Délibération SAN-2023-015 du 12 octobre 2023

Commission Nationale de l'Informatique et des Libertés
Nature de la délibération : Sanction
Etat juridique : En vigueur
Date de publication sur Légifrance : Jeudi 19 octobre 2023

Délibération de la formation restreinte n°SAN-2023-015 du 12 octobre 2023 concernant la société GROUPE CANAL +

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte com-posée de M. Alexandre LINDEN, président, M. Philippe-Pierre CABOURDIN, vice-président, Mme Christine MAUGÜÉ et MM. Alain DRU et 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 la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notam-ment 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 les saisines n° […] ;

Vu la décision n° 2021-017C du 21 janvier 2021 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par la société GROUPE CANAL + ou pour son compte, en tout lieu susceptible d'être concerné par leur mise en œuvre ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés por-tant désignation d'un rapporteur devant la formation restreinte, en date du 9 mars 2023 ;

Vu le rapport de Mme Valérie PEUGEOT, commissaire rapporteure, notifié à la société GROUPE CANAL + le 11 mai 2023 ;

Vu les observations écrites versées par la société GROUPE CANAL + le 12 juin 2023 ;

Vu les observations orales formulées lors de la séance de la formation restreinte du 14 septembre 2023 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte :

- Mme Valérie PEUGEOT, commissaire, entendue en son rapport ;

En qualité de représentants de la société GROUPE CANAL + :

- […].

La société GROUPE CANAL + ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. Fondée en 1998 en France, la société GROUPE CANAL + (ci-après la " société ") est spécialisée dans l'édition de chaînes et la distribution d'offres de télévision payante. En 2021, GROUPE CANAL + employait environ 3 223 employés en France et avait réalisé, pour l'année 2022, un chiffre d'affaires de 1 851 312 842 euros.

2. La société propose un service d'édition de chaînes premium et thématiques, dans la production et la distribution de films de cinéma et de séries télévisées. Elle édite également des chaînes gra-tuites sur la télévision numérique terrestre (TNT).

3. Entre les mois de novembre 2019 et janvier 2021, la Commission nationale de l'informatique et des libertés (ci-après " la CNIL " ou " la Commission ") a été saisie de 31 plaintes, portant no-tamment sur la prospection par voie téléphonique, la transmission de données bancaires et de l'exercice des droits. Cinq de ces plaintes ont été retenues dans le cadre de la présente procédure.

4. En application de la décision n° 2021-017C du 21 janvier 2021 de la présidente de la Commis-sion, une délégation de la CNIL a effectué plusieurs contrôles auprès de la société afin de vérifier le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après " la loi Informatique et Libertés " ou " loi du 6 janvier 1978 ") et du 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 (ci-après le " Règlement " ou " RGPD ").

5. Ainsi, le 26 janvier 2021, la délégation a procédé à une mission de contrôle en ligne des traite-ments mis en œuvre par la société ou pour son compte, sur le site web www.canalplus.com. Ce contrôle a donné lieu à un procès-verbal n° 2021-017/1, notifié le même jour à la société.

6. Le 25 février 2021, la délégation a envoyé un questionnaire à la société, auquel cette dernière a répondu le 26 mars 2021, portant sur son organisation, sur les traitements de données à caractère personnel qu'elle met en œuvre, sur sa qualification en tant que responsable de traitement, sur ses relations avec ses clients et partenaires et sur sa gestion des demandes d'exercice des droits.

7. D'avril 2021 à janvier 2022, la délégation de contrôle a adressé plusieurs demandes complémen-taires à la société, laquelle a répondu en fournissant les éléments sollicités.

8. Le 9 mars 2023, la présidente de la Commission a, sur le fondement de l'article 22 de la loi du 6 janvier 1978, désigné Mme Valérie PEUGEOT en qualité de rapporteure aux fins d'instruction de ces éléments.

9. Le 30 mars 2023, la rapporteure a adressé une demande complémentaire à laquelle la société a répondu le 6 avril 2023.

10. Le 11 mai 2023, à l'issue de son instruction, la rapporteure a fait notifier à la société un rapport détaillant les manquements aux articles 12, 13, 14, 15, 28, 32 et 33 du RGPD et à l'article L. 34-5 du code des postes et des communications électroniques (ci-après " le CPCE ") qu'elle estimait constitués en l'espèce.

11. Le 12 juin 2023, la société a produit des observations en réponse au rapport de la rapporteure.

12. Par courrier du 4 juillet 2023, la rapporteure a, en application de l'article 40, III, du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi Informatique et Libertés, informé la société que l'instruction était close.

13. Par courrier du 11 juillet 2023, la société a sollicité qu'un huis clos soit prononcé pour la séance de la formation restreinte. Cette demande a été rejetée par le président de la formation restreinte le 24 juillet 2023.

14. Par un courriel du 14 août 2023, la société a communiqué des observations complémentaires.

15. La rapporteure et la société ont présenté des observations orales lors de la séance de la formation restreinte du 14 septembre 2023.

16. […], expert en sécurité informatique de la société […], prestataire de la société GROUPE CANAL +, a été entendu sur le fondement de l'article 22, paragraphe 1, de la loi du 6 janvier 1978.

II. Motifs de la décision

A. Sur les griefs invoqués par la société en lien avec la procédure

17. La société affirme qu'elle a été conduite à produire des éléments de défense qui n'ont pas été sollicités durant l'instruction et qui portent pourtant sur des informations factuelles déterminantes permettant de vider de leur substance les motifs de certains griefs formulés par le rapporteur.

18. Elle considère en outre que les éléments à décharge produits par GROUPE CANAL + n'ont pas été pris en compte, le rapport se fondant sur des échantillons d'informations ou une perception très parcellaire des mesures de conformité prises par la société.

19. En premier lieu, la formation restreinte relève qu'au cours de la mission de contrôle, la société a pu répondre aux sollicitations des services de la CNIL, produire tout justificatif et faire part de ses observations. Chaque demande de complément d'information formulée ultérieurement par les services de la CNIL a été assortie d'un délai permettant à la société de rassembler les éléments qu'elle jugeait pertinents pour y répondre.

20. En second lieu, les dispositions de l'article 40 du décret n° 2019-536 du 29 mai 2019, qui prévoyant notamment que la personne physique ou morale à laquelle est notifié un rapport propo-sant une sanction dispose d'un délai d'un mois pour transmettre ses observations en réponse, ont été respectées.

21. Au regard de ces éléments, la formation restreinte estime que la procédure n'est pas entachée d'irrégularité.

B. Sur le manquement à l'obligation de recueillir le consentement des personnes con-cernées pour la mise en œuvre de prospection commerciale par voie électronique

22. 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 élec-troniques utilisant les coordonnées d'une personne physique […] qui n'a pas exprimé préalable-ment 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 in-formée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe. […] ".

23. L'article 4, paragraphe 11, du RGPD prévoit qu'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 ".

24. L'article 7, paragraphe 1, du RGPD dispose que " dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concer-née a donné son consentement au traitement de données à caractère personnel la concernant ".

25. 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 dispo-sitions de l'article 4, paragraphe 11, du RGPD, la rapporteure se fonde sur le fait que la société GROUPE CANAL +, qui fait réaliser des opérations de prospection commerciale électronique pour son compte par des prestataires, n'est pas en mesure de disposer et d'apporter la preuve d'un consentement valablement exprimé par les prospects pour être ainsi démarchés. En effet, les don-nées de ces prospects proviennent de fournisseurs […] (ci-après " […] "), en l'espèce […]. Or, la rapporteure note que ces prospects, en cochant la case prévue sur les formulaires de collecte pour donner leur consentement à recevoir de la prospection commerciale par voie électronique, n'ont pas valablement consenti à recevoir de la prospection de la part de la société GROUPE CANAL +, dans la mesure où ils n'ont pas été informés de l'identité de ce prospecteur pour le compte du-quel le consentement serait collecté, l'information n'étant pas disponible sur les formulaires de collecte ou via un lien URL cliquable.

26. En défense, la société soutient que la responsabilité pour le recueil du consentement licite des prospects concernés ne pèse pas sur elle mais sur les […] qui sont à l'origine de la collecte des données et avec lesquels elle a conclu des contrats répartissant les responsabilités de chaque par-tie. Elle ajoute que ces […] sont responsables du partage des données de leurs clients. Elle consi-dère d'ailleurs que le rapport ne précise pas la base légale qui fonderait sa propre obligation à re-cueillir ce consentement. La société affirme également que la règlementation applicable ne re-quiert pas l'information des personnes sur l'identité des destinataires de leurs données pour que le consentement soit considéré comme valablement recueilli. Elle conclut qu'au regard de ces élé-ments, le rapport méconnaît les principes de légalité des délits et des peines et le principe de res-ponsabilité personnelle.

27. En premier lieu, la formation restreinte rappelle que, en application des dispositions combinées des articles L. 34-5 du CPCE et 7, paragraphe 1, du RGPD, tel qu'éclairé par l'article 4, para-graphe 11, du RGPD, l'organisme – en l'espèce la société GROUPE CANAL + – qui fait réaliser des opérations de prospection commerciale par voie électronique à partir de données collectées par ses partenaires, doit disposer d'un consentement constituant une " manifestation de volonté, libre, spécifique, éclairée et univoque " des personnes concernées. Lorsque les données des pros-pects n'ont pas été collectées directement auprès d'eux par l'organisme qui prospecte, le consen-tement peut avoir été recueilli au moment de la collecte initiale des données par le primo-collectant, pour le compte de l'organisme qui réalisera les opérations de prospection ultérieures. À défaut, il revient à l'organisme qui prospecte de recueillir un tel consentement avant de procéder à des actes de prospection. En application des dispositions de l'article 7, paragraphe 1, du RGPD, le prospecteur doit alors être en mesure de prouver qu'il dispose de ce consentement. En outre, pour que le consentement soit éclairé, les personnes doivent notamment être clairement informées de l'identité du prospecteur pour le compte duquel le consentement est collecté et des finalités pour lesquelles les données seront utilisées. Pour ce faire, en cas de consentement recueilli par le primo-collectant pour le compte des prospecteurs, une liste exhaustive et mise à jour est tenue à la disposition des personnes au moment du recueil de leur consentement, par exemple directement sur le support de collecte ou, si celle-ci est trop longue, via un lien hypertexte renvoyant vers la-dite liste et les politiques de confidentialité des prestataires et fournisseurs (voir en ce sens, CNIL, FR, 24 novembre 2022, SANCTION, n° SAN-2022-021, publié).

28. En l'espèce, la formation restreinte note que 3 346 632 prospects dont les données ont été collectées auprès de […] et 588 324 auprès de […] ont fait l'objet de prospection par voie élec-tronique au cours de l'année 2021 par le prestataire intervenant pour le compte de la société GROUPE CANAL +. Pour l'ensemble de ces prospects, la société n'est pas en mesure de fournir de pièces démontrant l'obtention d'un consentement valablement recueilli auprès des personnes, que ce soit par ses soins – ce qu'elle a précisé ne pas faire – ou par les primo-collectants.

29. En effet, si la société a fourni à la délégation de contrôle des exemples de formulaires type de collecte de données des prospects mis à disposition par […], la formation restreinte relève qu'aucune liste de partenaires – incluant GROUPE CANAL + – devant être tenue à la disposi-tion des prospects au moment de consentir, n'a été communiquée dans le cadre de la procédure. Pour la société […], le formulaire de collecte prévoit une case à cocher avec la mention suivante : " accepter de recevoir des informations commerciales pour des services/produits […] et parte-naires ". Pour la société […], la mention précise : " accepter de recevoir des informations com-merciales de la part des sociétés du […] ou de leurs partenaires selon mes centres d'intérêt ou l'endroit où je me trouve ". Dans les deux cas, aucune information sur l'identité des partenaires concernés n'est disponible sur le formulaire de collecte ou via un lien hypertexte cliquable.

30. Ainsi, la société GROUPE CANAL + n'établit pas qu'elle dispose d'un consentement valable des personnes pour ses opérations de prospection commerciale par voie électronique. En effet, si tant est que les personnes aient bien donné leur consentement aux sociétés […] à recevoir de la prospection commerciale électronique en cochant les cases présentes à cet effet sur les formulaires en cause, elles n'ont pas valablement consenti à recevoir de la prospection de la part de la société GROUPE CANAL +, dans la mesure où elles n'ont pas été informées de l'identité de ce pros-pecteur pour le compte duquel le consentement serait collecté. Le consentement recueilli ne sau-rait être considéré comme étant éclairé, les personnes concernées n'étant pas informées de l'identité du prospecteur pour le compte duquel le consentement est collecté, à savoir la société GROUPE CANAL +. En l'absence de cette information, le consentement ne saurait être consi-déré comme valable.

31. En deuxième lieu, la société fait valoir le fait que les données des prospects ne lui seraient pas directement transmises, mais à des prestataires, et que la société ne serait ainsi pas destinataire des adresses de messagerie électronique des clients des […], qui ne se trouvent pas dans sa base de données. La formation restreinte considère que la circonstance selon laquelle la société fait appel à des prestataires pour mener les opérations de prospection est sans incidence sur le fait que, pour pouvoir se prévaloir d'un consentement valable recueilli par le primo-collectant, la so-ciété GROUPE CANAL + doit figurer dans la liste des partenaires auxquels les données sont transmises, dès lors que ces prestataires sous-traitants agissent pour son compte. La société est responsable de la prospection commerciale qu'elle met en œuvre, y compris lorsqu'elle est réalisée pour son compte par un sous-traitant.

32. En troisième lieu, la formation restreinte relève que, dans le cadre du contrôle sur pièces, la société a indiqué que les […] sont en charge de la collecte du consentement des personnes con-cernées. La société a précisé n'exercer aucun contrôle sur les formulaires de recueil de consente-ment utilisés, indiquant que " ces formulaires sont gérés uniquement par le […] concerné, en [leur] qualité de responsable de traitement. En conséquence, Groupe Canal+ n'est pas en charge de définir les modalités de collecte du consentement des abonnés des […] ".

33. La formation restreinte considère dès lors que les mesures mises en place par la société GROUPE CANAL + pour s'assurer auprès de ses partenaires que le consentement avait été valablement donné par les prospects avant de les démarcher étaient insuffisantes.

34. Dans ces conditions, la formation restreinte considère 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 dispo-sitions de l'articles 4, paragraphe 11, du RGPD.

C. Sur les manquements en lien avec l'obligation d'informer les personnes concer-nées du traitement de leurs données à caractère personnel

1) S'agissant de l'information fournie aux utilisateurs lors de la création d'un compte pour le service MyCanal

35. L'article 12, paragraphe 1, du RGPD prévoit que " le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour pro-céder 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 (…) ".

36. L'article 13, paragraphe 1, du RGPD impose au responsable de traitement de fournir à la per-sonne concernée différentes informations relatives notamment à son identité et ses coordonnées, aux finalités du traitement mis en œuvre, sa base juridique, les destinataires ou les catégories de destinataires des données et au fait que le responsable du traitement a l'intention d'effectuer un transfert de données vers un pays tiers.

37. L'article 13, paragraphe 2, du RGPD prévoit que, lorsque cela apparaît nécessaire pour garantir un traitement équitable et transparent des données, le responsable de traitement doit fournir à la personne " la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée " et l'information relative au " droit d'introduire une réclamation auprès d'une autorité de contrôle ".

38. Les lignes directrices sur la transparence au sens du règlement (UE) 2016/679, venant éclairer les dispositions précitées, précisent que : " la durée de conservation […] devrait être formulée de ma-nière à ce que la personne concernée puisse évaluer, selon la situation dans laquelle elle se trouve, quelle sera la période de conservation s'agissant de données spécifiques ou en cas de finalités spé-cifiques. Le responsable du traitement ne peut se contenter de déclarer de façon générale que les données à caractère personnel seront conservées aussi longtemps que la finalité légitime du trai-tement l'exige. Le cas échéant, différentes périodes de stockage devraient être mentionnées pour les différentes catégories de données à caractère personnel et/ou les différentes finalités de traite-ment, notamment les périodes à des fins archivistiques. "

39. En l'espèce, la rapporteure note que lors de la création d'un compte sur le service MyCanal, un lien situé sous le formulaire de collecte des données renvoie l'utilisateur vers une page intitulée " Données personnelles et confidentialité ". Elle considère que la politique de confidentialité de la société ne développe pas de manière suffisamment précise les durées de conservation des don-nées. Elle relève en effet que celle-ci se limite à indiquer que " vos données personnelles sont con-servées selon des durées déterminées au regard de nos finalités

et des obligations légales, fiscales et comptables nous incombant. Les données liées à votre abonnement font l'objet d'un archivage électronique pendant toute la durée de souscription à l'abonnement et pendant les durées légales de prescription ". En outre, la rapporteure observe que la possibilité d'introduire une réclamation auprès de la CNIL n'est pas mentionnée dans la politique de confidentialité.

40. La société fait valoir, d'une part, que si le RGPD impose bien d'informer les personnes concer-nées sur la durée de conservation de leurs données, ni le RGPD, ni les lignes directrices sur la transparence du G29 ne contiennent une indication quant au degré de granularité attendu pour la fourniture de cette information. Le choix opéré par la société permet d'être transparent sans alourdir, de manière excessive, sa politique de confidentialité.

41. Elle précise toutefois qu'elle a modifié, le 6 février 2023, sa politique de confidentialité pour fournir des informations plus précises et granulaires.

42. D'autre part, s'agissant de l'information relative à la possibilité d'introduire une réclamation auprès de la CNIL, la société reconnaît qu'elle ne figurait pas dans la politique de confidentialité au moment du contrôle mais qu'elle a été ajoutée lors de la refonte de celle-ci. Elle précise que l'information était en revanche fournie dans les conditions générales d'utilisation, disponibles depuis le site web, et dans les conditions générales d'abonnement fournies à chaque souscription d'un service.

43. En premier lieu, s'agissant de la durée de conservation des données, la formation restreinte relève que le document, daté du 3 décembre 2020, n'est pas assez précis en ce qu'il se limite à affirmer que la durée de conservation des données est liée à la poursuite de certaines finalités (respect d'obligation légales, comptables, fiscales) ou à la durée de l'abonnement, sans indiquer les durées précises applicables. Les durées de conservation sont énoncées de manière générique et ne sont pas suffisamment explicites, la formation restreinte relevant en outre que certains utilisa-teurs du service ne sont pas abonnés mais ont uniquement créé un espace personnel sur le site.

44. Or, la formation restreinte considère que cette information est importante pour garantir un " traitement équitable et transparent " puisqu'elle contribue à assurer pour les utilisateurs la maîtrise sur le traitement de leurs données.

45. Au vu de ce qui précède, la formation restreinte considère que l'information relative à la durée de conservation des données des utilisateurs n'est pas suffisamment détaillée, ce qui constitue un manquement à l'article 13 du RGPD.

46. La formation restreinte note toutefois que les durées de conservation indiquées dans la politique de confidentialité modifiée au 6 février 2023 sont conformes aux préconisations de la CNIL.

47. En second lieu, la formation restreinte relève qu'il n'est pas fait mention du droit d'introduire une réclamation auprès de la CNIL dans la politique de confidentialité de la société alors que cette information est expressément visée à l'article 13, paragraphe 2, d), du RGPD.

48. Cependant, elle constate que la compilation de plusieurs documents, accessibles depuis le site web, permet d'obtenir l'information, qui n'est dès lors pas manquante, quand bien même elle n'est pas aisément accessible. Ce dernier grief relevant toutefois de l'article 12 du RGPD n'a pas été soulevé par la rapporteure dans son rapport de sanction.

49. Dans ces conditions, la formation restreinte considère que le manquement à l'article 13 du RGPD, s'agissant de l'information relative à la possibilité d'introduire une réclamation auprès de la CNIL, n'est pas constitué.

50. Par ailleurs, la formation restreinte relève que la société a modifié sa politique de confidentialité, accessible depuis le formulaire de collecte, qui est désormais complète.

51. La formation restreinte relève qu'au cours de la procédure, la société a modifié sa politique de confidentialité pour y mentionner le droit d'introduire une réclamation auprès de la CNIL.

2) S'agissant des informations fournies aux prospects lors des appels de démarchage téléphonique

52. L'article 14 du RGPD précise les informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée. Cet article prévoit que les mêmes élé-ments d'information que ceux visés à l'article 13 du RGPD doivent être fournis à la personne concernée, ainsi que les catégories de données à caractère personnel collectées et, si cela est né-cessaire pour garantir un traitement équitable et transparent, d'autres éléments parmi lesquels la source d'où proviennent ces données.

53. L'article 14 du RGPD précise également que les informations doivent être communiquées à la personne concernée " dans un délai raisonnable après avoir obtenu les données à caractère per-sonnel, mais ne dépassant pas un mois, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées " ou " si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne ".

54. En l'espèce, la rapporteure relève que, dans le cadre du contrôle, la société a fourni à la déléga-tion de la CNIL un échantillon composé de soixante-dix enregistrements d'appels téléphoniques effectués par un sous-traitant dans le cadre de campagnes de prospection réalisées à partir de données obtenues par le biais de ses partenaires.

55. Elle relève que l'écoute de ces enregistrements a permis de constater que seize personnes démar-chées par téléphone pour le compte de la société n'ont pas bénéficié pas d'une information com-plète dispensée dans les conditions prévues par l'article 14 précité et, pour quatre autres per-sonnes, aucune information n'a été fournie.

56. En défense, la société indique que, s'agissant des seize appels pour lesquels les mentions seraient incomplètes, les informations sont complètes dans trois cas. Pour six appels, elle affirme que le téléconseiller n'a pas eu le temps de fournir ces informations car le prospect a raccroché trop vite. Pour un cas, l'appel concernait une personne déjà abonnée, qui avait donc déjà reçu, à plusieurs reprises, ces informations. Pour les six derniers cas, la société reconnaît que le prospect n'a pas eu toutes les informations requises, mais qu'elle met en place des procédures précises visant à s'assurer que ces situations ne se produisent pas.

57. S'agissant des quatre appels pour lesquels aucune information n'a été fournie, la société relève qu'il s'agit d'appels très courts, pour lesquels le téléconseiller n'a pas pu fournir ces informations.

58. La société indique, de manière générale, que ces cas ne représentent qu'une minorité au regard du nombre d'appels effectués.

59. La formation restreinte rappelle qu'il résulte de l'article 14 du RGPD que, lorsqu'un prospec-teur récupère un numéro de téléphone d'un tiers à des fins de prospection par voie téléphonique, il doit informer la personne prospectée du traitement de ces données pour cette finalité, au plus tard lors de l'appel téléphonique. Lorsqu'une information prévue par le RGPD est fournie dans le cadre d'échanges téléphoniques, il est admis que cette information puisse se limiter aux éléments les plus importants pour l'interlocuteur, afin de rester brève, à condition d'indiquer un moyen d'obtenir les informations complètes (exemples : touche à activer sur le téléphone, courriel reçu par l'interlocuteur, renvoi vers une page web) (voir en ce sens, CNIL, FR, 23 juin 2022, SANC-TION, n° SAN-2022-011, publié). L'information sur le traitement des données transmises par les […], notamment les coordonnées téléphoniques des personnes, à des fins de prospection télépho-nique, en application de l'article 14 du RGPD, et celle relative à l'enregistrement de la conversa-tion, en application de l'article 13 du RGPD, peuvent par ailleurs être fusionnées.

60. La formation restreinte note que la société a fourni à la délégation de contrôle de la CNIL un échantillon d'enregistrements d'appels effectués dans le cadre des campagnes de prospection et a précisé que les enregistrements étaient effectués de manière aléatoire. La société a également pré-cisé à la délégation que les personnes appelées sont en principe informées, en tout début de l'appel, de leur faculté discrétionnaire de s'opposer à l'enregistrement, conformément aux instruc-tions reçues par les " conseillers d'appels internes et externes ".Or, dans tous les cas visés par le rapport (information incomplète ou absence d'information), la formation restreinte relève que le téléconseiller avait entamé la discussion sur les offres proposées par GROUPE CANAL +. Ainsi, même si l'appel était bref, le téléconseiller avait initié une démarche de prospection.

61. La formation restreinte observe en outre que, dans certains cas, les personnes contactées à des fins de prospection n'ont bénéficié d'aucune information. Dans d'autres cas, certains points pré-vus à l'article 14 du RGPD – comme les finalités du traitement ou encore l'existence de diffé-rents droits – n'ont pas été portées à leur connaissance, et la société n'a pas mis en place de mo-dalité permettant aux personnes concernées d'obtenir une information plus complète relative au traitement de leurs données, par exemple via l'activation d'une touche sur le clavier téléphonique Or, la formation restreinte relève que tous les appels visés par la rapporteure durent au moins trente secondes, et que le téléconseiller aurait donc eu le temps de procéder, par exemple, à un renvoi vers la politique de confidentialité de GROUPE CANAL +.

62. Enfin, la formation restreinte considère que si les enregistrements communiqués à la CNIL ne révèlent pas l'existence d'un manquement structurel en matière d'information, il n'en demeure pas moins qu'elle a méconnu ses obligations dans le cadre des appels susmentionnés.

63. Dans ces conditions, la formation restreinte considère que le manquement à l'article 14 du RGPD est constitué.

D. Sur le manquement aux obligations relatives aux modalités d'exercice des droits des personnes

64. Aux termes de l'article 12, paragraphe 3, du RGPD, " 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 de-mande 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 ".

65. Aux termes de l'article 12, paragraphe 4, du RGPD, " 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 inac-tion et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel. "

66. La rapporteure, pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant de l'article 12 du RGPD, se fonde sur les saisines de trois plaignants, M. […] (saisine n° […]) et Mmes […] (saisine n° […]) et […] (saisine n° […]). Les deux premières font état de difficultés rencontrées pour l'effacement de leurs données à caractère personnel, la troisième concerne une demande d'opposition.

67. La rapporteure observe qu'il ressort des constats effectués lors de la procédure de contrôle que ces demandes ont été traitées par la société mais sans que les personnes concernées soient infor-mées des suites apportées à leur demande. Par ailleurs, s'agissant de la demande d'opposition, elle a été traitée par la société en dehors des délais prévus par le RGPD.

68. En défense, s'agissant des deux demandes d'effacement, la société indique que celles-ci concer-naient, à chaque fois, une demande de résiliation et une demande d'effacement. En raison d'une erreur de qualification de la demande, l'effacement a bien été traité mais la personne concernée n'en a pas été avisée. La société fait valoir qu'il s'agit de cas isolés et que la demande d'effacement a bien été traitée.

69. S'agissant de la demande d'opposition, la société considère que la demande initiale du plaignant n'a pas été identifiée comme telle par le service client. Mais dans le cadre du contrôle sur pièces, la société a pris connaissance de l'existence de la plainte et a contacté le plaignant. La demande a finalement été identifiée comme une demande d'opposition aux sollicitations commerciales, de-mande qui a été traitée le jour même.

70. La formation restreinte relève d'abord que les demandes formulées par les plaignants auprès de la société étaient claires, en ce qu'elles visaient une demande de " suppression " ou une demande d' " opposition " et qu'elles étaient adressées directement au délégué à la protection des données de la société.

71. Ensuite, la formation restreinte observe qu'en vertu de l'article 12, paragraphe 3, du RGPD, le responsable de traitement doit en principe fournir aux personnes concernées des informations sur les mesures prises à la suite d'une demande dans un délai maximal d'un mois. Or, au jour du con-trôle sur pièces, réalisé le 25 février 2021, soit largement plus d'un mois après les demandes ini-tiales – adressées respectivement les 30 octobre 2019 et 17 décembre 2020 –, la société n'avait pas informé les personnes concernées des suites données, ce qu'elle ne conteste pas.

72. Enfin, la formation restreinte considère que si les saisines reçues par la CNIL ne révèlent pas l'existence d'un manquement structurel en matière d'exercice des droits, comme le souligne la société, il n'en demeure pas moins que celle-ci a méconnu ses obligations dans le traitement des demandes qui lui ont été adressées.

73. Dans ces conditions, la formation restreinte considère que le manquement à l'article 12 du RGPD est constitué.

E. Sur le manquement en matière de droit d'accès des personnes concernées

74. 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 auxdites données à caractère personnel ainsi qu'à cer-taines informations, notamment " lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source ". Il est égale-ment prévu au paragraphe 3 du même article que " le responsable du traitement fournit une copie des données à caractère personnel faisant l'objet d'un traitement ".

75. La rapporteure, pour proposer à la formation de considérer que la société a méconnu ses obligations résultant de l'article 15 du RGPD, se fonde sur trois saisines de la CNIL, émanant de MM. […] (n° […]) et […] (n° […]) et Mme […] (n° […]), ces personnes faisant état de l'absence de réponse de la société à leurs demandes.

76. La société reconnaît une erreur ou un dysfonctionnement dans la qualification de l'objet de la demande s'agissant de la saisine n° […] et affirme n'avoir jamais reçu la demande relative à la saisine n° […].

77. En revanche, s'agissant de la saisine n° […], la société considère que la demande de la plaignante n'était pas précisément formulée comme une demande d'accès à ses données à caractère person-nel. Elle considère qu'il s'agissait d'une demande de la preuve d'un contrat de souscription, ce qui ne relève pas du RGPD.

78. La formation restreinte relève d'abord qu'il ressort des éléments du dossier que les demandes des plaignants ont bien toutes été reçues par la société.

79. Ensuite, elle considère que les demandes ont été formulées dans des termes suffisamment clairs. S'agissant de la saisine n° […], la plaignante demandait à la société de lui " transmettre les élé-ments dont vous disposez dans les plus brefs délais, ou à défaut d'annuler ce contrat en cours et également de procéder à la suppression des données personnes personnelles […] conformément aux dispositions de l'article 17.1 du Règlement général sur la protection des données person-nelles ". La plaignante exprimait ainsi explicitement le souhait d'obtenir la transmission des élé-ments dont la société disposait. Cela aurait dû amener la société à traiter la demande comme une demande d'accès puis d'effacement.

80. Enfin, la formation restreinte considère que si les saisines reçues par la CNIL ne révèlent pas l'existence d'un manquement structurel en matière d'exercice du droit d'accès, il n'en demeure pas moins que la société a méconnu ses obligations dans le traitement des demandes qui lui ont été adressées.

81. Dans ces conditions, la formation restreinte considère que le manquement à l'article 15 du RGPD est constitué.

F. Sur le manquement à l'obligation d'encadrer par un acte juridique formalisé les traitements effectués pour le compte d'un responsable de traitement

82. L'article 28, paragraphe 3, du Règlement prévoit que le traitement effectué par un sous-traitant pour le compte d'un responsable de traitement est régi par un contrat ou tout autre acte juridique formalisé qui définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel, les catégories de personnes concernées ainsi que les obligations et les droits du responsable de traitement. Ce contrat prévoit en outre les conditions dans les-quelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opé-rations de traitement.

83. La rapporteure a constaté que plusieurs contrats de sous-traitance relatifs à l'hébergement des données à caractère personnel, communiqués par la société, ne contenaient pas toutes les men-tions prévues par l'article susmentionné. Elle relève que des contrats avec […] ont été conclus avant l'entrée en vigueur du RGPD et n'ont pas depuis fait l'objet d'une mise à jour pour viser les mentions prévues à l'article 28, paragraphe 3, du Règlement.

84. En défense, la société affirme qu'elle a mis fin aux services d'hébergement fournis par […] à partir de 2016, soit avant l'entrée en vigueur du RGPD. Ce service ayant été transféré à un autre sous-traitant, le contrat n'a pas été mis à jour. S'agissant du contrat avec […], la société affirme que des avenants ont été signés jusqu'en 2022 et que ces avenants sont complétés par des con-trats relatifs au traitement des données à caractère personnel contenant l'ensemble des mentions prescrites par le RGPD. La relation contractuelle avec […] a pris fin le 27 juin 2023. S'agissant du contrat avec […], la société indique que le contrat contient plusieurs documents, dont un qui n'a pas été communiqué à la CNIL lors du contrôle sur pièces. La combinaison de ces documents ferait apparaître que les mentions prévues par le RGPD encadrent bel et bien la relation contrac-tuelle entre les deux acteurs. A la suite du rachat de […] par la société […], une nouvelle trame contractuelle incluant une annexe " Traitement des données " est par ailleurs en cours de discus-sion.

85. La formation restreinte constate que de nombreux éléments ont été communiqués par la société dans le cadre de la procédure de sanction, après la notification du rapport.

86. A la lumière de ces éléments, il apparaît que s'agissant du contrat régissant les relations avec […], celles-ci ont pris fin en 2016, avant l'entrée en application du RGPD, de sorte que le manquement n'est pas constitué

87. S'agissant ensuite des actes encadrant les relations avec la société […], au regard du contrat d'origine conclu avec […] qui a été communiqué en réponse au rapport de sanction, et qui com-plète celui communiqué par GROUPE CANAL + lors des contrôles, la formation restreinte re-lève que l'ensemble des mentions requises par l'article 28 du RGPD figurent bien dans les con-trats lorsque les deux documents sont lus conjointement. Le manquement n'est pas donc consti-tué pour l'encadrement de ces relations.

88. S'agissant enfin du contrat conclu avec […], les avenants au contrat n'ont pas été communiqués aux services de la CNIL dans le cadre de la procédure de contrôle, ce que reconnaît la société. Lors du contrôle sur pièces du 25 février 2021, la société a fourni à la délégation de la CNIL un contrat datant de 2019, conclu pour une durée d'une année, qui ne comportait pas l'ensemble des mentions requises au titre de l'article 28, paragraphe 3, du RGPD. Elle a par la suite fourni, en réponse au rapport de sanction, des avenants qui auraient été conclus à l'expiration de ce contrat, et qui auraient été renouvelés depuis. La formation restreinte relève que ces nouvelles pièces comportent bien à présent toutes les mentions nécessaires. Elle observe toutefois que ces docu-ments fournis ne sont pas signés et semblent être des versions de travail (certains comportent une mention surlignée en jaune indiquant " […] Cloud Service Agreement for INSERT DESCRIP-TION OT THE SYSTEM " et " contract number " sans le numéro de contrat). En outre, la seule date indiquée est une version " revised " du 4 mars 2022. Ces observations sur la forme des pièces fournies en défense ayant été soulevées, la formation restreinte considère, en tout état de cause, qu'il n'est pas nécessaire de déterminer si les avenants fournis constituent des justificatifs rece-vables dans la mesure où le manquement est bien constitué pour les faits passés, au regard des constatations effectuées par la délégation au moment du contrôle.

89. Dans ces conditions, la formation restreinte considère que le manquement à l'article 28, para-graphe 3, du RGPD est constitué pour les faits passés concernant le contrat régissant les relations avec […].

G. Sur le manquement à l'obligation de sécurité

90. L'article 32, paragraphe 1, 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 per-sonnes 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 " pro-cédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ".

91. La rapporteure considère que le stockage des mots de passe des collaborateurs de la société dans l'application […] sous une forme hachée au moyen de l'algorithme MD4 n'est pas conforme à l'état de l'art.

92. En défense, la société relève que l'insuffisance de mesures de sécurité visée dans le rapport de sanction n'est pas établie. Elle affirme que le rapport se fonde sur des réponses courtes apportées à des questions ciblées formulées lors du contrôle, qui n'avaient pas vocation à permettre à la CNIL d'être pleinement informée du niveau global de sécurité entourant les mots de passe traités par la société. Elle fait ainsi valoir d'autres mesures qui seraient mises en place par la société et qui permettraient d'assurer un niveau de sécurité approprié, comme par exemple une surveillance permanente de l'activité au sein du réseau informatique ou un nombre limité de comptes adminis-trateurs. Elle précise également qu'une politique de migration vers une nouvelle version de Win-dows Server l'a incitée à faire évoluer les algorithmes utilisés vers des versions plus robustes, avec une migration achevée en février 2023. Depuis, la chaîne d'algorithme […] est utilisée.

93. La société considère en outre que la rapporteure se fonde à tort sur la délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres se-crets partagés et abrogeant la délibération n° 2017-012 du 19 janvier 2017, qui n'a pas de carac-tère normatif, est postérieure au contrôle et admet la mise en œuvre de dispositifs supplétifs aux seuls mots de passe. Sa violation ne pourrait donc pas être passible de sanction.

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

95. 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. Ainsi, en matière d'authentification, il est nécessaire de veiller à ce qu'un mot de passe permettant de s'authentifier sur un système ne puisse pas être divulgué. La conservation des mots de passe de manière sécurisée constitue une précaution élémentaire en matière de protection des données à caractère personnel. Dès 2013, l'Agence nationale de sécurité des systèmes d'information (ANS-SI) alertait et rappelait les bonnes pratiques s'agissant de la conservation des mots de passe en indiquant qu'ils doivent " être stockés sous une forme

transformée par une fonction cryptogra-phique à sens unique (fonction de hachage) et lente à calculer telle que PBKDF2 " et que " la transformation des mots de passe doit faire intervenir un sel aléatoire pour empêcher une attaque par tables précalculées " (ANSSI, " Bulletin d'actualité CERTA-2013-ACT-046 ", 15 novembre 2013, https://www.cert.ssi.gouv.fr/actualite/CERTA-2013-ACT-046/). De même, dans sa délibé-ration n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe, la CNIL indiquait déjà qu'elle " recommande [que le mot de passe] soit transformé au moyen d'une fonction cryptographique non réversible et sûre (c'est-à-dire utilisant un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue), intégrant l'utilisation d'un sel ou d'une clé ". En effet, les fonctions de hachage non robustes présentent des vulnérabilités connues qui ne permettent pas de garantir l'intégrité et la confidentialité des mots de passe en cas d'attaque par force brute après compromission des serveurs qui les hébergent.

96. Or, la formation restreinte relève que l'algorithme MD4, utilisé par la société pour le stockage des mots de passe de collaborateurs au moment des contrôles, était déjà réputé obsolète et insuffi-samment robuste pour assurer la confidentialité des mots de passe à la date des constations faites par la délégation. En effet, la fonction de hachage MD4 fait l'objet d'une vulnérabilité connue depuis plusieurs années et immédiatement exploitable par des attaquants (présentant un risque de collision) (Voir en ce sens ANSSI, " Bulletin d'actualité CERTFR-2014-ACT-028 ", 11 juillet 2014, https://www.cert.ssi.gouv.fr/actualite/CERTFR-2014-ACT-028/). Si la société a fait valoir que les positions prises par l'ANSSI dans des documents de 2014 ont été depuis remplacés par d'autres documents plus récents, il n'en demeure pas moins qu'une fonction de hachage qui n'était plus à l'état de l'art en 2014 ne l'était pas davantage au jour des contrôles. L'utilisation de l'algorithme MD4 suppose en effet d'avoir recours au protocole NTLM pour l'authentification, alors que ce protocole était déjà critiqué par l'ANSSI au moment des contrôles (Voir en ce sens ANSSI, " Recommandations pour la protection des systèmes d'information essentiels ", 18 dé-cembre 2020, https://www.ssi.gouv.fr/uploads/2020/12/guide_protection_des_systemes_essentiels.pdf). L'utilisation de cette fonction de hachage ne permet donc pas de garantir la sécurité des données à caractère personnel concernées. La formation restreinte considère, par ailleurs, que la robustesse des mesures de sécurité périphériques ne suffit pas à compenser l'utilisation de l'algorithme MD4. En effet, la fragilité inhérente à la fonction de hachage utilisée, sur laquelle se fonde la sécurité du stockage des mots de passe des employés de la société, est telle qu'elle ne peut pas être recti-fiée par d'autres mesures.

97. Dans ces conditions, la formation restreinte considère que le manquement à l'article 32 du RGPD est constitué.

98. La formation restreinte prend note que, depuis février 2023, la société utilise une nouvelle version de Windows Server qui a recours à un algorithme conforme à l'état de l'art.

H. Sur le manquement à l'obligation de notifier à la CNIL une violation de données à caractère personnel

99. L'article 4.12 du RGPD définit la violation de données à caractère personnel comme " une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ".

100. L'article 33 du RGPD dispose qu'" en cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du re-tard (…) Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu ".

101. Le considérant 87 du RGPD précise qu'" il convient de vérifier si toutes les mesures de protection techniques et organisationnelles appropriées ont été mises en œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et la personne concernée ".

102. Dans les lignes directrices sur la notification de violations de données à caractère personnel du 6 février 2018, le Comité européen de la protection des données (CEPD) considère, à titre d'illustration, " qu'un responsable du traitement devrait être considéré comme ayant pris " con-naissance " [de la violation de données à caractère personnel] lorsqu'il est raisonnablement cer-tain qu'un incident de sécurité s'est produit et que cet incident a compromis des données à carac-tère personnel. Le RGPD exige du responsable du traitement qu'il mette en œuvre toutes les me-sures de protection techniques et organisationnelles appropriées pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et les personnes concernées (…). Le responsable du traitement se voit ainsi tenu de prendre les mesures nécessaires pour s'assurer de prendre " connaissance " de toute vio-lation dans les meilleurs délais afin de pouvoir réagir de façon appropriée ".

103. Le CEPD fournit l'exemple suivant : " un tiers informe un responsable du traitement qu'il a accidentellement reçu les données à caractère personnel de l'un de ses clients et fournit la preuve de cette divulgation non autorisée. Dès lors que le responsable du traitement a reçu des preuves claires attestant d'une violation de la confidentialité, il ne fait aucun doute qu'il en a pris ''con-naissance'' ".

104. La rapporteure constate que la société a été informée par des abonnés, le 5 février 2020, d'une violation de données. A la suite d'une mise à jour de l'espace client CANAL +, des abonnés ac-cédant à leur compte ont pu visualiser les informations relatives à d'autres abonnés. Malgré le nombre de personnes concernées et le type de données rendues accessibles, la rapporteure relève que la société n'a pas procédé à une notification de cette violation de données à la CNIL. La rap-porteure considère qu'en ne procédant pas à cette notification, la société a méconnu les disposi-tions de l'article 33 du RGPD.

105. En défense, la société indique qu'elle aurait suivi les lignes directrices du CEPD et les recom-mandations de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour conclure qu'elle n'avait pas à notifier la violation. Sur le fondement de ces textes, elle considère qu'au regard du caractère peu sensible des données concernées et du nombre peu élevé de personnes potentiellement impactées, elle n'était pas tenue de procéder à une notification. Elle fait notamment valoir que la perte temporaire de confidentialité, qui a per-mis à sept personnes de visualiser les données d'autres clients, n'a duré que 5 heures 35 minutes. Elle ajoute que les données concernées ne sont pas sensibles et que les personnes ayant pu les visualiser sont d'autres abonnés, sans intention malveillante et sans expertise particulière leur permettant d'extraire les données accessibles. Elle précise également que le nombre précis de per-sonnes ayant pu avoir accès aux données de 10 154 abonnés est inconnu. Il serait toutefois limité à 777 personnes maximum, qui se trouvaient, selon la société, en capacité technique d'y avoir accès.

106. La formation restreinte relève tout d'abord que le nombre de personnes concernées par la violation, de 10 154, n'est pas négligeable. Elle note que plusieurs personnes ont indiqué à la so-ciété avoir eu effectivement accès aux données de tiers. La formation restreinte relève ensuite que les données à caractère personnel rendues accessibles par la violation étaient de nature à pouvoir porter atteinte au droit au respect de la vie privée des abonnés dès lors que leur adresse postale et leur numéro de téléphone avaient été divulgués. Par suite, la société aurait dû procéder à la notifi-cation de violation de données à caractère personnel à la CNIL.

107. Dans ces conditions, la formation restreinte considère que le manquement à l'article 33 du RGPD est constitué.

III. Sur le prononcé de mesures correctrices et la publicité

108. L'article 20 de la loi n° 78-17 du 6 janvier 1978 modifiée prévoit que : " lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut […] saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […] 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 an-nuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypo-thèses 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 for-mation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83 ".

109. L'article 83 du RGPD, tel que visé par l'article 20, paragraphe III, de la loi Informatique et Libertés, prévoit quant à lui que : " Chaque autorité de contrôle veille à ce que les amendes admi-nistratives 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.

110. En premier lieu, sur le principe du prononcé d'une sanction, la société indique qu'outre le fait qu'elle conteste les manquements reprochés par la rapporteure ou les justifie, elle a d'ores et déjà pris des mesures pour remédier à certains des faits reprochés et assurer sa conformité à la législa-tion applicable. Elle ajoute que certains des griefs qui lui sont faits par la rapporteure le sont au regard de recommandations et d'un référentiel de la CNIL qui n'ont pas de valeur impérative, et qui sont en outre postérieurs aux faits en cause. Elle souligne en outre que plusieurs des man-quements allégués ne sont pas substantiels en l'espèce et qu'ils ont représenté un impact limité voire inexistant sur les droits et libertés des personnes concernées. Elle insiste enfin sur la bonne volonté et les efforts dont elle a fait preuve tout au long de la procédure. La société considère que les facteurs d'atténuation prévus par l'article 83, paragraphe 2, du RGPD devraient amener la formation restreinte à ne pas prononcer de sanction financière, ou à tout le moins, à réduire très significativement le montant de l'amende proposée par la rapporteure.

111. 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 du-rée 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 caté-gories de données à caractère personnel concernées par la violation.

112. La formation restreinte souligne que les manquements commis par la société portent, pour certains, sur des obligations touchant aux principes fondamentaux de la protection des données à caractère personnel et que de nombreux manquements sont constitués. Elle note que certains de ces manquements sont structurels et d'une gravité certaine, d'autres présentent une gravité moindre.

113. Ainsi, s'agissant plus particulièrement du recueil du consentement à des fins de prospection par voie électronique, la formation restreinte rappelle que la société traite un nombre important de données à des fins de prospection commerciale. Il ressort en effet des éléments communiqués par la société que 3 934 956 prospects ont été démarchés par voie électronique en 2021.

114. La formation restreinte prend en considération, à titre de facteurs d'atténuation, les mesures prises par la société, qui s'est mise en conformité sur certains points, ainsi que la faible gravité de certains manquements, notamment le fait que les appels de démarchage pour lesquels le manque-ment relatif à l'information est retenu ne concernent qu'une petite partie des personnes démar-chées. La formation restreinte note en outre, au regard des saisines versées aux débats, que les manquements aux droits des personnes ne sont pas structurels et résultent principalement d'erreurs humaines. Elle relève enfin le caractère isolé du contrat pour lequel les justificatifs ne permettent pas de conclure à une conformité aux exigences du RGPD.

115. Au vu de l'ensemble de ces éléments, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative pour les manquements aux articles 7, paragraphe 1, 12, 13, 14, 15, 28, 32 et 33 du RGPD et à l'article L. 34-5 du CPCE.

116. En second lieu, la formation restreinte rappelle que les violations du RGPD relevées en l'espèce comportent des manquements à des principes susceptibles de faire l'objet, en vertu de l'article 83 du RGPD, d'une amende administrative pouvant s'élever jusqu'à 20 000 000 euros ou jusqu'à 4 % du chiffre d'affaires annuel mondial de l'exercice précédent, le montant le plus élevé étant retenu.

117. Elle rappelle également que les amendes administratives doivent être à la fois dissuasives et proportionnées. Elle considère en particulier que l'activité de la société et sa situation financière doivent notamment être prises en compte pour la détermination du montant de l'amende adminis-trative. Elle relève à cet égard que la société GROUPE CANAL + a réalisé un chiffre d'affaires de 1 851 312 842 euros en 2022.

118. Dès lors, au regard de la responsabilité de la société, de ses capacités financières et des critères pertinents de l'article 83, paragraphe 2, du RGPD évoqués ci-avant, la formation restreinte estime qu'une amende de 600 000 euros apparaît justifiée.

119. En troisième lieu, s'agissant de la publicité de la sanction, la société demande à la formation restreinte de ne pas rendre publique sa décision.

120. La formation restreinte considère au contraire que la publicité de la présente décision se justifie au regard de la gravité de certains des manquements en cause, de la portée du traitement et du nombre de personnes concernées.

121. Elle relève également que cette mesure permettra d'informer les personnes concernées par les opérations de prospection de la société. Cette information leur permettra, le cas échéant, de faire valoir leurs droits auprès de la société.

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

PAR CES MOTIFS

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

• prononcer une amende administrative à l'encontre de la société GROUPE CANAL + d'un montant de six cent mille euros (600 000 €) pour manquements aux articles 7, paragraphe 1, 12, 13, 14, 15, 28, 32 et 33 du RGPD et à l'article L. 34-5 du code des postes et des communications électroniques ;

• rendre publique, sur le site web de la CNIL et sur le site web de Légifrance, sa délibération, qui ne permettra plus d'identifier nommément la société à l'issue d'une durée 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.