Délibération SAN-2022-017 du 3 août 2022

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Etat juridique : En vigueur

Date de publication sur Légifrance : Vendredi 19 août 2022

Délibération de la formation restreinte n° SAN-2022-017 du 3 août 2022 concernant la société ACCOR SA

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

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

Vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

Vu le code des postes et des communications électroniques ;

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

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

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

Vu les saisines nos […] ;

Vu la décision n° 2019-046C du 18 février 2019 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par la société ACCOR ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 16 octobre 2020 ;

Vu le rapport de Madame Sophie LAMBREMON, commissaire rapporteur, notifié à la société ACCOR le 24 novembre 2020 ;

Vu les observations écrites versées par la société ACCOR le 22 décembre 2020 ;

Vu les autres pièces du dossier ;

Vu la décision 01/2022 concernant le litige relatif au projet de décision de l'autorité de contrôle française concernant Accor SA en application de l'article 65, paragraphe 1, point a), du RGPD ;

Étaient présents, lors de la séance de la formation restreinte du 28 janvier 2021 :

- Madame Sophie LAMBREMON, commissaire, entendue en son rapport ;

En qualité de représentants de la société ACCOR :

[…]

La société ACCOR ayant eu la parole en dernier ;

La formation restreinte a adopté le projet de décision suivant :

I. Faits et procédure

1. La société ACCOR SA (ci-après " la société ") est une société anonyme à conseil d'administration créée en 1960, spécialisée dans le secteur de l'hôtellerie. Son siège social est situé 82, rue Henri Farman à Issy-les-Moulineaux (92130).

2. En 2021, la société a réalisé un chiffre d'affaires de […]. À l'été 2020, 5100 hôtels, implantés dans 110 pays, sous 39 marques différentes, étaient exploités dans le cadre de contrats liant leurs propriétaires à la société ACCOR (contrats de franchise ou de " management ", principalement). La société emploie environ 1500 salariés.

3. Entre décembre 2018 et septembre 2019, la Commission nationale de l'informatique et des libertés (ci-après " la CNIL " ou " la Commission ") a été directement saisie de cinq plaintes (saisines nos […]) portant sur l'absence de prise en compte du droit d'opposition à la réception par courriel de messages de prospection commerciale (courriels publicitaires, courriels de bienvenue au programme de fidélité, newsletters) de la part de la société. Le 22 septembre 2019, la CNIL a en outre reçu une plainte (saisine n° […]) relative aux difficultés rencontrées dans le cadre de l'exercice du droit d'accès notamment à des données bancaires collectées par la société à l'occasion de la réservation d'une chambre d'hôtel.

4. Conformément à l'article 56 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après " le Règlement " ou " le RGPD "), dans le cadre du traitement des plaintes reçues à l'encontre de la société, la CNIL a informé, le 12 décembre 2018, l'ensemble des autorités de contrôle européennes de sa compétence pour agir en tant qu'autorité de contrôle chef de file concernant les traitements transfrontaliers mis en œuvre par la société, compétence tirée par la CNIL de ce que l'établissement principal de la société se trouve en France.

5. Par le biais de la plateforme d'échange entre autorités de protection des données européennes, la CNIL a engagé la procédure permettant aux autorités de contrôle concernées de se déclarer. Dix autorités se sont déclarées concernées par cette procédure, au sens de l'article 4 (22) du RGPD.

6. Parallèlement, entre janvier 2019 et février 2020, la CNIL a été rendue destinataire, en qualité " d'autorité chef de file ", en application des mécanismes de coopération prévus par le Règlement, de cinq autres plaintes reçues respectivement par les autorités de contrôle de la Sarre, de l'Espagne, de l'Irlande, de la Pologne et de la Basse Saxe (saisines nos […]). Ces plaintes portaient également sur des demandes d'opposition au traitement de données personnelles à des fins de prospection commerciale par courriel et à l'exercice du droit d'accès à des données collectées par la société ACCOR.

7. Le 6 mars 2019, en application de la décision n° 2019-046C du 18 février 2019 de la présidente de la CNIL, un questionnaire a été adressé à la société ACCOR, auquel cette dernière a répondu par courrier du 8 avril puis par des courriers complémentaires des 22 mai, 1er août, 11 octobre et 27 décembre 2019. Cette mission de contrôle sur pièces a eu pour objet de vérifier le respect par la société ACCOR de l'ensemble des dispositions du RGPD et de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après " la loi du 6 janvier 1978 modifiée " ou la loi " Informatique et Libertés ").

8. À la suite de ce premier contrôle, la CNIL, tenant compte de la réponse apportée par la société au courrier d'instruction qui lui avait été adressé et de sa mise en conformité sur plusieurs points, a soumis à ses homologues européens, le 23 décembre 2019, en application de l'article 60 du RGPD, un projet de décision de sa présidente rappelant la société à ses obligations, conformément aux dispositions de l'article 58.2.b) du RGPD.

9. Ce projet de décision a fait l'objet de la part de certaines autorités concernées d'objections pertinentes et motivées au sens de l'article 60 du RGPD, demandant que la société ne fasse pas seulement l'objet d'un rappel à l'ordre mais qu'elle soit sanctionnée par une amende administrative et soulignant, notamment, le nombre de manquements, le nombre de plaintes et la taille de la société. Compte tenu de ces objections et des nouvelles plaintes reçues depuis le premier contrôle, la CNIL a décidé de reprendre ses investigations auprès de la société.

10. Le 11 février 2020, la délégation de la CNIL a procédé à une mission de contrôle dans les locaux de la société. Un contrôle en ligne du site web de la société (www.all.accor.com) a ensuite été réalisé le 24 février 2020, en application de la décision n° 2019-046C précitée. À la suite de ces investigations, la société a adressé à la CNIL des éléments complémentaires par courriers en date des 21 février, 10 mars, 19 mars et 7 août 2020.

11. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 16 octobre 2020, désigné Madame Sophie LAMBREMON en qualité de rapporteure, sur le fondement de l'article 22 de la loi du 6 janvier 1978 modifiée.

12. À l'issue de son instruction, la rapporteure a fait notifier à la société, le 24 novembre 2020, un rapport détaillant les manquements aux dispositions des articles L. 34-5 du code des postes et des communications électroniques (ci-après le " CPCE ") et 12-1, 12-3, 13, 15-1, 21-2 et 32 du RGPD qu'elle estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de la Commission de prononcer à l'encontre de la société une amende administrative et que cette décision soit rendue publique mais ne permette plus d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

13. Était également jointe au rapport une convocation à la séance de la formation restreinte du 28 janvier 2021 indiquant à la société qu'elle disposait d'un délai d'un mois pour communiquer ses observations écrites en application des dispositions de l'article 40 du décret n° 2019-536 du 29 mai 2019.

14. La société ACCOR a répondu au rapport de sanction par des observations écrites en date du 22 décembre 2020.

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

II. Motifs de la décision

A. Sur la procédure de coopération européenne

16. Aux termes de l'article 56, paragraphe 1, du Règlement " l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60 ".

17. En l'espèce, la formation restreinte relève, d'abord, que le siège social de la société se trouve en France depuis la création de l'entreprise en 1983 et que la société est immatriculée au registre du commerce et des sociétés en France depuis l'origine.

18. La formation restreinte relève, ensuite, que les premiers hôtels du groupe ACCOR étaient implantés en France, la société ayant lancé son activité à l'étranger seulement dans un second temps.

19. Enfin, à ce jour, bien que les hôtels du groupe ACCOR soient implantés dans 110 pays à travers le monde, plus de la moitié des hôtels exploités sous la marque " AccorHotels " en Europe se situent en France (1657 hôtels sur les 3051 présents dans l'Union européenne).

20. L'ensemble de ces éléments concourent à considérer que l'établissement principal de la société se trouve en France et que la CNIL est compétente pour agir en tant qu'autorité de contrôle chef de file concernant les traitements transfrontaliers effectués par cette société, conformément à l'article 56, paragraphe 1, du Règlement.

21. La formation restreinte relève qu'à la date du présent projet de décision les autorités de contrôle des pays suivants étaient concernées par la présente procédure : Allemagne, Autriche, Belgique, Bulgarie, Croatie, Danemark, Espagne, Estonie, Grèce, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Suède et République tchèque.

22. À l'issue d'une procédure contradictoire, un projet de décision a été adopté par la formation restreinte et a été transmis aux autres autorités de contrôle européennes concernées en application de l'article 60, paragraphe 3, du RGPD.

23. Le 28 mai 2021, l'autorité polonaise de protection des données a formulé trois objections, conformément à l'article 60, paragraphe 4, du RGPD.

24. Par la délibération n° SAN-2022-001 du 13 janvier 2022, la formation restreinte a exposé son point de vue sur les objections de l'autorité polonaise et expliqué les motifs pour lesquels elle a décidé de ne pas suivre ces objections.

25. Le 15 juin 2022, le Comité européen de protection des données (ci-après " CEPD ") a adopté la décision 01/2022 concernant le litige relatif au projet de décision de l'autorité de contrôle française concernant Accor SA en application de l'article 65, paragraphe 1, point a), du RGPD. Par cette décision, le CEPD s'est prononcé sur le litige relatif au projet de décision qui ne portait plus que sur une seule objection de l'autorité polonaise, concernant le montant de l'amende fixé dans le projet de décision.

B. Sur le manquement relatif à l'obligation de recueillir le consentement de la personne concernée par une opération de prospection directe au moyen d'un système automatisé de communications électroniques en application de l'article L. 34-5 du CPCE

1. Sur l'absence de consentement des personnes à la réception de messages de prospection commerciale de la société ACCOR

26. L'article L. 34-5 du CPCE dispose : " Est interdite la prospection directe au moyen de système automatisé de communications électroniques au sens du 6° de l'article L. 32, 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.

Toutefois, la prospection directe par courrier électronique est autorisée si les coordonnées du destinataire ont été recueillies auprès de lui, dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'occasion d'une vente ou d'une prestation de services, si la prospection directe concerne des produits ou services analogues fournis par la même personne physique ou morale, et si le destinataire se voit offrir, de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais, hormis ceux liés à la transmission du refus, et de manière simple, à l'utilisation de ses coordonnées au moment où elles sont recueillies et chaque fois qu'un courrier électronique de prospection lui est adressé au cas où il n'aurait pas refusé d'emblée une telle exploitation.

[…] ".

Aux termes de l'alinéa 6 du même article, " La Commission nationale de l'informatique et des libertés veille, pour ce qui concerne la prospection directe utilisant les coordonnées d'un abonné ou d'une personne physique, au respect des dispositions du présent article en utilisant les compétences qui lui sont reconnues par la loi n° 78-17 du 6 janvier 1978 précitée. A cette fin, elle peut notamment recevoir, par tous moyens, les plaintes relatives aux manquements aux dispositions du présent article […] ".

27. Il ressort des investigations réalisées par la CNIL que, lorsqu'une personne réservait une chambre d'hôtel directement auprès du personnel d'un hôtel d'une des marques hôtelières du groupe ACCOR (sur place ou par téléphone) ou sur le site d'une des marques hôtelières du groupe (Ibis, Novotel, Mercure, Fairmont, Sofitel, Adagio etc.), elle était rendue destinataire des courriels de la société contenant la newsletter " All – Accor Live Limitless ", la case relative au consentement à recevoir la newsletter étant pré-cochée par défaut.

28. La rapporteure estime que, dans ces hypothèses, le consentement des personnes destinataires des courriels électroniques de la société contenant la newsletter " All – Accor Live Limitless " n'était pas valablement recueilli. Elle relève notamment à cet égard que les offres commerciales et promotionnelles présentes dans la newsletter " All – Accor Live Limitless " ne portent pas uniquement sur des services fournis par la société mais portent également sur les services de sociétés " partenaires " – telles que, par exemple, des compagnies aériennes ou de sociétés gestionnaires de parcs de stationnement.

29. Dans ces conditions, la rapporteure considère que la société ne peut pas se prévaloir de l'exception prévue à l'article L. 34-5 alinéa 4 du CPCE, qui prévoit qu'un organisme peut adresser des messages de prospection commerciale par courrier électronique sans recueillir préalablement le consentement des personnes concernées lorsque les données ont été collectées auprès de ces personnes à l'occasion d'une vente ou d'une prestation de services et que la prospection commerciale concerne des produits ou services analogues fournis par la même personne physique ou morale.

30. La société soutient que c'est bien elle qui collecte dans tous les cas les données auprès des personnes concernées car, d'une part, elle édite et gère tous les sites de réservation de toutes les marques du groupe et, d'autre part, même lorsqu'ils sont utilisés par les personnels des hôtels du groupe à la demande de clients, les outils de réservation et d'adhésion au programme de fidélité sont gérés par elle seule et viennent alimenter sa propre base de données.

31. La formation restreinte prend acte de ce que la société est détentrice des sites de réservation de toutes les marques du groupe (Ibis, Novotel, etc.). La formation restreinte relève néanmoins que les messages de prospection commerciale adressés par la société ne portent pas exclusivement sur des produits ou services analogues fournis par cette société mais qu'ils sont susceptibles de contenir par exemple des offres promotionnelles de partenaires, telle que des compagnies aériennes ou des sociétés gestionnaires de parcs de stationnement.

32. Dans ces conditions, la formation restreinte considère que la société était tenue de recueillir le consentement préalable, libre, spécifique et informé des personnes à recevoir des messages de prospection directe par courrier électronique, conformément à l'alinéa 1er de l'article L. 34-5 du CPCE, ce que ne permettait pas l'existence, en l'espèce, d'une case relative au consentement à recevoir la newsletter pré-cochée par défaut. La formation restreinte rappelle que dans son arrêt Planet49 du 1er octobre 2019 (affaire C-673/19), la Cour de justice de l'Union européenne a indiqué qu'un consentement recueilli au moyen d'une case pré-cochée ne peut pas être considéré comme valablement donné par l'utilisateur.

33. Dans le cadre de la procédure, la société a justifié avoir pris des mesures pour mettre en conformité l'ensemble de ses outils de collecte du consentement des personnes concernées à recevoir des messages de prospection commerciale par courriel électronique, afin que pour chacun des parcours de réservation et d'adhésion au programme ce consentement ne soit plus recueilli par défaut.

34. La formation restreinte considère par conséquent que le manquement à l'article L. 34-5 du CPCE est constitué, mais que la société s'est mise en conformité à la date de clôture de l'instruction.

2. Sur l'absence de consentement des personnes créant un espace client, à la réception des messages de prospection commerciale

35. Dans le cadre de l'instruction, la délégation de contrôle de la CNIL a constaté que, lors de la création d'un espace client, la société ne recueillait pas le consentement des personnes pour le traitement de leurs données à caractère personnel à des fins de prospection commerciale par courriers électroniques. En effet, il a été constaté que les données à caractère personnel utilisées par la société à des fins de prospection commerciale pouvaient être collectées depuis un formulaire de création d'un espace client, indépendamment d'une réservation, sur lequel figurait une case " pré-cochée " par défaut portant sur le consentement à recevoir de la prospection commerciale.

36. La formation restreinte considère que la société est tenue de recueillir le consentement préalable, libre, spécifique et informé des personnes créant un espace client sur son site web, à recevoir des messages de prospection directe par courriers électroniques, conformément à l'alinéa 1 de l'article L. 34-5 du CPCE. En effet, dans la mesure où la création d'un espace client peut intervenir sans réservation préalable, l'exemption au recueil du consentement prévue à l'article L. 34-5 lorsque sont proposés des services analogues n'est pas mobilisable dans ce cas de figure.

37. En réponse, la société a justifié avoir modifié son formulaire de création d'un espace client, afin que le consentement des personnes concernées à recevoir des messages de prospection ne soit plus recueilli par défaut.

38. Dans ces conditions, la formation restreinte considère que le manquement à l'article L. 34-5 du CPCE est constitué, mais que la société s'est mise en conformité à la date de clôture de l'instruction.

C. Sur le manquement relatif à l'obligation d'informer les personnes en application des articles 12 et 13 du RGPD

39. Aux termes de l'alinéa 1 de l'article 12 du RGPD : " Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples […] ".

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

41. En premier lieu, s'agissant du caractère accessible de l'information, la délégation a constaté lors du contrôle en ligne du 24 février 2020 que les formulaires permettant la création d'un compte client ou l'adhésion au programme de fidélité

du groupe ACCOR ne comportaient pas les informations exigées par l'article 13 du RGPD. Les personnes n'étaient pas non plus invitées à effectuer une quelconque démarche pour prendre connaissance de l'information fournie au titre de l'article 13 du RGPD, par exemple en accédant par le biais d'un lien hypertexte à la " charte de protection des données personnelles " de la société.

42. La formation restreinte rappelle que pour considérer qu'un responsable de traitement satisfait à son obligation de transparence, il convient notamment que l'information fournie soit " aisément accessible " pour les personnes concernées au sens de l'article 12 du Règlement.

43. Elle relève, à cet égard, que cette disposition doit être interprétée à la lumière du considérant 61 du Règlement, aux termes duquel : " les informations sur le traitement des données à caractère personnel relatives à la personne concernée devraient lui être fournies au moment où ces données sont collectées auprès d'elle ". En ce sens, elle partage la position du G29 présentée dans les lignes directrices sur la transparence au sens du Règlement, adoptées dans leur version révisée le 11 avril 2018 et endossées le 25 mai 2018 par le Comité européen de protection des données (CEPD) qui rappelle que " la personne concernée ne devrait pas avoir à rechercher les informations mais devrait pouvoir tout de suite y accéder ".

44. La formation restreinte considère qu'en l'espèce les mentions d'information des personnes concernées n'étaient pas " aisément accessibles " pour ces dernières, en ce que, lors de la création d'un compte, l'accès à la " charte de protection des données personnelles " de la société n'était organisé que via un lien hypertexte disponible tout en bas des pages du site internet, ce qui nécessitait que l'internaute fasse défiler la page dans son intégralité et recherche l'information, en méconnaissance de l'article 12 du RGPD.

45. Dans le cadre de l'instruction, la société a indiqué avoir procédé à des rectifications, afin de délivrer une information conforme aux exigences du RGPD. Par une vérification informelle, il a en effet été constaté que les mentions d'informations relatives au traitement des données personnelles avaient été complétées sur les formulaires de création de compte et d'adhésion au programme de fidélité et que la " charte de protection des données personnelles des clients " était désormais directement accessible à partir d'un lien inséré sur ces formulaires.

46. En second lieu, la délégation de contrôle a constaté que la " charte de protection des données personnelles des clients " de la société précise que la base légale du traitement des données personnelles en lien avec l'envoi de prospections commerciales est " l'intérêt légitime " ou " l'exécution d'un contrat ".

47. Or, la rapporteure soutient que, dans les hypothèses précédemment mentionnées, pour l'envoi de messages de prospection relatifs aux produits ou services de tiers, la société ne peut se dispenser de recueillir le consentement des personnes concernées à recevoir des messages de prospection commerciale.

48. En réponse, la société indique que, même si le consentement des personnes concernées doit être recueilli en vertu des dispositions de l'article L. 34-5 du CPCE, les traitements mis en œuvre aux fins de prospection commerciale ont pour base légale l'intérêt légitime.

49. Ainsi qu'il a été précédemment exposé, la formation restreinte considère que dans certaines hypothèses la société est tenue de recueillir le consentement préalable, libre, spécifique et informé des personnes concernées à recevoir des messages de prospection directe par courriers électroniques, conformément aux dispositions de l'alinéa 1 de l'article L. 34-5 du CPCE.

50. La formation restreinte estime que lorsque le recueil du consentement de la personne concernée s'impose pour le traitement de ses données à caractère personnel pour une finalité déterminée (et non seulement pour une opération donnée), la base légale du traitement ainsi mis en œuvre est le consentement.

51. Par conséquent, la formation restreinte relève qu'en ne mentionnant pas le consentement comme base légale du traitement, pour la prospection tendant à promouvoir les produits ou services de tiers, la société a méconnu son obligation au titre de l'article 13 du RGPD.

52. La formation restreinte considère dès lors que l'ensemble de ces faits constituent des manquements aux articles 12 et 13 du RGPD.

D. Sur le manquement relatif à l'obligation de respecter le droit d'accès des personnes en application de l'article 15 du RGPD

53. L'article 15.1 du RGPD prévoit un droit d'accès de la personne concernée à ses données à caractère personnel en ces termes : " La personne concernée a le droit d'obtenir du responsable de traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel (…) ".

54. L'article 12.3 du RGPD précise en outre que " le responsable du traitement fournit à la personne concernée des informations sur les mesures prises à la suite d'une demande formulée en application des articles 15 à 22, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande ".

55. Lors de l'instruction de la réclamation n° […] reçue par la CNIL, il est apparu que la société a manqué à son obligation de fournir à la plaignante, dans le délai imparti par le RGPD, une copie de ses données à caractère personnel qu'elle détenait dans sa base de données.

56. La rapporteure relève que l'auteure de la réclamation a formulé une demande de droit d'accès le 1er août 2019, date à laquelle son compte client avait fait l'objet d'une suspension à la suite d'une détection de connexion frauduleuse. Toutefois, alors que la plaignante avait justifié de son identité le 10 janvier 2020, permettant ainsi la réouverture de son compte client par la société, aucune réponse n'avait encore été fournie à sa demande de droit d'accès à la date du contrôle de la délégation de la CNIL, le 11 février 2020. La société a fait droit à la demande de la plaignante le 24 février 2020.

57. La formation restreinte considère, que dans l'hypothèse où le compte d'un client a fait l'objet d'une détection de connexion frauduleuse, la société peut certes avoir un doute raisonnable sur l'identité du demandeur souhaitant exercer son droit d'accès, justifiant qu'une pièce d'identité soit sollicitée auprès de la personne concernée.

58. La formation restreinte estime toutefois que, dès lors que le doute est levé sur l'identité de la personne, la demande de droit d'accès doit être honorée par le responsable du traitement.

59. Dans ces conditions, la formation restreinte considère que le manquement à l'article 15 du RGPD est constitué s'agissant de la plainte n° […], bien qu'il ne ressorte pas du dossier qu'au-delà de cette plainte ponctuelle le manquement ait eu un caractère structurel.

E. Sur le manquement relatif à l'obligation de respecter le droit d'opposition des personnes en application de l'article 21 du RGPD

60. Aux termes de l'article 21.2 du RGPD : " lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection ".

61. En premier lieu, la rapporteure a relevé que l'auteur de la plainte n° […] s'est opposé à la réception de messages de prospection de la part de la société sur ses deux adresses de messagerie électronique, le 11 décembre 2018.

62. La rapporteure a considéré que la société n'avait pas répondu de manière satisfaisante à la demande d'opposition du plaignant, dès lors que sa demande d'opposition n'a été prise en compte que le 11 janvier 2020 et pour une seule des deux adresses électroniques concernées.

63. En réponse, la société a indiqué ne pas avoir trouvé trace de cette demande d'opposition dans ses systèmes. Elle indique en outre ne pas avoir retrouvé non plus dans sa base de données la première adresse électronique visée par le plaignant dans sa demande et précise, s'agissant de la seconde adresse électronique, que c'est l'auteur de la plainte lui-même qui s'est désinscrit des newsletters le 11 janvier 2020.

64. La formation restreinte considère que, s'agissant de cette première plainte, les éléments du débat ne permettent pas de conclure à l'existence d'un manquement commis par la société.

65. En second lieu, l'instruction des plaintes n° […] reçues par la CNIL a révélé l'existence de dysfonctionnements du lien de désinscription figurant en bas des courriels de prospection adressés par la société, résultant de deux types de problèmes techniques affectant l'une ou l'autre des étapes du processus de désabonnement.

66. D'abord, entre le 11 novembre 2018 et le 21 janvier 2019, des dysfonctionnements sont intervenus dans la transmission d'informations relatives aux désabonnements entre l'outil permettant de gérer l'envoi des newsletters et le référentiel clients, qui consigne l'information selon laquelle un client est, ou non, abonné aux newsletters. Ainsi, pendant cette période, l'outil de gestion des newsletters n'était pas informé par le référentiel clients des créations ou mises à jour de contacts et des désabonnements aux newsletters associés réalisés tous les dimanches entre 0 h et 20 h. Dès lors, jusqu'au 21 janvier 2019, l'auteur de la réclamation n°[…] a continué à recevoir des messages de prospection commerciale de la part de la société, malgré sa demande de désabonnement formulée le dimanche 18 novembre 2018 dans l'après-midi.

67. Ensuite, une autre anomalie, affectant également la synchronisation des désabonnements entre le référentiel clients et l'outil qui gère l'envoi des newsletters, a été identifiée par la société le 8 février 2019. Cette anomalie explique que l'auteure de la réclamation n° […] ait continué à recevoir la newsletter de la société ACCOR entre le 2 janvier 2019 et le 8 février 2019, malgré la suppression de ses données au sein du référentiel clients dès le 1er janvier 2019.

68. La formation restreinte considère que ces deux anomalies, qui se sont reproduites pendant plusieurs semaines, sont susceptibles d'avoir empêché un nombre significatif de personnes de s'opposer efficacement à la réception des messages de prospection. Elle relève à cet égard qu'il ressort des pièces du dossier qu'en 2019, […] millions de personnes recevaient sur une adresse électronique valide au moins l'une des newsletters du groupe ACCOR.

69. En réponse, la société indique avoir pris des mesures visant à améliorer la gestion des demandes d'exercice des droits et à prévenir les anomalies dans la prise en compte des demandes d'opposition.

70. La formation restreinte prend acte des mesures de mise en conformité adoptées par la société, mais considère que la société a méconnu pour le passé ses obligations au titre des dispositions de l'article 21.2 du RGPD, dès lors que les anomalies précitées ont fait échec à la prise en compte dans un délai raisonnable des demandes d'opposition à recevoir des messages de prospection commerciale de la part des personnes concernées.

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

71. L'article 32 du Règlement dispose :

" 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

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

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement […]".

72. En premier lieu, la rapporteure relève que, lors du contrôle sur place du 11 février 2020, la délégation a constaté que l'utilisation d'un mot de passe composé de huit caractères contenant seulement deux types de caractères (sept lettres majuscules et un caractère spécial) permettait d'accéder à l'outil de gestion l'envoi des communications aux clients.

73. La rapporteure estime que, compte tenu notamment du volume de données à caractère personnel traité par l'outil " Adobe Campaign ", les exigences mises en place par la société en matière de robustesse des mots de passe sont insuffisantes et ne permettent pas d'assurer la sécurité des données à caractère personnel.

74. En réponse, la société fait valoir que, compte tenu de l'existence d'une mesure complémentaire de sécurité – tenant en ce que l'accès au logiciel " Adobe Campaign " n'est possible que depuis un terminal connecté au réseau ACCOR – un seul niveau de complexité (minuscule ou chiffre) manquait pour que le mot de passe constaté par la délégation réponde aux recommandations de la CNIL. La société justifie par ailleurs avoir renforcé les règles de complexité du mot de passe d'accès au logiciel " Adobe Campaign ", qui doit désormais comprendre un minimum de neuf caractères et quatre niveaux de complexité.

75. La formation restreinte considère que la longueur et la complexité d'un mot de passe demeurent des critères élémentaires permettant d'apprécier la force de celui-ci. Elle relève à cet égard que la nécessité d'un mot de passe fort est également soulignée par l'Agence nationale de sécurité des systèmes d'information.

76. À titre d'éclairage, la formation restreinte rappelle que pour assurer un niveau de sécurité suffisant et satisfaire aux exigences de robustesse des mots de passe, lorsqu'une authentification repose uniquement sur un identifiant et un mot de passe, la CNIL recommande, dans sa délibération n° 2017-012 du 19 janvier 2017, que le mot de passe comporte au minimum douze caractères - contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial - ou alors comporte au moins huit caractères - contenant trois de ces quatre catégories de caractères - s'il est accompagné d'une mesure complémentaire comme, par exemple, la temporisation d'accès au compte après plusieurs échecs (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (comme un " captcha ") et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses.

77. En l'espèce, la formation restreinte considère qu'au regard des règles encadrant leur composition, la robustesse des mots de passe admis par la société pour l'accès au logiciel " Adobe Campaign " était trop faible, conduisant à un risque de compromission des données à caractère personnel qu'il contient.

78. La formation restreinte relève toutefois que la société justifie avoir renforcé le niveau de complexité des mots de passe de connexion au logiciel " Adobe Campaign ".

79. En conséquence, la formation restreinte considère que le manquement relatif à l'obligation d'assurer la sécurité des données à caractère personnel est constitué, mais que la société s'est mise en conformité sur ce point avant la clôture de l'instruction.

80. En second lieu, la rapporteure a indiqué que lorsque le compte d'un client est suspendu en raison d'une suspicion de connexion frauduleuse, le service client invite la personne concernée à transmettre la copie de sa pièce d'identité en pièce jointe d'un courriel.

81. La rapporteure relève que les conditions dans lesquelles la copie de la pièce d'identité des clients dont le compte a été suspendu est transmise, ne permettent pas de se prémunir contre son interception par un tiers.

82. La formation restreinte estime que la pratique consistant en la transmission de données non chiffrées par courriel électronique génère un risque important pour la confidentialité des données transmises.

83. A cet égard, la formation restreinte rappelle que, dans son guide sur " la sécurité des données personnelles ", la CNIL recommande comme précaution élémentaire de sécurité le chiffrement des données avant leur enregistrement sur un support physique ou leur transmission par messagerie électronique. Elle recommande également d'assurer la confidentialité du mot de passe de déchiffrement en le transmettant par un autre canal.

84. Au regard de l'ensemble de ces éléments, la formation restreinte considère que les faits précités sont constitutifs d'un manquement à l'article 32 du RGPD.

III. Sur les mesures correctrices et leur publicité

85. Aux termes du III de l'article 20 de la loi du 6 janvier 1978 modifiée :

" Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […]

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

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

87. En défense, la société soutient qu'une sanction n'est pas nécessaire compte tenu de l'ensemble des mesures qu'elle a prises pour remédier aux manquements constatés et considère, en tout état de cause, que le montant de l'amende administrative proposée par la rapporteure est disproportionné eu égard, notamment, à la faible gravité des manquements, aux mesures prises pour y remédier, à sa coopération avec les services de la CNIL et à sa situation financière, sensiblement dégradée en raison de la crise sanitaire actuelle. La société soutient par ailleurs que la publicité de la décision de sanction de la formation restreinte aurait pour elle des conséquences manifestement disproportionnées.

88. S'agissant de la nature et de la gravité de la violation, la formation restreinte relève d'abord le nombre de manquements reprochés à la société : réalisation de campagnes de prospection massives par courrier électronique sans consentement des personnes, absence d'information aisément accessible et complète sur les traitements effectués, difficultés rencontrées dans le cadre de l'exercice de leurs droits par les plaignants et défauts de sécurité des données. Elle souligne que ces manquements portent sur plusieurs principes fondamentaux de la législation applicable en matière de protection des données à caractère personnel et qu'ils constituent une atteinte substantielle aux droits des personnes concernées.

89. La formation restreinte relève ensuite le nombre particulièrement important de personnes concernées par ces manquements, dès lors qu'en 2019, […] millions de personnes recevaient sur une adresse électronique valide au moins l'une des newsletters du groupe ACCOR.

90. La formation restreinte retient, enfin, que ces manquements ont eu des conséquences directes pour les personnes concernées, comme en témoigne notamment le fait que la CNIL a été saisie de onze plaintes portant en particulier sur le droit d'opposition à recevoir des messages de prospection commerciale.

91. Dès lors, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative au regard des manquements constitués.

92. S'agissant du montant de l'amende concernant les manquements au RGPD, la formation restreinte rappelle que le paragraphe 3 de l'article 83 du Règlement prévoit qu'en cas de violations multiples, comme c'est le cas en l'espèce, le montant total de l'amende ne peut excéder le montant fixé pour la violation la plus grave. Dans la mesure où il est reproché à la société un manquement aux articles 12.1, 12.3, 13, 15.1, 21.2 et 32 du Règlement, le montant maximum de l'amende pouvant être retenu s'élève à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

93. La formation restreinte relève que le chiffre d'affaires de la société s'élevait à […] d'euros en 2021.

94. S'agissant du montant de l'amende relative au manquement à l'article L.34-5 du CPCE, la formation restreinte rappelle qu'en ce qui concerne les manquements à des dispositions trouvant leur origine dans d'autres textes que le RGPD, comme c'est le cas de l'article L.34-5 du CPCE qui transpose en droit interne la directive " ePrivacy ", l'article 20, paragraphe III, de la loi " informatique et libertés " lui donne compétence pour prononcer diverses sanctions, notamment une amende administrative dont le montant maximal peut être équivalant à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent réalisé par le responsable de traitement. En outre, la détermination du montant de cette amende s'apprécie également au regard des critères précisés par l'article 83 du RGPD.

95. Pour évaluer la proportionnalité de l'amende, la formation restreinte a tenu compte de ce que la société s'est mise en conformité avec l'ensemble des manquements relevés et de ce que certains d'entre eux, en lien avec l'exercice des droits des personnes, ne revêtaient pas un caractère structurel. Elle relève en outre que la société a pleinement coopéré avec la CNIL.

96. La formation restreinte tient également compte, dans la détermination du montant de l'amende prononcée, de la situation financière de la société. À cet égard, la société fait état d'une baisse de son chiffre d'affaires en 2020 et 2021 par rapport à 2019. En effet, le chiffre d'affaires de la société s'élevait à […] en 2019, […] en 2020 et […] en 2021.

97. Enfin, la formation restreinte prend acte de la décision du CEPD n°01/2022 concernant le litige relatif au projet de décision de l'autorité de contrôle française concernant Accor SA en application de l'article 65, paragraphe 1, point a), du RGPD. En particulier, elle note que le CEPD a enjoint la CNIL de réexaminer les éléments sur lesquels elle s'est fondée pour calculer le montant de l'amende, afin de s'assurer que ladite amende satisfait au critère d'effet dissuasif prévu par l'article 83, paragraphe 1, du RGPD.

98. Dès lors, au regard du contexte économique causé par la crise sanitaire de la Covid-19, de ses conséquences sur la situation financière de la société et des critères pertinents de l'article 83, paragraphe 2, du RGPD évoqués ci-avant, la formation restreinte considère que le prononcé d'une amende administrative de 600 000 euros apparaît justifié.

99. La formation restreinte estime enfin que la publication de sa décision de sanction pour une durée de deux ans se justifie au regard de la pluralité des manquements relevés, de leur gravité et du nombre de personnes concernées.

100. La formation restreinte précise que l'amende administrative de 600 000 euros à l'encontre de la société ACCOR s'applique à hauteur de 100 000 euros pour le manquement aux dispositions de l'article L. 34-5 du CPCE et à hauteur de 500 000 euros pour les manquements de la société aux dispositions des articles 12.1, 12.3, 13, 15.1, 21.2 et 32 du Règlement.

PAR CES MOTIFS

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

• prononcer à l'encontre de la société ACCOR SA une amende administrative d'un montant de 600 000 euros pour l'ensemble des manquements constatés, qui se décompose comme suit :

- **100 000 (cent mille) euros au titre du manquement de la société à l'article L. 34-5 du Code des postes et des communications électroniques ;**
- **500 000 (cinq cent mille) euros au titre des manquements de la société aux articles 12.1, 12.3, 13, 15.1, 21.2 et 32 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.**

• rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération, qui n'identifiera plus nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

Le président

Alexandre LINDEN

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'État dans un délai de deux mois à compter de sa notification.