manquement aux dispositions applicables. Elle considère que les saisines litigieuses sont contemporaines de la date d'entrée en application du RGPD et antérieures à la mise en place du nouvel outil de ticketing en juin 2019 qui a permis d'améliorer le traitement des demandes d'exercice des droits.

65. En premier lieu, s'agissant de la saisine n° 19008223 intervenue en avril 2019, Madame […] a saisi la CNIL, expliquant qu'au cours des années 2018 et 2019, elle avait fait l'objet de démarchages téléphoniques par la société [...]. Au cours de cette période, la plaignante a manifesté à deux reprises, par courriers datés du 27 septembre 2018 et du 29 avril 2019, son opposition au traitement de ses données à caractère personnel à des fins de prospection.

66. Le rapporteur relève qu'il ressort des constats effectués par la délégation de contrôle que la plaignante a fait l'objet de deux campagnes de prospection le 28 août 2018 et le 11 avril 2019. Le rapporteur considère, dès lors, que la plaignante a été rendue destinataire de prospection commerciale près de huit mois après avoir, pour la première fois, manifesté son opposition.

67. En défense, la société admet qu'une " erreur humaine " a été commise, de sorte que la plaignante a fait l'objet d'une campagne de prospection en avril 2019 alors qu'elle avait préalablement exercé son droit d'opposition. Cependant, la société considère qu'aucun manquement ne peut être retenu à son encontre dans la mesure où elle a " dûment pris en compte " l'opposition de la plaignante formulée par courrier du 29 avril 2019, soit avant les opérations de contrôle sur place auxquelles la CNIL a procédé en janvier 2020.

68. Sur ce dernier point, la formation restreinte considère que l'existence d'un manquement ne saurait se limiter aux éléments attestant d'une non-conformité au jour des constatations effectuées dans le cadre d'un contrôle mené en application de l'article 19 de la loi " Informatique et Libertés ", mais peut tout aussi bien reposer sur tout élément obtenu par les services de la CNIL ou le rapporteur, attestant d'une non-conformité pour des faits ayant donné lieu à une plainte auprès de la CNIL et à une saisine de la formation restreinte, même si au moment du contrôle il a été mis fin à cette non-conformité. En l'espèce, le manquement repose sur des éléments probants, et est donc avéré.

69. Dans ces conditions, la formation restreinte considère qu'en ne prenant pas en compte l'opposition de la plaignante au traitement de ses données à caractère personnel à des fins de prospection dans les délais prévus, la société a méconnu ses obligations découlant des articles 12 et 21 du RGPD.

70. Elle relève néanmoins que, dans le cadre de la procédure de sanction, la société a justifié avoir pris en compte la demande d'opposition de la plaignante et dès lors, avoir pris des mesures de mise en conformité avec les obligations du RGPD.

71. En deuxième lieu, s'agissant de la saisine n° 19016318 intervenue en septembre 2019, émanant de Monsieur […], celui-ci a expliqué avoir fait l'objet de prospection commerciale par SMS sur des offres commercialisées par la société [...] jusqu'en juillet 2019, et fourni les captures d'écran des SMS correspondants dans sa plainte. Le plaignant indique avoir manifesté à plusieurs reprises son opposition au traitement de ses données à caractère personnel à des fins de prospection commerciale, notamment en juin 2018 auprès du délégué à la protection des données (ci-après " le DPO ") du [...].

72. Le rapporteur observe qu'il ressort des éléments complémentaires communiqués par la société à la suite des contrôles que la société n'avait " au jour de la présente communication, pas retrouvé de trace de réponse apportée au plaignant " sans être en mesure d'en justifier la raison. Il considère, dès lors, que la société n'a pas pris en compte l'opposition du plaignant à recevoir de la prospection commerciale puisque ce dernier a continué à recevoir des sollicitations jusqu'en juillet 2019, soit près d'un an après avoir manifesté son opposition.

73. En défense, la société indique avoir pris en compte " promptement " la demande du plaignant, dès le 25 juillet 2018, après avoir reçu deux courriels de sa part les 10 juin et 8 juillet 2018. La société joint à cet effet une capture d'écran de la date d'inscription du plaignant au sein d'une base " anti prospection ". S'agissant ensuite des captures d'écran jointes par le plaignant, la société fait valoir qu'elles sont " dénuées de valeur probante puisque le numéro du destinataire n'apparaît pas, de sorte qu'il n'est pas établi que les SMS capturés par le plaignant aient été effectivement reçus par lui ". En revanche, elle ne conteste pas l'absence de réponse à la demande d'opposition du plaignant. Elle indique que le nouvel outil de ticketing mis en place à compter de juin 2019 permet désormais d'assurer une réponse systématique aux personnes concernées.

74. La formation restreinte considère que même si la société indique avoir pris en compte " promptement " la demande du plaignant, ce n'est pas pour autant qu'elle lui a apporté une réponse, puisque ce dernier n'en a reçu aucune et n'a donc pas eu d'information quant à la prise en compte de sa demande, ce qui est contraire aux dispositions de l'article 12 du RGPD.

75. Ensuite, s'il est exact que le numéro de téléphone n'apparaît pas sur les captures d'écran transmises par le plaignant, la formation restreinte relève qu'il est fréquent et compréhensible que les personnes qui déposent une plainte auprès de la CNIL transmettent les captures d'écran des messages reçus sur leur téléphone, ce qui ne permet logiquement pas de faire apparaître le numéro de téléphone du destinataire du message. Elle observe également que les sollicitations figurant sur les captures d'écran communiquées par le plaignant font bien référence à des dates ultérieures à la prise en compte de la demande de droit d'opposition du plaignant, confirmée par le DPO, puisqu'elles mentionnent des offres valables entre le 11 décembre 2018 et le 11 juillet 2019. Ainsi, la formation restreinte relève qu'aucun élément ne justifie de douter de la bonne foi du plaignant. Enfin, la formation restreinte rappelle que le droit d'opposition est attaché à une personne et non à un numéro de téléphone. La formation restreinte considère, dès lors, que ces captures d'écran révèlent que le plaignant a continué à recevoir des sollicitations près d'un an après avoir manifesté son opposition auprès du DPO du [...], en juin 2018.

76. Enfin, la formation restreinte rappelle que les améliorations apportées par l'outil de ticketing sont sans incidence sur l'existence et la matérialité du manquement, tant au regard des dispositions qui découlent de l'article 12 du RGPD (absence de réponse de la société au plaignant) que de son article 21 (Monsieur […] ayant continué à recevoir de la

prospection commerciale près d'un an après avoir manifesté son opposition à l'utilisation de ses données pour cette finalité).

77. Dans ces conditions, la formation restreinte considère qu'en ne prenant pas en compte l'opposition du plaignant au traitement de ses données à caractère personnel à des fins de prospection dans les délais prévus, la société a méconnu ses obligations découlant des articles 12 et 21 du RGPD.

78. Elle relève néanmoins que, dans le cadre de la procédure de sanction, la société a justifié avoir pris des mesures pour se mettre en conformité avec les obligations découlant des articles 12 et 21 du RGPD.

79. En dernier lieu, s'agissant des saisines n° 17017795, de septembre 2017 et n° 19018125, d'octobre 2019, émanant de Monsieur […], celui-ci a expliqué qu'il a fait l'objet à plusieurs reprises de prospection par SMS et par courriers de la part de la société [...] portant sur la commercialisation d'offres, notamment celle relative au " Forfait [...] avec appels illimités […] ". Il indique avoir manifesté par courrier à plusieurs reprises, dès le mois de mars 2015, son opposition au traitement de ses données à caractère personnel à des fins de prospection commerciale et avoir pourtant continué à recevoir des sollicitations commerciales jusqu'en octobre 2019.

80. Par courriel du 21 septembre 2018, les services de la Commission ont rappelé à la société ses obligations en matière de prospection commerciale et lui a demandé de ne plus traiter les données du plaignant pour cette finalité commerciale. Par courriel du 3 octobre 2018, le DPO du [...] a répondu avoir pris en compte la demande et " supprimé les coordonnées de Monsieur […] ".

81. Le rapporteur observe qu'il ressort des éléments relevés lors du contrôle que, malgré les demandes formulées par le plaignant depuis 2015 et l'assertion du DPO du [...] en 2018 par laquelle il confirme " avoir supprimé les coordonnées de Monsieur […] ", son opposition au traitement de ses données à des fins de prospection n'a été prise en compte qu'à compter du 17 décembre 2019, soit plus de quatre ans après que la société a été destinataire de sa première demande.

82. En défense, la société indique qu'elle n'a jamais reçu de demande d'opposition du plaignant, à la différence de la société [...]. Elle considère qu'une demande d'opposition formée auprès de la société [...] n'est pas opposable à la société [...]. Elle indique toutefois qu'elle a pris en compte la volonté du plaignant lorsqu'il a " activé l'option anti démarchage sur son espace abonné ". Elle précise que cette opposition est effective depuis le 17 décembre 2019. La société précise ensuite que le courriel produit par le rapporteur, indiquant que le DPO du [...] confirme " avoir supprimé les coordonnées de Monsieur […] ", est une reconstitution d'un courriel et non l'original, ce qui ne constitue pas une preuve recevable, et elle relève par ailleurs que le courriel n'a pas été adressé aux bons interlocuteurs et qu'il n'incombait pas à la société [...] de prendre en compte la demande d'opposition du plaignant.

83. S'agissant d'abord de l'absence de réception de la demande d'opposition du plaignant par la société, la formation restreinte relève que le DPO du [...] – qui, par courriel du 3 octobre 2018, a indiqué à la CNIL " avoir supprimé les coordonnées de Monsieur […] " - est le DPO en charge des demandes relatives aux abonnés [...] et aux abonnés [...]. La formation restreinte considère qu'il lui incombait donc de traiter cette demande dans son ensemble ou de la répercuter, le cas échéant, auprès des services compétents afin qu'elle soit prise en compte.

84. En conséquence, l'argumentation de la société, selon laquelle il incombait à la seule société [...] de prendre en compte la demande du plaignant, ne peut être retenue. En effet, la demande du plaignant était une demande d'opposition générale à recevoir de la prospection commerciale par voie postale et par voie électronique (SMS et courriel) qui concernait aussi bien la société [...] que la société [...]. Dans son courrier du 5 mars 2015 adressé au service " Informatique et Libertés " de la société [...], le plaignant avait pris soin de préciser ses identifiants [...] et [...] et de formuler sa demande comme suit : " Conformément aux dispositions de l'article 38 alinéa 2 de la loi du 6 janvier 1978 modifiée, je vous demande de supprimer mes coordonnées de vos fichiers de contacts publicitaires, qu'ils soient par voie postale, téléphonique ou informatique. ".

85. S'agissant enfin de l'irrecevabilité du courriel du 3 octobre 2018 confirmant la réception et la prise en compte de la demande du plaignant par le DPO du [...], la formation restreinte observe que ce dernier ne figure pas dans sa forme originale dans l'outil métier de la CNIL (outil métier dans lequel sont enregistrés les éléments liés au traitement d'une plainte). Ce courriel était enregistré sous la forme d'une " communication ", qui est un onglet dans l'outil métier permettant à l'agent en charge de la plainte de ne pas enregistrer en tant que tel le courriel en pièce jointe du dossier mais d'indiquer manuellement qu'il a reçu un courriel de la société, en renseignant la date de réception, sélectionnant l'émetteur du message dans une liste de choix pré-définis et en copiant le contenu du message original. La formation restreinte considère, dès lors, que la manière dont ce courriel a été reproduit correspond bien à une procédure prévue dans l'outil métier de la CNIL et qu'elle peut le prendre en compte dans la mesure où l'ensemble des éléments pertinents y figurent, c'est-à-dire la date, le contenu du texte et l'identité de son auteur, et qu'ils présentent manifestement un lien direct avec l'objet de la plainte. Enfin, la formation restreinte relève que, si la société conteste la recevabilité de ce courriel, elle n'indique pas pour autant ne jamais avoir envoyé ce message.

86. Dès lors, la formation restreinte considère que l'argumentaire de la société n'est pas de nature à remettre en cause le fait que l'opposition du plaignant n'a été prise en compte qu'à compter du 17 décembre 2019, ce qui correspond selon la société à la date à laquelle le plaignant a activé " l'option anti démarchage sur son espace abonné ", ce qui est intervenu plus d'un an après l'indication par le DPO du [...], le 3 octobre 2018, de la prise en compte effective de cette demande, formulée initialement le 5 mars 2015.

87. Dans ces conditions, la formation restreinte considère qu'en ne prenant pas en compte l'opposition du plaignant au traitement de ses données à caractère personnel à des fins de prospection dans les délais prévus, la société a méconnu ses obligations découlant des articles 12 et 21 du RGPD.

88. Elle relève néanmoins que la société a justifié avoir pris des mesures pour se mettre en conformité avec les obligations découlant des articles 12 et 21 du RGPD.

89. Au vu de ce qui précède, la formation restreinte considère qu'un manquement aux obligations des articles 12 et 21 du RGPD est constitué pour les plaintes déposées par Madame […], Messieurs […] et […].

4. Sur le manquement relatif à l'obligation de protéger les données à caractère personnel dès la conception

90. Aux termes de l'article 25 du RGPD " 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée […] ".

91. Le rapporteur se fonde sur deux saisines de la CNIL en novembre 2019, émanant de Messieurs […] (plainte n° 19019626) et […] (plainte n° 19020342) et dans le cadre desquelles les plaignants faisaient état du fait qu'ils ne parvenaient pas à faire cesser l'envoi, par la société [...], de factures sur lesquelles apparaissait la mention d'une ligne mobile résiliée, pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant de l'article 25 du RGPD.

92. En défense, la société explique tout d'abord qu'elle adresse des factures à zéro euro à des clients après la résiliation de leur abonnement car ces derniers bénéficient d'un abonnement dit " multilignes ". La société précise que ce service permet à un abonné de rattacher à une ligne mobile principale, une ou plusieurs lignes secondaires, ce qui a pour conséquence de regrouper les factures des différentes lignes sur le compte principal associé à la ligne principale, et de procéder à un seul prélèvement correspondant à la somme des forfaits associés. La société fait ainsi valoir que " le traitement du numéro de téléphone correspondant à la ligne [mobile] principale résiliée est nécessaire, puisqu'il poursuit des finalités visant à permettre à [...] de poursuivre la bonne exécution de leur contrat en identifiant le débiteur des lignes multiples souscrites par ses abonnées et d'améliorer pour les abonnés, la lisibilité de la facturation de leurs abonnements et des prélèvements effectués sur leur compte ". Ensuite, la société précise néanmoins avoir initié une refonte de sa procédure de facturation de sorte que les factures des comptes multilignes associées à une ligne mobile principale résiliée comportent désormais la mention d'un identifiant permettant à l'abonné et à la société [...] de savoir, à des fins de facturation, qui est l'unique débiteur des lignes, sans continuer à mentionner la ligne principale résiliée sur la facture.

93. La formation restreinte relève qu'il ressort de l'article 25 du RGPD précité que les responsables de traitement doivent mettre en œuvre des mesures techniques et organisationnelles appropriées afin de respecter de façon effective les principes relatifs à la protection des données.

94. La formation restreinte considère que si l'information qu'une personne a été titulaire d'une ligne mobile résiliée peut effectivement être conservée à des fins d'exécution du contrat et à des fins comptables, ou encore pour la gestion du contentieux, il n'est en revanche pas nécessaire de continuer à traiter cette information dans le cadre de l'émission des facturations en cours, et de la faire apparaître sur ces dernières, alors que l'utilisation d'un identifiant permettant d'identifier le débiteur des différentes lignes mobiles (principales et secondaires) peut être utilisé à la place. La société aurait dû prévoir, dès la conception, des mesures organisationnelles et techniques pour ne plus traiter ces données dans ce cadre à la suite d'une demande de résiliation d'une ligne principale par la personne concernée.

95. Dans ces conditions, la formation restreinte considère que les faits précités constituent un manquement à l'article 25 du RGPD dès lors que la société n'a pas mis en œuvre les mesures organisationnelles et techniques permettant de procéder à l'effacement des données à caractère personnel qui n'étaient plus nécessaires pour les besoins de la facturation.

96. Elle relève néanmoins que, dans le cadre de la procédure de sanction, la société a justifié avoir effectué une refonte de sa procédure de facturation, de sorte que les factures comprennent désormais uniquement la mention des lignes actives,

sans mention des lignes résiliées. La formation restreinte considère dès lors que la société s'est mise en conformité avec les obligations découlant de l'article 25 du RGPD.

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

97. L'article 32 du RGPD prévoit que : " Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (…) " et, notamment, " des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement " et 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 ".

98. En premier lieu, le rapporteur se fonde sur deux saisines émanant de Mesdames […] (plainte n° 19012802 de juillet 2019) et […] (plainte n° 19019490 d'octobre 2019) et dans le cadre desquelles les plaignantes faisaient état de l'absence d'authentification systématique de l'utilisateur pour accéder à un compte utilisateur [...] (pour l'utilisateur disposant d'un téléphone équipé d'une carte SIM [...] ou pour une personne bénéficiant du partage de connexion d'un utilisateur doté d'un téléphone équipé d'une carte SIM [...]), pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant de l'article 32 du RGPD.

99. En défense, la société fait valoir que les contrôles de la CNIL n'ont pas porté sur ces plaintes et que l'accès à l'espace mobile d'un abonné depuis un autre appareil via un partage de connexion n'est pas possible.

100. Au vu des éléments apportés par la société, la formation restreinte estime qu'il n'y a pas lieu de retenir de manquement à l'article 32 du RGPD au titre de ces faits.

101. En second lieu, le rapporteur observe qu'il ressort des constats effectués dans le cadre de la procédure de contrôle que la société transmet par courriel, en clair, les mots de passe des utilisateurs lors de leur souscription à une offre auprès de la société [...].

102. En défense, la société fait d'abord valoir qu'en tant que responsable de traitement, elle est libre de choisir les mesures de sécurité à mettre en place et que les guides et les recommandations émises par la CNIL ou l'Agence nationale de la sécurité des systèmes d'information (ANSSI) n'ont pas de caractère impératif et n'ont pas valeur de loi. Dès lors, la société considère qu'aucun manquement ne peut être retenu en l'absence d'une " violation caractérisée de l'obligation de sécurité, matérialisé par la survenance d'une violation de données à caractère personnel ", ce qui n'est pas le cas en l'espèce d'après elle.

103. La société fait ensuite valoir qu'à l'époque des opérations de contrôle, les abonnés étaient incités à modifier leur mot de passe sur leur espace abonné et sensibilisés sur l'importance de garder ces mots de passe confidentiels. Elle indique en outre que le mot de passe initial attribué par la société [...] présente un niveau de robustesse élevé. Elle précise enfin que l'espace abonné permet uniquement d'accéder à des informations " basiques " et non à des informations sensibles.

104. Tout d'abord, la formation restreinte rappelle que, en application de l'article 32 du RGPD, pour assurer la protection des données à caractère personnel, il incombe au responsable de traitement de prendre des " mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ". La formation restreinte considère qu'en l'espèce, les modalités 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. En effet, la transmission, en clair, d'un mot de passe qui n'est ni temporaire, ni à usage unique et dont le renouvellement n'est pas imposé, le rend aisément et immédiatement utilisable par un tiers qui aurait un accès indu au message qui le contient. Ce tiers pourrait ainsi accéder à toutes les données à caractère personnel présentes dans le compte utilisateur [...] de la personne concernée (notamment les nom, prénom, numéro de ligne mobile, adresse postale, adresse électronique, relevé d'identité bancaire, numéro de ligne mobile). Il pourrait également accéder à sa messagerie vocale, télécharger ses factures et le relevé de ses consommations, procéder à la modification du mot de passe, de l'adresse électronique ou des options du compte. Le fait que le mot de passe soit en lui-même robuste et que les personnes soient incitées à modifier leur mot de passe ne suffit pas à compenser ces risques, qui peuvent notamment entraîner des usurpations d'identité et des tentatives d'hameçonnage. Dès lors, la prise en compte de ces risques pour la protection des données à caractère personnel et de la vie privée des personnes conduit la formation restreinte à considérer que les mesures déployées pour garantir la sécurité des données en l'espèce sont insuffisantes.

105. Ensuite, la formation restreinte précise que si la délibération n° 2017-012 du 19 janvier 2017 ayant pour objet d'apporter des recommandations relatives aux mots de passe, le guide de la CNIL relatif à la sécurité des données à caractère personnel et la note technique de l'ANSSI relative aux mots de passe cités dans les écrits du rapporteur n'ont certes pas de caractère impératif, ils exposent toutefois les précautions élémentaires de sécurité correspondant à l'état de l'art. Dès lors, la formation restreinte rappelle qu'elle retient un manquement aux obligations découlant de l'article 32 du

RGPD et non du non-respect des recommandations, qui constituent au demeurant un éclairage pertinent pour évaluer les risques et l'état de l'art en matière de sécurité des données à caractère personnel.

106. Outre ces recommandations, la formation restreinte souligne qu'elle a, à plusieurs reprises, adopté des sanctions pécuniaires où la caractérisation d'un manquement à l'article 32 du RGPD est le résultat de mesures insuffisantes pour garantir la sécurité des données traités, et non pas seulement le résultant de l'existence d'une violation de données à caractère personnel. Les délibérations n° SAN-2019-006 du 13 juin 2019 et n° SAN-2019-007 du 18 juillet 2019 visent notamment l'insuffisante robustesse des mots de passe ainsi que leur transmission aux clients de la société par courriel, en clair (lisible dans le corps du message), après la création du compte.

107. Dans ces conditions, eu égard aux risques encourus par les personnes rappelés ci-dessus, la formation restreinte considère que les faits précités constituent un manquement à l'article 32 du RGPD dès lors que la société transmet par courriel, en clair, les mots de passe des utilisateurs lors de leur souscription à une offre auprès de la société [...].

108. Elle relève néanmoins que, dans le cadre de la procédure de sanction, la société atteste de la mise en œuvre obligatoire du renouvellement des mots de passe des utilisateurs lors de leur première connexion. Le mot de passe demandé par la société est conforme aux préconisations de la CNIL contenues dans sa recommandation de 2017 relative aux mots de passe. En outre, la formation restreinte relève que la société s'engage à ne plus transmettre les mots de passe des nouveaux abonnés en clair par courriel mais, à compter de la fin mars 2022, à ce que ces derniers créent eux-mêmes leur mot de passe, qui devra être conforme aux préconisations de la CNIL en la matière.

III. Sur les mesures correctrices et leur publicité

109. 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. "

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

111. En premier lieu, sur le principe du prononcé d'une amende, la société soutient qu'une telle mesure n'est pas justifiée. En effet, s'agissant des manquements relatifs à l'exercice des droits d'accès et d'opposition, la société considère que les plaintes qui sous-tendent ces manquements présentent un caractère isolé et, qu'en tout état de cause, elle a répondu aux demandes d'accès et pris en compte les demandes d'opposition des plaignants. S'agissant du manquement à l'obligation de protéger les données dès la conception, la société considère que le traitement du numéro de téléphone correspondant à la ligne mobile principale résiliée est nécessaire aux besoins de la bonne exécution du service de téléphonie mobile. S'agissant du manquement relatif à la sécurité des données, la société considère qu'en l'absence d'une violation de données à caractère personnel, la transmission en clair des mots de passe des utilisateurs n'est pas une " violation caractérisée de l'obligation de sécurité ".

112. 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.

113. La formation restreinte considère d'abord que la société a fait preuve d'une négligence certaine s'agissant de principes fondamentaux du RGPD puisque quatre manquements sont constitués, 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. Elle souligne en outre, s'agissant du

manquement relatif à la sécurité des données, que la transmission par courriel, en clair, des mots de passe des utilisateurs lors de leur souscription à une offre auprès de la société [...], peut présenter un risque pour la vie privée des personnes concernées.

114. La formation restreinte relève ensuite que la société [...] est un acteur particulièrement important du secteur des télécommunications puisqu'elle dénombrait, en décembre 2020, environ […] abonnés aux offres de téléphonie mobile, […]. La formation restreinte observe également que la société, en sa qualité d'opérateur de téléphonie mobile, est au cœur de l'acheminement des flux de données à caractère personnel quotidiens de nombreuses personnes et doit dès lors faire preuve d'une particulière rigueur dans la gestion de la sécurité des données à caractère personnel concernées.

115. Enfin, la formation restreinte relève que les mesures de mise en conformité mises en place à la suite de la notification du rapport de sanction n'exonèrent pas la société de sa responsabilité pour les manquements constatés.

116. 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, 21, 25 et 32 du RGPD.

117. 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 constate que les plaintes ayant donné lieu à des manquements apparaissent extrêmement isolées et peu nombreuses - leur nombre, de sept, doit être rapporté au nombre d'abonnés, […] -, de sorte que ces manquements ne peuvent aucunement être regardés comme ayant un caractère systémique. La formation restreinte tient également compte de l'activité de la société et de sa situation financière.

118. Dès lors, au vu de ces éléments, la formation restreinte considère que le prononcé d'une amende de 300 000 euros apparaît justifié.

119. En troisième lieu, une injonction de mettre en conformité le traitement avec les dispositions des articles 12, 15, 21, 25 et 32 du RGPD a été proposée par le rapporteur lors de la notification du rapport.

120. 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.

121. 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 12, 15, 21, 25 et 32 du RGPD. Elle considère dès lors qu'il n'y a plus lieu de prononcer d'injonction.

122. En dernier lieu, s'agissant de la publicité de la sanction, la société soutient qu'une telle mesure serait disproportionnée au regard des manquements retenus et du faible nombre de plaintes visées. Elle considère également que cette peine de publicité complémentaire porterait un dommage irréversible à sa réputation.

123. La formation restreinte considère que la publicité de la sanction se justifie au regard de la pluralité des manquements relevés, de leur persistance, et du nombre de personnes concernées.

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, 21, 25 et 32 du RGPD ;
• 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.