Délibération SAN-2025-002 du 15 mai 2025

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Date de publication sur Légifrance : Mardi 27 mai 2025
Etat juridique : En vigueur

Délibération de la formation restreinte n°SAN-2025-002 du 15 mai 2025 concernant la société CALOGA

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Philippe-Pierre CABOURDIN, président, Mmes Laurence FRANCESCHINI et Isabelle LATOURNARIE-WILLEMS, M. Bertrand du MARAIS et M. Didier KLING, membres ;

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

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

Vu le code des postes et des communications électroniques ;

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° 2022-052C du 25 mars 2022 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 liés à la mise en œuvre par la société CALOGA auprès de tout organisme 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 du 22 avril 2024 portant désignation d'un rapporteur devant la formation restreinte ;

Vu le rapport de Mme Aminata NIAKATÉ, commissaire rapporteure, signifié à la société CALOGA le 21 juin 2024 ;

Vu les observations écrites versées par la société CALOGA le 22 juillet 2024 ;

Vu la réponse de la rapporteure à ces observations, signifiée à la société le 22 août 2024 ;

Vu les nouvelles observations écrites versées par la société CALOGA le 30 septembre 2024 ;

Vu la clôture de l'instruction, signifiée à la société le 3 décembre 2024 ;

Vu les observations orales formulées lors de la séance de la formation restreinte du 13 mars 2025 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 13 mars 2025 :

- Mme Aminata NIAKATÉ, commissaire, entendue en son rapport ;

En qualité de représentants de la société CALOGA :

- […]

Le président ayant vérifié l'identité des représentants du mis en cause, présenté le déroulé de la séance et rappelé que les mis en cause peuvent, s'ils le souhaitent, présenter des observations orales introductives ou en réponse aux questions des membres de la formation restreinte ;

La société CALOGA ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. FAITS ET PROCÉDURE

1. La société CALOGA (ci-après la société) est une société par action simplifiée sise 75 rue Guy Moquet à Malakoff (92240). Créée en 2000, la société CALOGA poursuit deux activités : elle réalise des opérations de prospection commerciale par voie électronique pour le compte d'annonceurs auprès des prospects de ses bases de données, constituées auprès de partenaires primo-collectants qui organisent notamment des jeux-concours. Elle intervient également comme courtier en données (data broker), en transmettant des données, collectées par des partenaires primo-collectants, à des partenaires qui vont faire de la prospection commerciale pour leurs propres annonceurs.

2. En 2021, la société CALOGA comptait neuf salariés. Elle a réalisé, pour la même année, un chiffre d'affaires de […] euros pour un résultat net de […] euros. La société a ensuite progressivement cessé ses activités. En 2022, son chiffre d'affaires s'élevait à […] euros pour un résultat net de […] euros. En 2023, son chiffre d'affaires s'élevait à […] euros pour un résultat net déficitaire de […] euros.

3. En application de la décision n° 2022-052C du 25 mars 2022 de la Présidente de la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission), un contrôle a été réalisé les 11 et 12 mai 2022 dans les locaux de la société. Cette mission avait pour but de vérifier la conformité des traitements mis en œuvre par la société avec les dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après la loi Informatique et Libertés ou loi du 6 janvier 1978 modifiée) et des autres dispositions relatives à la protection des données personnelles prévues par les textes législatifs et réglementaires, le droit de l'Union européenne et les engagements internationaux de la France.

4. Des procès-verbaux n° 2022-052/1 et n° 2022-052/2 des 11 et 12 mai 2022, ont été notifiés à la société à l'issue des journées de contrôle sur place. Plusieurs échanges entre la société et la délégation ont eu lieu entre mai 2022 et mai 2023.

5. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 22 avril 2024, désigné Mme Aminata NIAKATÉ en qualité de rapporteure sur le fondement de l'article 22 de la loi du 6 janvier 1978 modifiée.

6. Le 21 juin 2024, à l'issue de son instruction, la rapporteure a fait signifier à la société un rapport détaillant les manquements aux articles 5, paragraphe 1, e), 6 et 32 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le Règlement ou le RGPD) et L. 34-5 du Code des postes et des communications électroniques (ci-après CPCE) qu'elle estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de prononcer à l'encontre de la société 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.

7. Plusieurs échanges d'écriture ont par la suite eu lieu entre la rapporteure et la société, jusqu'à la clôture de l'instruction signifiée à la société le 3 décembre 2024.

8. A l'issue de la procédure contradictoire écrite, la rapporteure et la société ont présenté des observations orales lors de la séance de la formation restreinte.

II. MOTIFS DE LA DECISION

A. Sur les traitements en cause et la responsabilité de la société CALOGA

9. Aux termes de l'article 4, point 2, du RGPD, le traitement de données à caractère personnel s'entend comme toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction . L'article 4, point 7 du RGDP définit le responsable de traitement comme 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 .

10. La formation restreinte relève que, dans l'écosystème de la prospection commerciale, la qualité à conférer aux différents acteurs de la chaîne en matière de responsabilité de traitement – à savoir à l'annonceur pour le compte duquel la prospection électronique est adressée et à l'intermédiaire intervenant entre lui et le primo-collectant, qui peut notamment être chargé de l'envoi des messages de prospection électronique pour l'annonceur – dépend d'un certain nombre de paramètres (comme par exemple la propriété de la base de données, ses modalités de constitution et de gestion, les choix opérés en matière de segmentation ou encore le degré et la précision des instructions données par l'annonceur). Ces attribution et répartition des responsabilités entre les différents acteurs peuvent varier en fonction des rôles et des actions menées par chacun, selon les cas d'espèce, et elles doivent par conséquent faire l'objet d'une analyse au cas par cas. La qualification retenue par les acteurs eux-mêmes, notamment dans leurs actes contractuels, constitue un élément important à prendre en compte, mais non déterminant s'il ne correspond pas à la réalité des critères de l'article 4 du RGPD. En fonction des cas de figure, peuvent être qualifiés de responsables de traitement l'annonceur, c'est-à-dire l'entité souhaitant promouvoir ses produits ou services (v. CNIL, FR, 3 août 2022, n° SAN-2022-017, publié ; CNIL, 24 novembre 2022, n° SAN-2022-021, publié ; CNIL, FR, 12 octobre 2023, n° SAN-2023-015, publié ; CE, 23 mars 2015, GROUPE DSE, n° 357556, Rec.) ou encore certains prestataires spécialisés offrant des services publicitaires et produits de marketing (v. CE, 11 mars 2015, TUTO4PC, n° 368624, T ; CNIL, FR, 7 décembre 2020, SAN-2020-016, publié). Parmi ces prestataires figurent des sociétés constituant des bases de données de contact à partir de diverses sources tierces (appelées primo-collectants), qu'elles revendent à des partenaires ou utilisent pour proposer des prestations de prospection commerciale à des annonceurs. Ces acteurs peuvent, selon les configurations, être sous-traitants de l'annonceur ou responsables de traitement des opérations de prospection, sans exclure une possible coresponsabilité entre l'annonceur et son prestataire.

11. En matière de prospection commerciale, la formation restreinte a par exemple retenu la qualité de responsable de traitement d'un organisme ayant pour activité la constitution d'une base de données de contacts destinés à la prospection commerciale par voie électronique ainsi que l'envoi de courriers électroniques de prospection au bénéfice d'annonceurs, sur la base des éléments suivants : en premier lieu, s'agissant de la détermination des finalités, la formation restreinte relève que […] la société est propriétaire de la base de données utilisée dans le cadre des campagnes de prospection, les annonceurs et agences web ne fournissant pas les données à caractère personnel des prospects à contacter et n'ayant pas accès aux données à caractère personnel des prospects. En second lieu, la formation restreinte considère que la société détermine les moyens essentiels du traitement en ce qu'elle définit les données personnelles qui figurent dans sa base de prospects, les durées pendant lesquelles ces données y sont conservées et les éventuelles mises à jour devant être opérées. En conséquence, et sans qu'en l'espèce il soit nécessaire de se prononcer sur une éventuelle responsabilité conjointe des partenaires annonceurs de la société […], la formation restreinte retient que cette dernière a défini les finalités et les moyens du traitement lié à la gestion et la mise à disposition de sa base de données personnelles à des fins de prospection commerciale par courrier électronique (CNIL, FR, 7 décembre 2020, SAN-2020-016, publié).

12. La rapporteure considère d'abord que la société CALOGA intervient en qualité de responsable du traitement pour les activités de prospection commerciale par voie électronique effectuées à partir des données contenues dans ses bases pour le compte de ses clients annonceurs. Ensuite, s'agissant de la transmission de données de prospects à ses partenaires afin qu'ils réalisent des opérations de prospection commerciale par voie électronique pour le compte d'annonceurs, la rapporteure considère que la société CALOGA intervient en qualité de responsable de traitement conjoint avec les partenaires destinataires des données.

13. La société confirme sa qualité de responsable du traitement pour la gestion de la base et les opérations de prospection commerciale par voie électronique effectuées pour le compte d'annonceurs. S'agissant des opérations de transmission de données de prospects, la société considère, contrairement au rapporteur, que ses partenaires ont la qualité de sous-traitant, et que l'exigence d'un consentement valable des prospects pour la transmission de leurs données ne saurait lui être opposé dans ce cadre, les données étant transmises à des sous-traitants. La base légale de ce traitement serait, selon la société, l'intérêt légitime. Elle indique avoir procédé à une analyse personnelle de la qualité des différents intervenants et qu'il ne peut pas lui être reproché d'avoir abouti à une conclusion différente de celle de la CNIL.

14. S'agissant de la constitution des bases de données de la société CALOGA, la formation restreinte relève que la société CALOGA achète ses données, collectées via des jeux concours ou des tests de produits, à des partenaires commerciaux (les primo-collectants) pour constituer ses bases de données prospects dont elle est propriétaire. A ce titre, il est prévu, notamment dans le contrat conclu avec la société […], fournisseur de données, que la société CALOGA devient elle-même un responsable du traitement dès lors qu'elle utilise les données à caractère personnel des internautes ayant accepté de rejoindre sa base pour mettre en œuvre des traitements dont elle a défini les finalités et les moyens . Les données collectées dans ce cadre sont les nom, prénom, civilité, adresse électronique, code postal, date de naissance et, de façon épisodique, l'adresse postale. Elle relève également que la société met en œuvre ce traitement de prospection commerciale en démarchant les prospects présents dans ses quatre bases de données (CALOGA, ZEPLAN, BASYLO ou VOZEKO) et en choisissant elle-même les segments qui seront démarchés.

15. Il apparaît ainsi que la société est responsable du traitement portant sur la constitution de ses quatre bases de données de contacts.

16. S'agissant de la réalisation d'opérations de prospection commerciale au bénéfice des clients annonceurs, la formation restreinte note que la société CALOGA offre un service d'envoi de courriels de prospection à la demande d'agences ou de plateformes d'affiliation qui fournissent à la société CALOGA des kits de prospection pour le compte d'annonceurs finaux.

17. Il ressort des éléments du dossier qu'en pratique, ces opérations de prospection commerciale par voie électronique sont réalisées à partir de données issues d'une des bases de données de la société CALOGA, déterminée en fonction de la volumétrie souhaitée, que la société a elle-même constituées à partir de données de prospects transmis par ses partenaires primo-collectants. En pareille hypothèse, les clients de la société CALOGA, non seulement ne fournissent pas les données utilisées, mais n'y ont en outre pas accès.

18. Il apparaît ainsi que, s'agissant des opérations de prospection commerciale pour le compte d'annonceurs, la société agit au moins en partie comme responsable de traitement lorsque ces opérations sont réalisées à partir de ses bases de données. A cet égard, il convient de souligner que la société a confirmé sa qualité de responsable de traitement, d'abord dans le cadre du contrôle sur place effectué en mai 2022, puis dans le cadre de ses observations avec la rapporteure. Par ailleurs, et sans qu'il soit nécessaire en l'espèce de se prononcer sur l'éventuelle responsabilité conjointe de ses clients, la formation restreinte observe que cette responsabilité de CALOGA n'exclut pas celle des annonceurs, agissant comme responsables conjoints du traitement. Il est également possible que dans certains cas la société CALOGA agisse comme sous-traitant de ses clients, mais ces hypothèses ne sont pas en cause en l'espèce.

19. Au vu de l'ensemble de ce qui précède, la formation restreinte entend préciser que la présente décision concerne les traitements pour lesquels la société CALOGA est, et se reconnait, responsable de traitement, et qui portent sur la réalisation d'opérations de prospection électronique à partir de ses bases au bénéfice de clients annonceurs.

20. S'agissant de la transmission des données de prospects à des fins de prospection commerciale par voie électronique, la formation restreinte relève que la société transmet régulièrement (une fois par mois) les données de prospects actifs présents au sein de ses bases de données, qu'elle a constituées, à des partenaires, principalement les sociétés […], afin qu'ils réalisent à leur tour des opérations de prospection commerciale par voie électronique pour le compte de leurs propres clients annonceurs. Cette transmission est réalisée par la livraison, au partenaire, d'une ou plusieurs bases de données de la société CALOGA, le partenaire ayant le choix de la base ou des bases de données qu'il veut recevoir. Cette livraison est effectuée par le téléchargement d'un fichier sécurisé qui annule et remplace le précédent. Les sociétés à qui les données sont transmises, telles […] ou […], effectuent ensuite de nouvelles opérations de prospection commerciale, notamment par voie électronique, pour le compte de leurs clients annonceurs à partir des bases dont ils ont ciblé avec leurs propres outils les segments qu'ils souhaitent solliciter. Ces opérations constituent de nouveaux traitements de données à caractère personnel, mis en œuvre par d'autres responsables de traitement que la société CALOGA.

21. Dans ces conditions, la formation restreinte considère que la société doit être regardée comme responsable de traitement, tant pour les opérations de prospection commerciale par voie électronique réalisées au bénéfice de ses clients à partir de sa base de données - nonobstant l'éventuelle responsabilité conjointe desdits clients et à l'exclusion de cas où elle n'agirait qu'en qualité de sous-traitant - que pour la transmission de données de prospects à des partenaires, afin qu'ils réalisent eux-mêmes de la prospection commerciale par voie électronique.

B. Sur la régularité de la procédure menée à l'encontre de la société

22. La société affirme qu'il ne saurait lui être reproché l'absence de vérifications s'agissant de la conformité du recueil du consentement sur le fondement d'exigences qui n'existaient pas au moment des contrôles. Une telle pratique porterait manifestement atteinte aux principes de la légalité des délits et des peines et de non-rétroactivité.

23. La formation restreinte entend préciser que le cadre juridique applicable sera examiné, au sein de la présente délibération, pour chacun des manquements relevés. Elle rappelle néanmoins d'ores et déjà que les décisions visées par la société comme étant postérieures aux opérations de contrôle ne constituent que l'application de règles pré-existantes et ne sauraient, dans ces conditions, se voir opposer le principe de non-rétroactivité des règles répressives, qui ne concerne que les règles à caractère impératif.

24. Elle souligne également que, si la CNIL dispose de pouvoirs de publication de lignes directrices, recommandations ou référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel (en application de l'article 8, paragraphe 2, b) de la loi Informatique et Libertés), les règles juridiques sont fixées par les législateurs français et européen et interprétées par les juridictions compétentes, et sont directement applicables aux organismes concernés. Dès lors, l'adoption par la CNIL de référentiels ou lignes directrices n'est pas un préalable à l'obligation de respecter les règles déjà édictées et à l'application de sanctions prévues par le RGPD ou la loi Informatique et Libertés en cas de violation. La formation restreinte relève par ailleurs qu'en l'espèce, les règles établies en matière de prospection commerciale, éclairées par les publications de la CNIL tel son référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales adopté en septembre 2021 et les pages dédiées à la question sur son site web, ainsi que par les lignes

directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 adoptées par le Comité européen de la protection des données (ci-après, le CEPD), permettaient aux acteurs d'appréhender, de manière suffisamment précise, le cadre juridique applicable et les obligations pesant sur eux.

25. Enfin, la formation restreinte entend souligner qu'il ressort du principe de responsabilité, tel que défini par le RGPD, qu'il appartient à l'organisme réalisant les traitements de définir et mettre en œuvre les mesures permettant le respect des dispositions légales applicables. A cet égard, le considérant 74 du RGPD dispose qu' il y a lieu d'instaurer la responsabilité du responsable du traitement pour tout traitement de données à caractère personnel qu'il effectue lui-même ou qui est réalisé pour son compte. Il importe, en particulier, que le responsable du traitement soit tenu de mettre en œuvre des mesures appropriées et effectives et soit à même de démontrer la conformité des activités de traitement avec le présent règlement, y compris l'efficacité des mesures. Ces mesures devraient tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque que celui-ci présente pour les droits et libertés des personnes physiques . Il apparait ainsi que c'est bien aux responsables de traitement – et non aux autorités de protection des données – qu'il appartient de déterminer les modalités pratiques de mise en œuvre des traitements qui leur paraissent les plus adaptées, à la condition que ces modalités leur permettent de démontrer le respect les obligations posées par les textes nationaux et européens.

C. Sur le manquement à l'obligation de recueillir le consentement des personnes concernées pour la mise en œuvre de prospection commerciale par voie électronique en application de l'article L. 34-5 du code des postes et des communications électroniques

26. A titre liminaire, la formation restreinte relève que la société réalise des opérations de prospection commerciale par courrier électronique à partir de données de prospects transmises par ses partenaires. Le cycle de vie de ces données peut ainsi être résumé de la manière suivante : les données sont collectées auprès des personnes concernées par des sociétés telles que […] et […] (appelées primo-collectants), chargées contractuellement de recueillir le consentement des personnes concernées à faire l'objet de prospection commerciale par voie électronique. La collecte de ces données et le recueil du consentement s'effectuent par le biais de formulaires de participation à des jeux-concours en ligne, conçus par ces sociétés. Ensuite, ces données sont transmises à la société CALOGA, qui les intègre dans une ou plusieurs de ses bases de données puis les utilise pour réaliser des opérations de prospection commerciale par voie électronique. Pour ce faire, elle se fonde sur le consentement préalablement recueilli par ses partenaires primo-collectants, pour son compte, à partir des formulaires précités.

27. En droit, aux termes de l'article L. 34-5 du CPCE, est interdite la prospection directe au moyen de système automatisé de communications électroniques […], d'un télécopieur ou de courriers électroniques utilisant les coordonnées d'une personne physique, abonné ou utilisateur, qui n'a pas exprimé préalablement son consentement à recevoir des prospections directes par ce moyen. / Pour l'application du présent article, on entend par consentement toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe. / Constitue une prospection directe l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services. Pour l'application du présent article, les appels et messages ayant pour objet d'inciter l'utilisateur ou l'abonné à appeler un numéro surtaxé ou à envoyer un message textuel surtaxé relèvent également de la prospection directe .

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

29. La rapporteure relève que la société CALOGA réalise des opérations de prospection commer-ciale par voie électronique à partir de données de prospects collectées dans le cadre de jeux-concours, d'offres de tests de produits et de sondages par des sociétés, primo-collectantes. Les formulaires de collecte de données mis en place par les primo-collectants ne permettent pas de recueillir un consentement valable des personnes concernées et les mesures mises en place par la société pour s'assurer que le consentement recueilli est conforme aux exigences du RGPD ne sont pas suffisantes.

30. En défense, la société affirme qu'elle ne pouvait pas prévoir la position de la CNIL sur la conception insatisfaisante des formulaires de collecte des données en l'absence de recommandation spécifique relative à la prospection commerciale, la recommandation cookies ne relevant pas du même secteur d'activité. Elle précise que les décisions évoquées par la rapporteure à l'appui de son argumentation sont postérieures aux opérations de contrôle.

31. Elle ajoute qu'elle ne dispose d'aucune marge de manœuvre sur l'édition des supports de recueil du consentement émis par les primo-collectants et qu'elle a mis en place des mesures pour vérifier la conformité du traitement dont elle a la responsabilité : encadrement contractuel et vérifications des données collectées.

1. Sur cadre juridique applicable et la responsabilité de la société CALOGA

1.1 Sur les conditions de validité du consentement

32. La société considère qu'à l'époque du contrôle, en mai 2022, le cadre juridique applicable ne lui permettait pas de conclure à l'invalidité des mécanismes de recueil du consentement mis en œuvre par ses partenaires. Elle soutient en effet que ce n'est que par une délibération du 29 décembre 2023 (CNIL, FR, 29 décembre 2023, Sanction, n° 2023-025, publié) que la formation restreinte s'est prononcée sur les modalités spécifiques de ce recueil dans le contexte des jeux-concours organisés par les primo-collectants, et qu'elle n'était pas en capacité d'anticiper une telle décision. Elle fait par ailleurs valoir que les recommandations et lignes directrices relatives aux cookies, citées au sein du rapport, ne peuvent trouver à s'appliquer en matière de prospection commerciale.

33. La formation restreinte rappelle que l'ensemble des règles applicables en matière de prospection par voie électronique, ainsi que celles relatives au consentement, sont fixées depuis de nombreuses années et qu'elles précèdent non seulement la publication de la décision susvisée, mais également les opérations de contrôle menées en mai 2022 auprès de la société CALOGA.

34. La formation restreinte rappelle ainsi que le consentement spécifique requis par les dispositions de l'article L. 34-5 du CPCE, combinées à celles de l'article 4 du RGPD, doit s'entendre comme une manifestation de volonté libre, spécifique, éclairée et univoque et ne peut résulter que d'un consentement exprès de l'utilisateur, donné en toute connaissance de cause après une information adéquate sur l'usage qui sera fait de ses données personnelles.

35. Elle relève que la Cour de justice de l'Union européenne a précisé, dans sa décision Planet49 GmbH de 2019 qui portait sur la validité du consentement donné dans le cadre d'une participation à un jeu-concours en ligne, que : l'article 7, sous a) de la directive 95 prévoit que le consentement de la personne concernée peut rendre un tel traitement licite pour autant que ce consentement est indubitablement donné par la personne concernée. Or, seul un comportement actif de la part de cette personne en vue de manifester son consentement est de nature à remplir cette exigence (CJUE, grande chambre, 1er octobre 2019, Planet49 GmbH, C-673/17, ECLI:EU:C:2019:801, point 54). Dès lors, il convient de considérer qu'à défaut d'être donné indubitablement, le consentement doit être considéré comme faisant défaut, ce qui rend le traitement illégal pour défaut de base légale. Plus précisément sur les modalités de recueil, la CJUE affirme que la manifestation de volonté visée à l'article 2, sous h), de la directive 95/46 doit, notamment, être spécifique , en ce sens qu'elle doit porter précisément sur le traitement de données concerné et ne saurait être déduite d'une manifestation de volonté ayant un objet distinct. En l'occurrence, contrairement à ce qu'a fait valoir Planet49, le fait pour un utilisateur d'activer le bouton de participation au jeu promotionnel organisé par cette société ne saurait dès lors suffire pour considérer que l'utilisateur a valablement donné son consentement au placement de cookies (Idem, points 58-59).

36. En outre, le Conseil d'Etat a retenu que le consentement libre, spécifique, éclairé et univoque ne peut qu'être un consentement exprès de l'utilisateur, donné en toute connaissance de cause et après une information adéquate sur l'usage qui sera fait de ses données personnelles. (CE, 10ème et 9ème chambres réunies, 19 juin 2020, Google LLC, n° 430810, pt. 21).

37. La formation restreinte remarque également, à titre d'illustration, que dès 2017, le groupe de travail Article 29 (aujourd'hui Comité européen de la protection des données, ci-après le CEPD) a publié des lignes directrices sur le consentement visant à clarifier les nouvelles dispositions introduites par le RGPD. De nouvelles lignes directrices 5/2020 sur le consentement ont été adoptées le 4 mai 2020, et précisent que le caractère libre du consentement implique un choix et un contrôle réel pour les personnes concernées. En règle générale, le RGPD dispose que si la personne concernée n'est pas véritablement en mesure d'exercer un choix, se sent contrainte de consentir ou subira des conséquences négatives importantes si elle ne donne pas son consentement, le consentement n'est pas valable […] En termes généraux, toute pression ou influence inappropriée exercée sur la personne concernée (pouvant se manifester de différentes façons) l'empêchant d'exercer sa volonté rendra le consentement non valable .

38. Enfin, la formation restreinte souligne que les travaux conduits par la Commission sur les pratiques mises en œuvre en matière de cookies s'agissant des bannières de recueil du consentement peuvent utilement servir à apprécier de manière plus générale les conditions de recueil d'un consentement libre, univoque, spécifique et éclairé, et servir de référence en matière de prospection commerciale lorsqu'elle est fondée sur le recueil du consentement. Il convient en effet de rappeler que les règles générales relatives aux conditions de validité du consentement, tirées notamment de l'article 4 du RGPD, n'ont pas vocation à différer en fonction du secteur concerné et que la CNIL n'est pas tenue de prendre des recommandations spécifiques à chaque secteur. A cet égard, la délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives aux cookies et autres traceurs rappelle expressément que le consentement exigé par l'article 82 de la loi Informatique et Libertés renvoie à la définition et aux conditions prévues aux articles 4.11 et 7 du RGPD (§ 5 et 6).

39. Ainsi, à titre d'illustration et de comparaison, la formation restreinte note que dans sa délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux cookies et autres traceurs , la Commission recommande aux organismes concernés de s'assurer que les utilisateurs prennent la pleine mesure des options qui s'offrent à eux, notamment au travers du design choisi et de l'information délivrée (§ 10) […] Afin de ne pas induire en erreur les utilisateurs, la Commission recommande que les responsables de traitement s'assurent que les interfaces de recueil des choix n'intègrent pas de pratiques de design potentiellement trompeuses laissant penser aux utilisateurs que leur consentement est obligatoire ou qui mettent visuellement plus en valeur un choix plutôt qu'un autre. Il est recommandé d'utiliser des boutons et une police d'écriture de même taille, offrant la même facilité de lecture, et mis en évidence de manière identique (§ 34). Elle ajoute qu'il convient d'être attentif à ce que l'information accompagnant chaque élément actionnable permettant d'exprimer un consentement ou un refus soit facilement compréhensible et ne nécessite pas d'efforts de concentration ou d'interprétation de la part de l'utilisateur. Ainsi, il est notamment recommandé de s'assurer qu'elle n'est pas rédigée de telle manière qu'une lecture rapide ou peu attentive pourrait laisser croire que l'option sélectionnée produit l'inverse de ce que les utilisateurs pensaient choisir. (§ 23). A défaut, le caractère univoque du consentement ne serait pas caractérisé.

40. La formation restreinte remarque également que des études menées sur les pratiques des interfaces numériques, en particulier concernant les cookies, relèvent l'impact considérable de l'apparence des bannières de recueil du consentement sur le choix des utilisateurs, pouvant inciter ces derniers à faire des choix ne reflétant pas leurs préférences sur le partage des données.

41. En outre, contrairement à ce que soutient la société, la formation restreinte relève que la décision de sanction du 29 décembre 2023 (CNIL, FR, 29 décembre 2023, SAN-2023-025, publiée) est fondée sur l'ensemble des éléments susvisés, sans poser aucune exigence nouvelle. Elle ne fait qu'appliquer des règles pré-existantes que la société était parfaitement en mesure d'appréhender.

42. Il ressort ainsi de l'ensemble de ces éléments que les règles relatives au consentement des personnes concernées sont bien antérieures aux opérations de contrôle menées à l'encontre de la société CALOGA et qu'elles apparaissaient suffisamment claires et précises pour permettre à cette dernière d'apprécier la validité du consentement recueilli par ses partenaires et sur lequel elle se fonde pour réaliser ses opérations de prospection.

1.2 Sur les obligations pesant sur la société CALOGA

43. La société reproche à la rapporteure de vouloir instaurer un régime de responsabilités solidaires, non prévu par les textes, entre elle et ses partenaires primo-collectants. Elle considère en effet que sa responsabilité ne doit pas s'apprécier au regard de la licéité des mécanismes de recueil du consentement mis en œuvre par ses partenaires – ces derniers ayant, seuls, la maîtrise des supports de collecte qu'ils éditent –, mais au regard des obligations qui lui incombaient, en propre, au moment des constats.

44. A cet égard, elle soutient que le cadre juridique applicable à l'époque du contrôle ne permettait pas aux acteurs du marketing digital de rendre prévisibles les obligations pesant sur chacun d'eux, l'exigence de procéder à des vérifications des conditions de recueil du consentement par les destinataires des données n'ayant été posée, selon elle, qu'à l'occasion des décisions rendues par la formation restreinte que postérieurement aux contrôles.

45. La société considère en tout état de cause avoir mis en œuvre les mesures nécessaires pour s'assurer de disposer d'un consentement valable, au regard des règles et recommandations applicables à l'époque du contrôle. Elle souligne à cet égard avoir, d'une part, encadré ses relations contractuelles avec ses partenaires primo-collectants et, d'autre part, procédé à des vérifications sur les formulaires mis en œuvre.

46. La formation restreinte relève que le secteur du courtage en données se caractérise par l'existence d'une chaîne de traitements faisant intervenir plusieurs acteurs, avec comme point de départ la collecte des données par les primo-collectants, suivie de leur transmission à un ou plusieurs partenaires pour permettre à ces derniers de réaliser des opérations de prospection commerciale. Dans ce cadre, chacun des organismes impliqués doit, en fonction de sa responsabilité propre, s'assurer de la licéité des opérations auxquelles il participe dans cette chaîne de traitements.

47. La formation restreinte rappelle qu'en application des dispositions combinées des articles L. 34-5 du CPCE et 4 du RGPD, cette licéité exige, pour le responsable de traitement qui entend réaliser ou faire réaliser des opérations de prospection commerciale par voie électronique, de disposer d'un consentement univoque, spécifique, libre et informé des personnes concernées.

48. Lorsque les données des prospects n'ont pas été collectées directement auprès d'eux par le responsable de traitement de la prospection, ce consentement peut avoir été recueilli au moment de la collecte initiale des données par le primo-collectant, pour le compte du responsable de traitement. À défaut, il revient au responsable de traitement de recueillir ou faire recueillir un tel consentement avant de procéder à des actes de prospection (CNIL, FR, 24 novembre 2022, Sanction,

n° SAN-2022-021, publié ; délibération n° 2021-131 du 23 septembre 2021 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales).

49. A cet égard, la formation restreinte a retenu la responsabilité d'un organisme en considérant qu'un simple engagement contractuel de l'organisme fournissant les données de respecter le RGPD et les règles applicables en matière de prospection commerciale ne constituait pas une mesure suffisante (CNIL, FR, 24 novembre 2022, Sanction, n° SAN-2022-021, publié ; CNIL, FR, 31 janvier 2024, Sanction, n° SAN-2024-003, publié ; CNIL, FR, 4 avril 2024, Sanction, n° SAN-2024-004, publié).

50. La formation restreinte insiste sur le fait qu'à l'instar des règles régissant les conditions de validité du consentement, ces exigences ne sont pas nouvelles et qu'elles découlent des textes auxquels tout organisme qui entend réaliser des opérations de prospection commerciale par voie électronique est soumis en sa qualité de responsable de traitement.

51. En l'espèce, c'est bien la société CALOGA qui, en tant que responsable de traitement de la base de données qui sert à la prospection, et en tant que responsable de traitement en aval d'opérations de prospection directe par voie électronique, se trouve soumise aux dispositions de l'article L. 34-5 du CPCE (et non les primo-collectants qui, eux, ne prospectent pas directement les personnes concernées) lequel exige clairement, depuis la transposition en droit français de la directive ePrivacy en 2004, de recueillir le consentement des personnes concernées. Il lui appartient donc, à ce titre, de garantir la licéité de ces opérations en s'assurant de la validité du consentement dont elle entend se prévaloir ou, à défaut, en recueillant elle-même ledit consentement. Il convient de souligner que l'article 7 du RGPD prévoit à cet égard que dans les cas où le traitement repose sur le consentement, le responsable de traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.

52. Par ailleurs, la formation restreinte rappelle que, quel que soit l'organisme qui se charge de recueillir le consentement des personnes concernées, la validité de ce dernier – et donc la licéité des traitements fondés sur un tel consentement – ne peut s'apprécier qu'au moment de son recueil ce qui suppose, en l'espèce, d'examiner les formulaires de collecte mis en œuvre par les partenaires de la société.

53. Ainsi, dans la mesure où la société CALOGA a fait le choix de ne pas recueillir elle-même ce consentement et de se prévaloir de celui recueilli par ses partenaires, le fait de s'assurer de la validité dudit consentement passe nécessairement par un contrôle des mécanismes de recueil mis en œuvre par les primo-collectants.

2. Sur la caractérisation du manquement

54. La formation restreinte relève que, pour constituer ses bases de données VOZEKO, ZEPLAN, BASYLO, CALOGA, la société récupère les adresses électroniques de prospects auprès de partenaires primo-collectants - les sociétés […] - qui les collectent en organisant des jeux-concours, offres de tests de produits, sondages etc.

55. Elle note que, dans les politiques de confidentialité accessibles par le biais des sites web édités par la société CALOGA pour chacune de ses bases de données, il est précisé que les données des prospects lui ont été transmises à la suite d'une participation à un jeu-concours ou à toute autre opération de collecte sur un site édité par une société tierce, mentionnant les bases de données VOZEKO, ZEPLAN, BASYLO, CALOGA en sa qualité de partenaire / sponsor de l'opération, la base légale du traitement de ces données étant le consentement.

56. La formation restreinte relève également que l'instruction a permis d'établir qu'en 2022, la société CALOGA a prospecté 2 315 189 personnes pour la société […] (sur la base de 2287 formulaires), 1 970 942 personnes pour la société […] (sur la base de 2259 formulaires), 2 050 706 personnes pour la société […] (sur la base de 2255 formulaires). Les données de ces prospects ont été collecté par le biais de formulaires essentiellement édités par les sociétés […] et […].

57. Parmi les 3 653 formulaires transmis par la société dont certains présentent des aspects identiques, la formation restreinte observe qu'au moins 21 d'entre eux proposent à l'utilisateur un bouton validant à la fois sa participation au jeu concours et l'utilisation de ses données pour recevoir des offres de la part de partenaires de la société organisatrice du jeu.

58. Après avoir complété ses coordonnées, l'utilisateur a le choix entre cliquer sur un bouton JE PARTICIPE ou JE VALIDE (pouvant aussi s'intituler CONTINUER , VALIDER MA PARTICIPATION , situé au bas du formulaire et permettant à la fois de valider sa participation au jeu et de consentir à ce que ses données soient transmises à des partenaires et utilisées par ces derniers à des fins de prospection commerciale, ou cliquer sur un lien permettant de participer uniquement au jeu-concours, en refusant la transmission et l'utilisation de ses données à des fins de prospection commerciale (lien pouvant être contenu dans la phrase pour participer sans recevoir les offres des sponsors, cliquez ici , ou encore pour participer sans recevoir les offres des sponsors et de leurs partenaires, cliquez ici).

59. La formation restreinte considère que tels qu'ils sont conçus, les formulaires proposés ne permettent pas aux personnes concernées d'exprimer de manière valable un choix reflétant leurs préférences en matière de transmission et d'utilisation de leurs données à des fins de prospection commerciale. En effet, l'aperçu global des interfaces met

particulièrement en valeur les boutons de type CONTINUER ou VALIDER qui, par leur taille – nettement supérieure au reste des mentions – et leur couleur – qui tranche avec le fond utilisé –, se distinguent des autres informations délivrées. De même, leur intitulé évoque davantage la conclusion du parcours utilisateur plutôt qu'une utilisation des données à des fins de prospection commerciale dans la mesure où, en langage courant, on valide les informations renseignées dans un formulaire et on autorise , on accepte une utilisation de données. Enfin, leur emplacement donne l'impression de devoir obligatoirement être cliqués pour terminer l'inscription et participer au jeu-concours. A contrario, le lien hypertexte permettant de participer au jeu sans accepter l'utilisation de ses données par les partenaires est présenté dans le corps du texte situé au-dessus ou en-dessous des boutons d'acceptation, en caractères d'une taille nettement inférieure à celle utilisée pour les boutons et sans mise en valeur particulière, de sorte qu'il n'apparait pas intuitif qu'il est possible de participer sans cliquer sur l'un des boutons précités et donc sans transmettre ses données à des tiers à des fins de prospection. Le consentement recueilli est, dans ces conditions, dépourvu de caractère univoque et libre.

60. La formation restreinte considère que l'utilisateur n'est pas mis à même de pouvoir donner son consentement en toute connaissance de cause, de manière libre et univoque, après une information adéquate sur l'usage de ses données. L'apparence trompeuse des formulaires l'incite à donner son consentement à l'utilisation de ses données à des fins de prospection.

61. Par ailleurs, la formation restreinte rappelle que, si la conception de ces formulaires ne lui est pas imputable, en tant que telle, la société aurait dû, comme indiqué aux points 46 à 50 de la présente délibération, s'assurer de la validité du consentement dont elle entend se prévaloir pour réaliser ses opérations de prospection.

62. La formation restreinte note que la société a mis en place des mesures de vérifications dès 2014 puis a procédé à une mise à jour de ces mesures en 2018 avec l'entrée en application du RGPD. A la date des contrôles, ces mesures de vérification portaient sur un engagement contractuel des primo-collectants permettant d'exiger qu'un consentement valable a été recueilli pour permettre la transmission des données. Avant chaque signature de contrat, la société procédait à une vérification des pratiques du primo-collectant. En cours de contrat, la société vérifiait la conformité des opérations de collecte organisées par les primo-collectants, c'est-à-dire les mentions d'information, le type de données collectées, la présence d'un lien pour participer sans consentir aux finalités de prospection et la présence du nom de la marque associée à une base de données dans la liste des destinataires. La société a toutefois indiqué que, dans le cadre de la procédure de contrôle, pour certains partenaires primo-collectants, les vérifications sont effectuées à la conclusion du partenariat et que l'ensemble des opérations est validé par défaut, la société ne procédant pas à des vérifications sur tous les formulaires, ce qu'elle confirme dans ses écritures. C'est le cas notamment du partenaire […], lequel transmet le plus grand nombre de données de prospects à la société.

63. La formation restreinte relève à cet égard que la société a indiqué, d'une part, avoir prévu dans ses relations contractuelles avec ses partenaires primo-collectants que ces derniers s'engageaient à recueillir valablement le consentement des personnes concernées et, d'autre part, avoir mis en place depuis 2018 certaines procédures de vérifications des formulaires de collecte. S'agissant du cadre contractuel, la formation restreinte relève que les clauses contenues dans les contrats passés avec ses partenaires apparaissent très générales – ces derniers s'engageant à recueillir valablement le consentement des personnes concernées, à documenter ledit consentement et à en transmettre la trace à CALOGA. La société destinataire des données ne peut s'en contenter et se doit d'opérer des vérifications concrètes sur les conditions de recueil du consentement sur lequel elle entend se fonder pour réaliser ses opérations de prospection. A cet égard, la formation restreinte relève que la société a bien procédé à l'examen régulier des formulaires de collecte mis en œuvre par ses partenaires. Néanmoins, les constatations réalisées montrent que les vérifications n'ont pas été effectuées à une fréquence suffisamment élevée au regard du nombre de formulaires de collecte utilisés et, qu'en tout état de cause, la société n'en a pas tiré les conséquences qui s'imposaient quant à l'absence de validité du consentement recueilli et a continué à utiliser les données transmises pour réaliser ses opérations de prospection commerciale. Il apparait en effet qu'au regard des pièces figurant au dossier, les formulaires analysés dans le cadre de la procédure de contrôle ne permettait pas de recueillir un consentement valable des personnes concernées, alors même que les vérifications opérées par la société avaient débuté plusieurs mois auparavant.

64. Il ressort de ce qui précède que, faute pour la société de disposer d'un consentement valable des personnes concernées pour constituer une base de contacts à des fins de prospection commerciale et l'utiliser, s'agissant des coordonnées recueillies par les sociétés […] et […], la société CALOGA a commis un manquement aux dispositions de l'article L.34-5 du CPCE.

D. Sur le manquement à l'obligation de respecter le droit au retrait du consentement en application de l'article L. 34-5 du CPCE

65. En droit, l'article L. 34-5 du CPCE, qui transpose la directive ePrivacy laquelle fait référence à la notion de consentement au sens de l'article 4 paragraphe 11 du RGPD, prévoit qu' est inter-dite la prospection directe au moyen de système automatisé de communications électroniques […], d'un télécopieur ou de courriers électroniques utilisant les coordonnées d'une personne phy-sique […] qui n'a pas exprimé préalablement son consentement à recevoir des

prospections di-rectes par ce moyen. Pour l'application du présent article, on entend par consentement toute ma-nifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des don-nées à caractère personnel la concernant soient utilisées à fin de prospection directe […]. En outre, aux termes de l'alinéa 5 de l'article L. 34-5 du CPCE, dans tous les cas, il est interdit d'émettre, à des fins de prospection directe, des messages au moyen de système automatisé de communications électroniques au sens du 6° de l'article L. 32, télécopieurs et courriers électro-niques, sans indiquer de coordonnées valables auxquelles le destinataire puisse utilement trans-mettre une demande tendant à obtenir que ces communications cessent sans frais autres que ceux liés à la transmission de celle-ci .

66. L'article L. 34-5 du CPCE conditionne donc la réalisation d'opérations de prospection directe au consentement du destinataire et prévoit de manière corrélative le droit à l'intéressé de retirer son consentement en transmettant une demande tendant à obtenir que les communications de pros-pection cessent. L'intéressé peut ainsi revenir sur son choix d'avoir accepté la réalisation d'opérations de prospection.

67. Le retrait du consentement des prospects en matière de prospection par voie électronique et ses modalités s'analysent au regard des dispositions de l'article 7 paragraphe 3 du RGPD, applicable s'agissant des dispositions de l'article L. 34-5 du CPCE dans la mesure où la directive ePriva-cy prévoit en son article 2 (f) que le consentement d'un utilisateur ou d'un abonné correspond au consentement de la personne concernée figurant dans la directive 95/46/CE, à laquelle s'est substitué le RGPD. Pour ce faire, les lignes directrices n° 5/2020 sur le consentement au sens du RGPD, adoptées le 4 mai 2020 par le CEPD, peuvent constituer une source d'inspiration.

68. Selon l'article 7 paragraphe 3 du RGPD, la personne concernée a le droit de retirer son consen-tement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement .

69. Dans ses lignes directrices n° 5/2020 sur le consentement au sens du RGPD adoptées le 4 mai 2020, le CEPD indique que : La personne concernée devrait également être en mesure de reti-rer son consentement sans subir de préjudice. Cela signifie, entre autres, qu'un responsable du traitement doit proposer la possibilité de retirer son consentement gratuitement ou sans entraîner la diminution du niveau de service (point 114). Cette disposition se lit à la lumière du considé-rant 42 de ce Règlement qui prévoit que : le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice .

70. La rapporteure relève que les prospects peuvent donner leur consentement à recevoir les offres de partenaires de CALOGA, par le biais des formulaires de collecte, en un seul clic. Leurs don-nées sont ensuite stockées dans les différentes bases de données de la société CALOGA. S'il est possible à l'utilisateur de se désabonner, lors de la réception d'un courriel, en cliquant sur le lien de désinscription, ce désabonnement ne vaudra que pour la base de données à partir de laquelle le courriel lui a été envoyé ou pour un annonceur final au nom duquel le courriel a été envoyé. Pour se désabonner des offres adressées par la société CALOGA en intégralité, il est nécessaire d'envoyer un courriel à la société CALOGA. La rapporteure considère qu'il n'est ainsi pas aussi simple de retirer son consentement que de le donner dans la mesure où il n'est pas possible de retirer son consentement à recevoir des offres issues de toutes les bases de données de la société CALOGA en un seul clic, alors que les prospects donnent leur consentement en un seul clic pour recevoir toutes les offres de partenaires adressées par CALOGA.

71. La société affirme que des liens insérés dans les courriels de prospection permettent de se désinscrire pour ne plus recevoir du contenu publicitaire d'un annonceur ou d'une base de don-nées spécifique. Elle précise que via l'adresse dpo@caloga.com , il est possible de solliciter un retrait du consentement pour l'ensemble des bases de données.

72. En outre, la société remet en question l'existence à un droit absolu au retrait du consentement dès lors que le consentement peut être donné, en un seul clic, à une multitude de partenaires. Elle interroge de ce fait l'obligation qui pèse sur l'ensemble de ces partenaires de prendre en compte le retrait du consentement et affirme s'être conformée aux préconisations de la CNIL publiées sur son site en matière de transmission de données à des partenaires.

73. En l'espèce, la formation restreinte relève que la société organise ses traitements autour de quatre bases de données : CALOGA, ZEPLAN, BASYLO et VOZEKO, qui comprennent cha-cune plus d'un million d'entrées, avec des doublons. Lorsque les prospects donnent leur consen-tement en un seul clic à la collecte de leurs données à des fins de prospection, ces données peu-vent être envoyées vers une ou deux bases de données de la société CALOGA. Ces bases de données sont présentées comme des partenaires différents dans les listes des partenaires des formulaires de collecte mis en œuvre par les primo-collectants.

74. La formation restreinte note que, dans les courriels de prospection envoyés pour le compte d'annonceurs, deux liens sont insérés. Le premier lien permet la désinscription à recevoir des con-tenus publicitaires d'un annonceur final spécifique, quelle que soit la base de données utilisée. Un second lien permet la désinscription à recevoir les contenus

publicitaires des partenaires d'une marque de la société CALOGA, c'est-à-dire d'une de ses bases de données. Ainsi, si le pros-pect s'est inscrit dans une autre base de données de la société, nommée différemment sous une autre marque, il continuera à recevoir des offres envoyées de cette autre base même s'il a utilisé le second lien pour se désabonner des offres reçues. La formation restreinte note également que, pour que le retrait du consentement d'un prospect soit pris en compte pour l'ensemble des bases de données gérées par la société CALOGA (c'est-à-dire pour l'ensemble des marques selon la terminologie employée par la société), le prospect ne peut pas exprimer cette demande par le biais d'un lien figurant dans un seul courriel de prospection mais doit adresser une demande explicite au DPO de la société par courriel ou cliquer sur plusieurs liens de désinscriptions insérés dans des courriers électroniques distincts.

75. Un prospect peut donc être inscrit dans une ou deux bases de données en un seul clic. Cepen-dant, lorsqu'il souhaite retirer son consentement à recevoir des offres d'annonceurs adressées par la société CALOGA et issues des deux bases auxquelles il est inscrit, il devra faire une demande spécifique de désinscription pour toutes les bases de données de la société dans lesquelles il est inscrit, ce qui nécessite plusieurs démarches et clics sur différents liens de désinscription contenus dans les courriels distincts de prospection ou d'envoyer un courriel à une adresse dédiée.

76. La formation restreinte relève donc que, dans le système mis en œuvre par la société CALOGA, il n'est pas possible, pour le prospect, de se désinscrire en un seul clic, des bases de données de CALOGA auxquelles il s'est inscrit en un seul clic. Elle prend toutefois note que si le prospect n'est inscrit que dans une seule base de données de CALOGA, le prospect n'aura besoin que d'un seul clic pour retirer son consentement. La formation restreinte considère que, lorsqu'un prospect est inscrit dans deux bases de données de la société en un seul clic au moment de la col-lecte, il devrait pouvoir, en un seul clic depuis un lien URL présent dans le courriel de prospec-tion, retirer son consentement pour ces deux bases de données. L'action de cliquer sur ce lien aurait ainsi les mêmes conséquences que l'envoi d'un courriel à la société afin d'obtenir une dé-sinscription aux bases de données de la société CALOGA auxquelles il s'est inscrit.

77. S'agissant plus particulièrement des règles publiées sur le site web de la CNIL dans une fiche pratique relative à la transmission des données à des partenaires, la formation restreinte relève qu'elles indiquent effectivement qu'il est possible pour un primo-collectant qui transmet des don-nées à des partenaires de recueillir le consentement d'un prospect, au moment de la collecte de ses données, en un seul clic pour le compte de plusieurs partenaires - qui seront destinataires des données et responsables de traitement de leurs opérations de prospection - dès lors qu'ils sont identifiés. Toutefois, contrairement à l'analyse qu'en tire la société, cette publication ne fait pas référence aux modalités de retrait du consentement des intéressés et ne comportent donc pas d'élément sur ce point, contrairement aux dispositions de l'article 7 du RGPD, qui dispose qu'il doit être aussi simple de retirer son consentement que de le donner. Sur ce fondement, la forma-tion restreinte considère qu'en donnant son consentement en un clic pour figurer dans deux bases de données de CALOGA, le prospect doit donc pouvoir retirer son consentement de ces deux bases de données en un clic, ce d'autant que les bases de données relèvent du même responsable de traitement.

78. Outre cette problématique générale, la formation restreinte relève également que la société CALOGA a intitulé une de ses quatre bases de données (ou marques) CALOGA (le nom des autres bases / marques étant ZEPLAN, BASYLO et VOZEKO). La formation restreinte souligne que ce système mis en place par la société prête à confusion dès lors que le prospect peut légiti-mement penser, en cliquant sur le lien de désinscription intitulé ne plus recevoir aucune offre des annonceurs de CALOGA , que l'action vaut pour toutes les bases de données de la société. En effet, il est fortement trompeur, du point de vue du prospect, que la société CALOGA ait donné son nom à une des bases de données. Un prospect qui, au moment de la collecte de ses données, vérifie la liste des partenaires, verra s'afficher le nom caloga en tant que marque et non en tant que société. Il ne s'apercevra pas que la société CALOGA possède d'autres marques, et donc d'autres bases de données, qui figurent sous un autre nom dans la liste des partenaires.

79. Il ressort de ces éléments qu'il existe un réel préjudice pour les prospects croyant avoir retiré leur consentement. Malgré une action positive de leur part sollicitant le retrait de leur consentement, ils continueront à recevoir des courriels de prospection dans un contexte de sollicitations intenses lié à la nature même du marché de la prospection par voie électronique.

80. A cet égard, et au vu de l'ensemble de ce qui précède, la formation restreinte considère que la société ne saurait se prévaloir de ses choix d'organisation interne, en optant pour une répartition des données collectées en différentes bases de données correspondant à différentes marques, pour se soustraire à ses obligations, ses choix organisationnels ne devant pas faire obstacle au re-trait du consentement dans les mêmes conditions que celles dans lesquelles il a été obtenu.

81. Partant, en ne proposant pas aux personnes concernées la possibilité de retirer son consen-tement en un seul clic des bases de données auxquelles elles se sont inscrites en un clic, la so-ciété a commis un manquement à l'article L. 34-5 du CPCE tel qu'éclairé par l'article 7, pa-ragraphe 3 du RGPD.

E. Sur le manquement relatif à l'obligation de disposer d'une base légale pour transmettre les données de prospects à des fins de prospection commerciale par voie électronique en application de l'article 6 du RGPD

82. L’article 6, paragraphe 1, du RGPD dispose que le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : a) la personne concernée a con-senti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spéci-fiques; b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci; c) le traite-ment est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis; d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concer-née ou d'une autre personne physique; e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement; f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le respon-sable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère per-sonnel, notamment lorsque la personne concernée est un enfant .

83. En vertu de l’article 4, paragraphe 11 du RGPD, le consentement de la personne concernée s’entend de 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 .

84. S’agissant de la qualité de recueil du consentement, la Cour de justice de l’Union européenne (CJUE) a précisé, dans sa décision Planet49 GmbH : l’article 7, sous a), de la directive 95 pré-voit que le consentement de la personne concernée peut rendre un tel traitement licite pour autant que ce consentement est indubitablement donné par la personne concernée. Or, seul un com-portement actif de la part de cette personne en vue de manifester son consentement est de nature à remplir cette exigence (CJUE, grande chambre, 1er octobre 2019, Planet49 GmbH, C-673/17, §54)

85. A défaut d’être donné indubitablement, le consentement doit être considéré comme faisant défaut, ce qui rend le traitement illégal pour défaut de base légale.

86. Sur les modalités de recueil du consentement, la CJUE affirme que la manifestation de volonté visée à l’article 2, sous h), de la directive 95/46 doit, notamment, être spécifique , en ce sens qu’elle doit porter précisément sur le traitement de données concerné et ne saurait être déduite d’une manifestation de volonté ayant un objet distinct. En l’occurrence, contrairement à ce qu’a fait valoir Planet49, le fait pour un utilisateur d’activer le bouton de participation au jeu promo-tionnel organisé par cette société ne saurait dès lors suffire pour considérer que l’utilisateur a va-lablement donné son consentement au placement de cookies (idem, §§ 58-59).

87. Par ailleurs, s’agissant de la qualité de l’information fournie lors du recueil du consentement, la CJUE a indiqué que une information claire et complète doit permettre à l’utilisateur de détermi-ner facilement les conséquences du consentement qu’il pourrait donner et garantir que ce consen-tement soit donné en pleine connaissance de cause. Elle doit être clairement compréhensible et suffisamment détaillée pour permettre à l’utilisateur de comprendre le fonctionnement des cookies qui sont utilisés (idem, §74).

88. Le Conseil d’Etat, quant à lui, a retenu que le consentement libre, spécifique, éclairé et univoque ne peut qu'être un consentement exprès de l'utilisateur, donné en toute connaissance de cause et après une information adéquate sur l'usage qui sera fait de ses données personnelles. […] Enfin, indépendamment des modalités dans lesquelles il est recueilli, le consentement n'est valide que s'il est précédé d'une présentation claire et distincte de l'ensemble des finalités poursuivies par le trai-tement (CE, 10ème et 9ème chambres réunies, 19 juin 2020, Google LLC, n° 430810, pt. 21).

89. Enfin, dans son référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales, la CNIL estime que si la transmission a pour finalité de permettre aux partenaires commerciaux de réaliser de la prospection nécessitant le re-cueil du consentement préalable des personnes concernées (prospection électronique) :

o eu égard au fait que la prospection commerciale par voie électronique présente des risques spécifiques (notamment par le volume de sollicitations susceptibles d’être reçues du fait de son automatisation), l’organisme transmettant les données doit informer les per-sonnes concernées, sur le support de collecte des données (formulaire en ligne ou formu-laire papier), et recueillir leur consentement à cette transmission ;

o l’organisme transmettant les données doit, au préalable, avoir permis aux personnes concernées d’apprécier les conséquences de leur choix quant à la transmission en les in-formant de l’étendue de celle-ci. La mise en évidence, auprès des personnes concernées, du nombre et du secteur d’activité des partenaires qui seraient rendus destinataires des données, est un exemple de mesure contribuant à respecter les attentes raisonnables des personnes concernées en la matière ;

o avant de réaliser de la prospection par voie électronique, les partenaires rendus destina-taires des données doivent prouver qu’ils disposent, eux aussi, du consentement des per-sonnes qui seront démarchées. […] .

La CNIL a en effet estimé qu'il devait y avoir un parallélisme entre la transmission de données à des tiers pour constituer des bases de données à des fins de prospection commerciale par voie électronique et le régime de cette transmission, impliquant que cette transmission se fasse sur un régime de consentement (opt in) alors que, lorsque la prospection est fondée sur un régime d'intérêt légitime avec opposition (opt out), la transmission des données à des tiers ne nécessite pas de consentement (mais la personne doit en être informée, avec les catégories de destinataires) et pouvoir s'y opposer (CNIL, P, 1er décembre 2021, Mise en demeure, Société X, n° MED-2021-131, non publié).

90. La rapporteure affirme que, contrairement à l'analyse de la société, les partenaires auxquels elle transmet des données de prospects à des fins de prospection commerciale par voie électronique n'interviennent pas en qualité de sous-traitants pour le compte de la société CALOGA et que la société aurait donc dû disposer du consentement des prospects pour transmettre leurs données à des partenaires commerciaux à des fins de prospection électronique. Or, le consentement recueilli au moment de la collecte des données de prospects n'étant pas valable, la société ne pouvait pas transmettre ces données à ses partenaires.

91. La société conteste la qualité de responsable de traitement de ses partenaires destinataires et les considère, sur le fondement d'une analyse factuelle, comme des sous-traitants. A ce titre, elle considère qu'elle n'a pas à recueillir un consentement spécifique pour la transmission des don-nées.

92. Elle affirme qu'en l'absence de recommandations de la CNIL, il ne peut pas lui être reproché de ne pas avoir anticipé les exigences de la CNIL relatives à la qualité des partenaires destinataires des données et donc à l'obligation de recueillir un consentement spécifique pour la transmission des données de prospects à ses partenaires.

93. La formation restreinte relève qu'en l'espèce, dans le cadre de son activité de courtier en données, la société constitue ses bases de données de prospects auprès de partenaires primo-collectants (les sociétés […], notamment) et les transmet ensuite à d'autres partenaires qui met-tent en œuvre des activités de prospection par voie électronique au bénéfice d'annonceurs finaux. Les principaux partenaires à qui ces données sont transmises sont les sociétés […] (1,9 millions de données de prospects transmises lors de la dernière transmission de février 2023) et […] (2,2 mil-lions de données de prospects transmises lors de la dernière transmission de mai 2023).

94. Comme elle l'a détaillé dans ses développements précédents (points 17 et 18), la formation restreinte relève que la société CALOGA transmet des données à ses partenaires afin que soient réalisées des opérations de prospection commerciale par voie électronique pour le compte de leurs clients annonceurs à partir des bases dont ses partenaires ont ciblé, avec leurs propres outils, les segments qu'ils souhaitent solliciter. L'administration de ces bases de données et les opérations constituent de nouveaux traitements de données à caractère personnel, mis en œuvre par d'autres responsables de traitement que la société CALOGA. Dans ce contexte, la formation restreinte considère que la société CALOGA doit être regardée comme responsable du traitement de transmission de données de prospects à des partenaires afin que soient réalisées des opérations de prospection commerciale par voie électronique par ces derniers pour le compte de tiers. Or, pour être licite, comme le souligne le référentiel relatif aux traitements de données à caractère person-nel mis en œuvre aux fins de gestion des activités commerciales de la CNIL, lorsque la transmis-sion des données a pour finalité de permettre aux partenaires commerciaux de réaliser de la pros-pection nécessitant le recueil du consentement préalable des personnes concernées (prospection électronique), l'organisme qui transmet les données doit recueillir le consentement des personnes concernées à cette transmission de leurs données. En effet, dès lors que les données sont trans-mises pour servir uniquement à des opérations pour lesquelles la loi est venue, en raison de leur intrusivité particulière, exiger un consentement, la CNIL estime que la base légale de l'intérêt légitime ne peut être retenue. Ainsi, dans l'écosystème spécifique des courtiers en données où la transmission des données de prospects a pour finalité des opérations de prospection par voie élec-tronique, prospection reposant sur la base légale du consentement, tous les traitements de trans-mission des données à caractère personnel pour cette finalité doivent également reposer sur la base légale du consentement.

95. Or, la société CALOGA ne dispose pas d'un consentement valable pour transmettre les données de prospects à ses partenaires à des fins de prospection commerciale par voie électronique pour le compte de leurs clients annonceurs, la société considérant qu'elle n'a pas à recueillir un consen-tement spécifique pour cette transmission, celle-ci relevant de son intérêt légitime.

96. En ne disposant pas du consentement des personnes concernées pour cette transmission de leurs données, et ainsi d'une base légale valable pour mettre en œuvre ce traitement, la socié-té a commis un manquement à l'article 6 du RGPD.

F. Sur le manquement relatif à l'obligation de conserver les données pour une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées en application de l'article 5-1-e du RGPD

97. Aux termes de l'article 5, paragraphe 1, e) du RGPD, les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (…) .

98. En application de ces dispositions, il incombe au responsable de traitement de définir une durée de conservation conforme à la finalité du traitement. Lorsque cette finalité est atteinte, les données doivent être supprimées ou anonymisées, ou faire l'objet d'un archivage intermédiaire pour une durée déterminée lorsque leur conservation est nécessaire, par exemple pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses notamment.

99. A cet égard, la formation restreinte a rappelé à plusieurs reprises que la durée de conservation des données à caractère personnel doit être déterminée en fonction de la finalité poursuivie par le traitement. Lorsqu'elles ne sont plus nécessaires au besoin de la finalité pour laquelle elles ont été collectées, les données doivent soit être supprimées, soit faire l'objet d'un archivage intermédiaire lorsque leur conservation est nécessaire, par exemple pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses. Cet archivage intermédiaire nécessite tout d'abord de réaliser un tri des données pertinentes à archiver, au regard des finalités justifiant la conservation de ces données (obligations légale ou comptable, finalité contentieuse, etc.), puis d'opérer une séparation avec la base active, qui peut être physique – via un transfert des données au sein d'une base d'archives dédiée – ou logique – via la mise en place de mesures techniques et organisationnelles garantissant que seules les personnes ayant un intérêt à traiter les données en raison de leurs fonctions puissent y accéder (CNIL, FR, 8 septembre 2022, Sanction, n° SAN-2022-018, publié ; CNIL, FR, 29 décembre 2023, Sanction, n° SAN-2023-023, publié).

100. S'agissant du point de départi du délai, la formation restreinte a également considéré qu'un responsable de traitement ne [pouvait], sans méconnaître le principe de limitation de la durée de conservation des données, considérer que la simple ouverture d'un courriel de prospection par une personne permet de refaire courir le point de départ du délai de conservation des données des prospects et ainsi conserver de telles données alors même que les prospects n'ont pas démontré, par un acte clair, un intérêt pour les produits ou services de la société pendant plusieurs années (CNIL, FR, 28 juillet 2020, délibération de sanction n°SAN-2020-003 ; CNIL, FR, délibération SAN-2020-016 du 7 décembre 2020). Cette position reflète la doctrine de la CNIL qui dès 2016, dans l'article 5 de la Délibération n° 2016-264 du 21 juillet 2016 portant modification d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects (NS-048), précisait que les données à caractère personnel relatives à un prospect non client peuvent être conservées pendant un délai de trois ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect (par exemple, une demande de documentation ou un clic sur un lien hypertexte contenu dans un cour-riel ; en revanche, l'ouverture d'un courriel ne peut être considérée comme un contact émanant du prospect) .

101. Ces éléments sont aujourd'hui rappelés dans le référentiel relatif aux traitement de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales : Les données à caractère personnel relatives à un prospect non client peuvent être conservées pendant un délai de trois ans à compter de leur collecte par le responsable de traitement ou du dernier contact éma-nant du prospect (par exemple, une demande de documentation ou un clic sur un lien hypertexte contenu dans un courriel renvoyant vers le produit promu ; en revanche, la simple ouverture d'un courriel ne devrait pas être considérée comme un contact émanant du prospect). Au terme de ce délai de trois ans, le responsable de traitement pourra reprendre contact avec la personne con-cernée afin de savoir si elle souhaite continuer à recevoir des sollicitations commerciales. En l'ab-sence de réponse positive et explicite de la personne, il conviendra de supprimer les données ou de les archiver pour une durée conforme aux dispositions en vigueur (page 11).

102. La rapporteure considère d'abord qu'en conservant les données de prospects pendant une durée de quatre ans, sans procéder à un tri ou à un archivage intermédiaire des données, alors que ces prospects sont considérés comme inactifs par la société passé un délai d'un an sans interaction, la société a conservé les données pour une durée excessive. Elle considère ensuite que le fait de prendre en compte l'ouverture d'un courriel comme point de départ du délai n'est pas conforme aux exigences du RGPD dès lors que cette interaction, parfois involontaire, pourrait permettre à la société de conserver les données de prospects sans limitation de durée en l'absence de tout acte volontaire des personnes concernées pour exprimer un souhait en ce sens.

103. La société indique qu'elle a compartimenté ses bases de données afin de poursuivre trois finali-tés : exploiter les données de prospects actifs, identifier les prospects ayant retiré leur consente-ment et conserver les données de prospects inactifs à des fins probatoires. Elle ajoute qu'elle met en œuvre différentes durées de conservation en fonction de la finalité poursuivie : 12 mois à compter de la dernière action du prospect (ouverture d'un courriel de prospection) à des fins d'exploitation pour la prospection commerciale. Au-delà des 12 mois, le prospect est considéré comme inactif. Les données des prospects inactifs sont conservées 4 ans à des fins probatoires liées au consentement.

104. En outre, elle précise que ces durées de conservation et le point de départ du délai lui sont imposés par les contraintes opérationnelles des Fournisseurs d'Accès Internet (FAI) ainsi que par les délais de prescription en matière pénale prévus à l'article 133-3 du code pénal.

105. La formation restreinte relève que la société CALOGA applique une durée de conservation de douze mois maximum à compter de la dernière action du prospect actif . La société prend en compte la date la plus tardive entre la date de collecte ou d'expression de consentement de la personne concernée, la date d'ouverture du courriel ou la date de clic dans un lien

situé dans un courriel. Au-delà de ces douze mois et sans interaction du prospect, ce dernier est considéré comme inactif . Une durée de conservation supplémentaire de quatre ans à compter du pas-sage en prospect inactif est ensuite appliquée par la société à des fins probatoires relatives au consentement des prospects. Elle relève que la société conserve ainsi plus de 13,5 millions d'adresses de courrier électronique correspondant à des prospects dont les données ont été collec-tées depuis plus de trois ans ou qui sont devenus inactifs depuis plus de trois ans.

106. En premier lieu, la formation restreinte relève que, pour déterminer le caractère actif ou inactif d'un prospect, la société a pris en compte la date de dernière ouverture d'un courriel électronique de prospection commerciale, comme date de dernière interaction avec le prospect faisant courir le délai de douze mois avant de passer le prospect au statut inactif. Ainsi, à chaque fois que le pros-pect ouvrira un courriel de la société – même par inadvertance –, la société prolongera la conser-vation des données de ce prospect dans ses bases actives, et ce potentiellement sans limitation. Selon une doctrine établie de longue date, la notion d' interaction , telle qu'entendue par la société, est trop large en ce que la seule ouverture d'un courrier électronique ne traduit pas néces-sairement une volonté de rester en contact avec la société qui démarche la personne concernée. En effet, selon le service de messagerie électronique utilisé, le fait de cliquer une seule fois sur un nouveau courrier électronique peut suffire à l'ouvrir, ce qui peut résulter d'un simple accident de navigation. L'ouverture d'un courrier électronique ne procède donc pas de la même démarche active de la part de la personne concernée que, par exemple, le fait de cliquer sur un lien url con-tenu dans un courrier électronique de prospection renvoyant vers un produit ou un service parti-culier, ou encore de solliciter la société pour obtenir de la documentation sur l'un de ses produits ou services.

107. En second lieu, la formation restreinte relève que les données des prospects de la société sont acquises pour une finalité déterminée, à savoir la prospection commerciale. Si, une fois cette fina-lité atteinte, la conservation de certaines données peut être justifiée au regard d'autres finalités, par exemple les finalités de conservation des preuves liées au consentement des prospects et celle visant à s'assurer de l'arrêt total de toute sollicitation commerciale dudit prospect, invoquées par la société, la formation restreinte considère en revanche que la société se doit, à compter du pas-sage au statut inactif , d'effectuer un tri pour supprimer les données qui ne sont plus néces-saires et ne conserver que celles devant l'être au regard de ces finalités, en procédant à leur archi-vage intermédiaire pour en limiter l'accès aux seules personnes ayant le besoin d'en connaître en raison de leurs fonctions. La formation restreinte note que la société a confirmé ne procéder à aucun archivage intermédiaire et conserver l'ensemble des données de ses prospects en base ac-tive pendant une durée de quatre ans à compter du moment où le prospect est considéré comme inactif , ne mettant ainsi en place aucun accès différencié en fonction des finalités poursuivies et en ne procédant à aucun tri ou suppression des données en cause, telles que la date de nais-sance, le code postal ou encore l'adresse postale. Une telle pratique ne permet pas de respecter le principe de limitation posé à l'article 5, paragraphe 1, e) du RGPD.

108. En tout état de cause, la formation restreinte considère que les contraintes opérationnelles imposées par des acteurs économiques ne peuvent pas justifier que les exigences découlant du RGPD soient écartées.

109. S'agissant des délais prévus en matière de procédure pénale, la formation restreinte considère que les dispositions du code pénal invoquées par la société, à savoir la combinaison des articles 226-16 et 133-3 du code pénal, ne s'appliquent pas au traitement de prospection mis en œuvre par la société CALOGA. En effet, l'article 226-16 du code pénal vise le fait, y compris par négli-gence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi , ce qui concerne uniquement les traitements nécessitant des formalités préalables au traitement comme les traitements dans le domaine de la santé, ce qui n'est pas le cas en l'espèce.

110. Par conséquent, la formation restreinte relève que le fait, pour la société, de considérer l'ouverture d'un courriel comme une interaction du prospect pour définir le point de départ de la durée de conservation et de conserver en base active, sans opérer de tri, les données de ses prospects pendant une durée de quatre ans à compter du passage en statut inactif , constitue un manquement aux dispositions de l'article 5, paragraphe 1, e) du RGPD.

G. Sur le manquement relatif à l'obligation d'assurer la sécurité des données à caractère personnel en application de l'article 32 du RGPD

111. 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 .

112. 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'ANSSI alertait et rappelait les bonnes pratiques s'agissant de la conservation des mots de passe en indiquant qu'ils doivent être stockés sous une forme transformée par une fonction cryptographique à sens unique (fonction de hachage) et lente à calculer telle que PBKDF2 et que la transformation des mots de passe doit faire intervenir un sel aléa-toire pour empêcher une attaque par tables précalculées .

113. La Commission précise également dès sa délibération n° 2017-012 du 19 janvier 2017, s'agissant des modalités de conservation, que le mot de passe ne doit jamais être stocké en clair. Elle re-commande qu'il 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. La commission estime de plus que le sel ou la clé doit être généré au moyen d'un générateur de nombres pseudo-aléatoires cryptographiquement sûr (c'est-à-dire basé sur un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue), et ne pas être stocké dans le même espace de stockage que l'élément de vérification du mot de passe . Ces exigences ont été reprises dans la délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés, et abrogeant la délibération n°2017-012 du 19 janvier 2017 (cf. §§ 48 et s.). En outre, la formation restreinte a, à plusieurs reprises, sanctionné des or-ganismes sur ce point (v. en ce sens, CNIL, FR, 24 novembre 2022, n° SAN-2022-021, publié et CNIL, FR, 12 octobre 2023, n° SAN-2023-015).

114. La rapporteure considère que les mots de passe permettant l'accès au back-office de la société sont stockés dans un fichier où ils sont hachés avec la fonction algorithmique MD5, considérée comme étant obsolète. En outre, elle affirme que l'accès aux bases de données de la société se fait via un unique compte utilisateur dont les identifiants sont connus par deux personnes.

115. La société considère qu'aucun élément ne permet d'affirmer que les accès aux bases de données étaient rendus possibles via le back-office. Elle précise que le stockage des mots de passe en MD5 concerne les personnes ayant accès au back-office. La société estime que, dès lors que le back-office ne permettait pas d'accéder à des données à caractère personnel, l'article 32 du RGPD n'est pas applicable au cas d'espèce.

116. En outre, elle affirme que le compte MySQL programmatique est un compte accessible via un identifiant et un mot de passe, et qui est destiné à être utilisé par l'ensemble des scripts PHP, c'est-à-dire des listes de commandes ou d'instruction utilisant le langage de programmation PHP, ayant besoin d'accéder à la base de données. L'accès à ces identifiants est protégé, ceux-ci n'étant accessibles que via une connexion préalable de l'un deux administrateurs. Elle conclut donc que les mesures permettant d'assurer la traçabilité relative aux connexions sur ce compte sont suffisantes.

117. En premier lieu, la formation restreinte rappelle qu'en ce qui concerne la sécurité des mots de passe, la fonction de hachage MD5 présente 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. Dans la mesure où, de manière générale, un grand nombre d'internautes utilise le même mot de passe pour s'authentifier à leurs différents comptes en ligne, des attaquants pourraient exploiter les données compromises pour multiplier les intru-sions sur leurs autres comptes aux fins d'effectuer par exemple des vols ou des escroqueries. La formation restreinte a déjà eu l'occasion de rappeler que le recours à la fonction de hachage MD5 par la société n'est plus considérée depuis 2004 comme à l'état de l'art et son utilisation en cryptographie ou en sécurité est proscrite. Ainsi, l'utilisation de cet algorithme permettrait à une personne ayant connaissance du mot de passe haché de déchiffrer celui-ci sans difficulté en un temps très court (par exemple, au moyen de sites internet librement accessibles qui permettent de retrouver la valeur correspondante au hash du mot de passe) (délibération SAN-2021-008 du 14 juin 2021).

118. La formation considère que les éléments du dossier ne permettent pas d'établir que le back-office permet d'accéder à des données à caractère personnel. Elle note toutefois que, dans l'hypothèse où les mots de passe permettant d'accéder au back-office et ceux permettant d'accéder à la base de données seraient stockés selon les même procédés, l'algorithme de hachage MD5 est considéré comme étant obsolète, il ne permettrait pas d'assurer la sécurité des données à caractère personnel.

119. En second lieu, la formation restreinte relève que l'accès à la base de données se fait par le biais d'un compte programmatique. Or, quand bien même les identifiants de ce compte sont partagés entre deux individus, l'accès restreint au compte programmatique à un nombre limité d'adresses IP permet effectivement d'assurer la traçabilité des connexions.

120. Par conséquent, la formation restreinte considère que le manquement à l'article 32 du RGPD n'est pas caractérisé.

III. SUR LES MESURES CORRECTRICES ET LEUR PUBLICITÉ

121. Aux termes de l'article 20-IV de la loi n° 78-17 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 […] saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […]

7° À l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83 .

122. L'article 83 du RGPD prévoit en outre 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.

123. Enfin, l'article 22, alinéa 2 de la loi Informatique et Libertés dispose que la formation restreinte peut rendre publique les mesures qu'elle prend .

124. La rapporteure propose à la formation restreinte de prononcer à l'encontre de la société une amende administrative au regard des manquements aux articles 5, paragraphe 1, e), 6 et 32 du RGPD et à l'article L. 34-5 du CPCE. Elle propose que la délibération de la formation restreinte soit rendue publique.

125. En défense, la société considère qu'elle a accordé tout au long de son activité une attention particulière à la conformité au RGPD. Elle affirme que le manquement relatif à la sécurité des données n'est pas caractérisé et que, s'agissant des autres manquements, il ne peut pas lui être reproché l'absence de conformité à des nouvelles exigences imposées par la CNIL.

126. Dans l'hypothèse où la formation restreinte déciderait du prononcé d'une amende, la société considère que le montant proposé par la rapporteure doit faire l'objet, a minima, d'une baisse significative. Elle précise que les éléments financiers à prendre en compte pour apprécier le montant de l'amende doivent être appréciés au moment où la décision d'imposer une amende est prise et non au moment de la violation. La formation restreinte doit donc prendre en compte l'exercice de l'année 2023, sachant que le chiffre d'affaires pour cette année s'élève à […] euros pour un résultat net déficitaire de […] euros. Elle affirme que sa situation économique l'a poussée à cesser son activité. Pour l'année 2024, la société a réalisé un chiffre d'affaire de […] euros pour un résultat net déficitaire de […] euros

127. Enfin, la société ne s'oppose pas à la publicité de la sanction.

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

128. A titre liminaire, la formation restreinte rappelle que l'exigence de motivation d'une sanction administrative n'impose pas à la formation restreinte de se prononcer sur l'ensemble des critères prévus à l'article 83 du RGPD, et qu'elle n'implique pas non plus que soient indiqués les éléments chiffrés relatifs au mode de détermination du montant de la sanction proposée ou prononcée (CE, 10e/9e ch., 19 juin 2020, n° 430810 ; CE, 10e/9e ch., 14 mai 2024, n° 472221). En outre, si les lignes directrices adoptées par le Comité européen de la protection des données ont pour ambition de fixer des montants de départ harmonisés et des orientations communes sur la base desquelles les amendes administratives peuvent être calculées, les autorités de contrôle ne sont aucunement tenues d'en observer toutes les étapes si ces dernières ne trouvent pas application dans un cas donné, ni d'exposer les motivations ayant trait aux aspects des lignes directrices qui sont sans objet. Cependant, le raisonnement devrait inclure au minimum les facteurs qui ont permis de déterminer le degré de gravité, le chiffre d'affaires appliqué ainsi que les facteurs aggravants ou atténuants qui ont été pris en considération .

129. Ceci étant rappelé, la formation restreinte considère qu'il convient, en l'espèce, d'examiner les critères pertinents de l'article 83 du RGPD pour décider s'il y a lieu d'imposer une amende administrative à la société et, le cas échéant, pour déterminer son montant.

1) Sur le prononcé de l'amende

130. Premièrement, la formation restreinte considère qu'il y a lieu de faire application du critère prévu à l'alinéa a) de l'article 83, paragraphe 2 du RGPD relatif à la nature, à la gravité et à la durée de la violation, compte tenu de la nature, de la portée du traitement et du nombre de personnes concernées et du niveau de dommage qu'elles ont subi.

131. La formation restreinte relève tout d'abord que les manquements aux articles 5, paragraphe 1, e) et 6 du RGPD concernent les principes fondamentaux de la protection des données et sont susceptibles d'être sanctionnés par l'amende la plus élevée prévue par le législateur européen, soit 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % de son chiffre d'affaires. A titre d'éclairage, les lignes directrices sur l'application et la fixation des amendes administratives adoptées par le groupe de travail article 29 (désormais, le CEPD) le 3 octobre 2017 soulignent qu'en fixant deux montants maximaux différents pour l'amende administrative (10 et 20 millions d'euros), le règlement indique déjà que la violation de certaines dispositions du règlement peut être plus grave que celle d'autres dispositions .

132. La formation restreinte souligne que ces manquements concernent les principes de base d'un traitement et ont trait notamment à sa licéité, certaines des opérations de prospection commerciale réalisées intervenant sans base légale valable (la société ne disposant pas du consentement des personnes concernées pour les démarcher par voie électronique et ne pouvant se fonder sur la base légale de l'intérêt légitime pour transmettre à ses partenaires les données de prospects à des fins de prospection par voie électronique). La formation restreinte insiste en outre sur le nombre particulièrement élevé de personnes dont la société traite les données de plus de 2,8 millions de prospects.

133. S'agissant plus particulièrement du manquement à l'article L. 34-5 du CPCE, la formation restreinte entend souligner sa particulière gravité dans la mesure où il a été constaté que les formulaires transmis par la société ne permettaient pas de recueillir un consentement valable des personnes concernées. Ces constats attestent du caractère systémique et non isolé du manquement, étant précisé que les formulaires examinés proviennent de deux des trois plus gros fournisseurs de données de la société. En outre, la formation restreinte entend insister sur le nombre de personnes concernées par le manquement, la société ayant indiqué avoir adressé 6 millions de messages de prospection par voie électronique au cours de l'année 2022.

134. Deuxièmement, la formation restreinte estime qu'il convient de tenir compte du critère prévu à l'article 83, paragraphe 2, b) du RGPD, relatif au fait que la violation ait été commise délibérément ou par négligence.

135. Ainsi qu'il a déjà été rappelé, la formation restreinte souligne que les règles relatives à la prospection commerciale sont définies depuis de nombreuses années et que la société était parfaitement consciente que pour réaliser ses opérations de prospection par voie électronique, elle devait disposer d'un consentement valable. La formation restreinte relève à cet égard que la société a mis en place, dès 2014, des procédures visant à réaliser des audits de ses fournisseurs et à vérifier la validité du consentement recueilli. Malgré ces vérifications, la société n'a pas pris les mesures propres à assurer sa mise en conformité. Au contraire, la société a continué à exploiter les données transmises. La formation restreinte considère qu'en s'affranchissant du respect de ces règles, la société s'est montrée, à tout le moins, fortement négligente.

136. Troisièmement, la formation restreinte entend tenir compte de certaines autres circonstances applicable aux faits de l'espèce, en application de l'article 83, paragraphe 2, k) du RGPD.

137. La formation restreinte considère notamment que la société a tiré des violations commises un avantage financier certain, dans la mesure où elle s'est vu rémunérer par ses clients pour la fourniture des données en cause.

138. La formation restreinte prend toutefois bonne note que la société a cessé son activité.

139. La formation restreinte considère que l'ensemble de ces éléments justifient le prononcé d'une amende administrative.

2) sur le montant de l'amende

140. La formation restreinte rappelle que les violations relevées sont susceptibles de faire l'objet, en vertu de l'article 83 du RGPD, d'une amende administrative pouvant s'élever jusqu'à 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaires annuel mondial de l'exercice précédent, le montant le plus élevé étant retenu.

141. Elle considère que l'activité de la société et sa situation financière doivent notamment être prises en compte. Elle relève à cet égard que l'activité de la société CALOGA a cessé. Pour l'année 2023, la société a réalisé un chiffre d'affaire de […] euros pour un résultat net déficitaire de […] euros. Pour l'année 2024, la société a réalisé un chiffre d'affaire de […] euros pour un résultat net déficitaire de […] euros.

142. 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 quatre-vingt mille (80 000) euros apparaît justifiée

B. Sur la publicité de la sanction

143. La formation restreinte considère qu'une telle mesure se justifie au regard de la gravité des manquements en cause, de la position de la société sur le marché ainsi que du nombre de personnes concernées, lesquelles se doivent d'être informées.

144. Elle relève également que cette mesure a notamment vocation à informer les personnes concernées par les traitements mis en œuvre par la société, ainsi que les sociétés partenaires. S'agissant des prospects, cette information leur permettra, le cas échéant, de faire valoir leurs droits.

145. Elle estime en outre que cette mesure apparait proportionnée dès lors que la décision n'identifiera plus nommément la société à l'issue 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 CALOGA d'un montant de quatre-vingt mille (80 000) euros** pour manquements aux articles 5, paragraphe 1, e) et 6 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et L. 34-5 du code des postes et 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

Philippe-Pierre CABOURDIN

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.