Délibération du 18 novembre 2020

Commission Nationale de l'Informatique et des Libertés
Nature de la délibération : Sanction
Etat juridique : En vigueur
Date de publication sur Légifrance : Jeudi 26 novembre 2020

Délibération de la formation restreinte n° SAN-2020-008 du 18 novembre 2020 concernant la société CARREFOUR FRANCE

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Messieurs Alexandre LINDEN, président, Philippe-Pierre CABOURDIN, vice-président, et de Mesdames Sylvie LEMMET et Christine MAUGÜE, membres ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

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 loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants;

Vu le code des postes et des communications électroniques ;

Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu l'ordonnance n° 2020-306 du 25 mars 2020 relative à la prorogation des délais échus pendant la période d'urgence sanitaire ;

Vu les saisines n°s 18011774, 18013824, 18018909, 18019816, 18022931, 18023308, 18023417, 18024794, 19000325, 19001602, 19001627, 19002040, 19002339, 19004654 et 19006872 ;

Vu les décisions n° 2019-081C du 24 avril 2019 et n° 2019-102C du 6 juin 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 cet organisme ou pour le compte de la société CARREFOUR et ses filiales, et notamment les sociétés CARREFOUR FRANCE, CARREFOUR SYSTÈMES D'INFORMATION, OOSHOP, CARREFOUR SERVICE CLIENTS et CARREFOUR HYPERMARCHÉS ;

Vu les observations adressées à la Commission par la société CARREFOUR le 5 décembre 2019 ;

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 10 décembre 2019 ;

Vu le rapport de Monsieur Éric PÉRÈS, commissaire rapporteur, notifié à la société CARREFOUR FRANCE le 10 janvier 2020 ;

Vu les observations écrites versées par le conseil de la société CARREFOUR FRANCE le 10 mars 2020 ;

Vu la réponse du rapporteur à ces observations notifiée par courriel le 22 avril 2020 au conseil de la société ;

Vu les observations écrites du conseil de la société CARREFOUR FRANCE reçues le 24 août 2020 ;

Vu les observations complémentaires reçues le 15 septembre 2020 ;

Vu les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 17 septembre 2020 :

- Monsieur Éric PÉRÈS, commissaire, entendu en son rapport ;

En qualité de représentants de la société CARREFOUR FRANCE :

- […] ;

- […] ;

- […] ;

- […] ;

- […] ;

- […].

La société CARREFOUR FRANCE ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La société CARREFOUR FRANCE (ci-après la société) est une filiale du groupe CARREFOUR (ci-après le groupe) sis 93 avenue de Paris à Massy (91300), intervenant dans de nombreux domaines. Son activité principale est la grande distribution, mais le groupe a diversifié ses activités, en intervenant par exemple dans le secteur bancaire et assurantiel, ainsi que comme agence de voyages ou encore vendeur spécialisé dans le commerce en ligne.

2. En 2019, le groupe CARREFOUR employait environ 360 000 salariés, avait réalisé un chiffre d'affaires d'environ 80 milliards d'euros et un résultat net ajusté, part du groupe, de 905 millions d'euros, en hausse par rapport à 2018 (804 millions d'euros). La société CARREFOUR FRANCE a réalisé, en 2019, un chiffre d'affaires d'environ 14 millions d'euros, pour un résultat net déficitaire d'environ 1,6 milliard d'euros.

3. Le groupe CARREFOUR est notamment constitué de la société mère CARREFOUR SA, qui détient la société CARREFOUR FRANCE à 99,61%. Cette dernière détient la société CARREFOUR HYPERMARCHÉS à 82% et la société CARREFOUR PROXIMITÉ FRANCE à 99%. En 2019, CARREFOUR HYPERMARCHÉS a réalisé un chiffre d'affaires de 14,3 milliards d'euros et CARREFOUR PROXIMITÉ FRANCE a réalisé un chiffre d'affaires de 636 millions d'euros.

4. Pour les besoins de son activité, la société CARREFOUR FRANCE édite notamment le site web www.carrefour.fr (ci-après le site carrefour.fr), permettant à ses clients de créer et d'accéder à un espace personnel et de passer commande.

5. Entre le 8 juin 2018 et le 6 avril 2019, la Commission a été destinataire de quinze plaintes de particuliers relatives aux sociétés du groupe CARREFOUR.

6. Sept de ces saisines (n^{os} 18018909, 18019816, 18022931, 18023308, 18023417, 19002040 et 19002339) faisaient état de prospection commerciale alors que les personnes concernées avaient préalablement exprimé leur opposition.

7. Quatre de ces saisines (n^{os} 18011774, 18013824, 19001602 et 19006872) faisaient suite à des demandes d'effacement des données auxquelles il n'avait pas été fait droit.

8. Trois de ces saisines (n^{os} 18024794, 19001627 et 19004654) faisaient suite à des demandes d'accès aux données auxquelles il n'avait pas été fait droit.

9. Une saisine (n^{o} 19000325) faisait étant d'un lien de désabonnement dans un courriel de prospection commerciale.

10. En application des décisions n^{o} 2019-081C du 24 avril 2019 et n^{o} 2019-102C du 6 juin 2019 de la présidente de la Commission, cinq contrôles ont été opérés en ligne ou dans les locaux de la société :

- un contrôle en ligne, réalisé le 24 mai 2019, relatif au site carrefour.fr et aux traitements mis en œuvre à partir de ce site ;

- un contrôle sur place, réalisé le 28 mai 2019, portant sur les traitements mis en œuvre par la société CARREFOUR FRANCE, notamment dans le cadre du programme fidélité Carrefour (ci-après le programme fidélité), ainsi que les différentes bases de données qu'elle utilisait pour la gestion de sa clientèle ;

- un contrôle sur place, réalisé les 11 et 12 juin 2019, relatif à l'exercice des droits et aux réponses apportées à plusieurs plaignants ayant saisi la CNIL d'une réclamation à l'encontre de la société ;

- un contrôle sur place, réalisé les 26 et 27 juin 2019, portant plus particulièrement sur la gestion des données à caractère personnel dans le cadre du programme fidélité ;

- un contrôle sur place, réalisé le 11 juillet 2019, relatif aux mesures de sécurité développées par CARREFOUR FRANCE pour protéger les données à caractère personnel qu'elle traite et aux violations de données intervenues.

11. Ces missions avaient pour objet de vérifier le respect, par la société, de l'ensemble des dispositions durèglement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le Règlement ou le RGPD) et dela loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après la loi du 6 janvier 1978 ou la loi informatique et libertés).

12. Différents échanges sont intervenus par courriel entre la société et la délégation de contrôle. Ces échanges concernaient la transmission de documents demandés à l'occasion des contrôles. Le 5 décembre 2019, la société a notamment fait parvenir à la délégation de contrôle des observations écrites reprenant la majorité des points relevés à l'occasion des contrôles et annonçant différentes actions visant à sa mise en conformité.

13. Aux fins d'instruction de ces éléments, la présidente de la Commission a désigné Monsieur Éric PÉRÈS en qualité de rapporteur, le 10 décembre 2019, sur le fondement de l'article 22 de la loi du 6 janvier 1978.

14. À l'issue de son instruction, le rapporteur a fait signifier par huissier de justice à la société CARREFOUR FRANCE, le 10 janvier 2020, un rapport détaillant les manquements au RGPD, à la loi informatique et libertés et au code des postes et des communications électroniques qu'il estimait constitués en l'espèce.

15. Ce rapport proposait à la formation restreinte de la Commission de prononcer une injonction de mettre en conformité le traitement avec les dispositions des articles 5, 12, 13, 15, 17, 21, 32 et 33 du Règlement et à l'article 82 de la loi informatique et libertés, assortie d'une astreinte, ainsi qu'une amende administrative. Il proposait également que cette décision soit rendue publique et ne permette plus d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

16. Le 29 janvier 2020, la société a sollicité la prolongation d'un mois du délai dans lequel elle devait répondre au rapport, le report de la séance initialement prévue le 24 mars 2020 ainsi qu'une rencontre avec le rapporteur. Le 3 février, le président de la formation restreinte a accordé la prolongation sollicitée pour une durée d'un mois. Le 6 février, le secrétaire général de la CNIL a fait droit à la demande de report de la séance au 21 avril 2020. Le même jour, le rapporteur a refusé la rencontre sollicitée par la société.

17. Le 10 mars 2020, par l'intermédiaire de son conseil, la société a produit des observations et formulé une demande pour que la séance devant la formation restreinte se tienne à huis clos.

18. Par courrier électronique du 23 mars 2020 et sur le fondement de l'article 40, alinéa 4, du décret n° 2019-536 du 29 mai 2019, le rapporteur a demandé au président de la formation restreinte un délai supplémentaire de quinze jours pour répondre aux observations de la société.

19. Par courrier du 24 mars 2020, prenant notamment acte du contexte de la crise sanitaire, le président de la formation restreinte a fait droit à la demande du rapporteur.

20. Par un courrier du même jour, la société a été informée du délai supplémentaire accordé au rapporteur et du fait qu'elle disposait, en vertu de l'alinéa 5 de l'article 40 du décret n° 2019-536 du 29 mai 2019, d'un délai d'un mois pour répondre à la réponse du rapporteur. Le courrier l'informait également du report de la séance de la formation restreinte, initialement prévue le 21 avril 2020.

21. Par courrier électronique du 7 avril 2020, le rapporteur a demandé au président de la formation restreinte un nouveau délai supplémentaire de quinze jours pour répondre aux observations de la société, qui lui a été accordé le 8 avril 2020. La société en a été informée le même jour.

22. Le rapporteur a répondu aux observations de la société le 22 avril 2020.

23. Par un courrier du même jour, le secrétaire général de la CNIL a informé la société qu'elle pouvait transmettre ses observations à la réponse du rapporteur jusqu'au 24 août 2020 en application de l'ordonnance n° 2020-306 du 25 mars 2020 relative à la prorogation des délais échus pendant la période d'urgence sanitaire.

24. Le 30 juin 2020, le président de la formation restreinte a fait droit à la demande de huis clos formulée par la société au motif que certains éléments versés aux débats étaient protégés par le secret des affaires, tel que prévu par l'article L151-1 du code du commerce.

25. Le 5 août 2020, les services de la CNIL ont notifié à la société une convocation à la séance de la formation restreinte du 17 septembre 2020.

26. Le 24 août, puis le 15 septembre, la société a produit de nouvelles observations en réponse à celles du rapporteur.

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

II. Motifs de la décision

A. Sur le manquement à l'obligation de conserver les données à caractère personnel pour une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées

28. L'article 5-1 e) du Règlement dispose que 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* .

1. Les données des clients membres du programme de fidélité et des utilisateurs du site carrefour.fr

29. D'une part, le rapporteur reproche à la société d'avoir fixé des durées de conservation excédant les durées nécessaires aux finalités des traitements. D'autre part, il reproche à la société d'avoir conservé des données à caractère personnel pendant une durée supérieure à celles prévues.

30. La société reconnaît ces points, mais rappelle qu'elle avait décidé, avant les contrôles de la CNIL, de réduire les durées de conservations de ses clients inactifs et qu'elle avait entamé les opérations de purges nécessaires au respect de ces nouvelles durées. Elle indique en outre avoir achevé l'ensemble de ces opérations durant la procédure de sanction.

31. **Sur le premier point**, la formation restreinte rappelle qu'au jour des contrôles, la société a indiqué que les données des clients fidélité étaient conservées en base active pendant quatre ans à compter de leur dernière activité (celle-ci pouvant s'entendre, selon les situations, comme la dernière transaction avec passage de la carte fidélité en caisse d'un magasin, la dernière transaction en ligne, la dernière modification de l'espace personnel sur le site web de la société ou le dernier contact avec le service client).

32. Elle rappelle que le programme fidélité établi par la société a pour but la prospection commerciale de ses adhérents, ainsi qu'il ressort des mentions d'information présentes sur le bulletin d'adhésion. La formation restreinte relève que les clients de la grande distribution, *a fortiori* ceux d'un programme fidélité , sont des clients d'habitude retournant de façon régulière dans les mêmes magasins. Dès lors, elle considère qu'un client n'ayant pas commercé avec la société pendant plusieurs années ne doit plus être considéré comme un client actif. À titre d'illustration, tant l'ancienne norme simplifiée n° 48 relative aux fichiers clients-prospects et à la vente en ligne que le récent projet de référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales recommandent que les données de clients inactifs soient conservées pendant une durée de trois ans à compter du dernier contact avec la société. Si cette durée est indicative et ne s'impose pas en tant que telle aux responsables de traitement, la formation restreinte considère qu'elle constitue une référence permettant d'apprécier une durée appropriée. En l'espèce, elle relève que cette durée est déjà conséquente dans le secteur de la grande distribution. Si les particularités des traitements mis en œuvre par la société CARREFOUR FRANCE, et notamment l'interconnexion profonde de ses bases, peuvent justifier que cette durée de trois ans ne soit pas jugée excessive, la formation restreinte estime qu'elle ne saurait être étendue jusqu'à la durée de quatre ans initialement fixée par la société. Considérant cette finalité de prospection commerciale du traitement fidélité , elle estime qu'une durée de conservation de quatre ans n'était pas strictement nécessaire à la finalité poursuivie, et donc excessive.

33. Elle relève néanmoins que la société a, avant l'engagement des procédures de contrôle, engagé un plan visant à réduire cette durée de conservation à trois ans pour l'ensemble de ses bases de données. Au regard de l'interconnexion entre les différentes bases de données de la société et de la nécessité opérationnelle de fixer une durée de conservation identique pour l'ensemble de ses données, la durée de conservation de trois ans pour les clients inactifs apparaît proportionnée à la finalité poursuivie.

34. **Sur le deuxième point**, la formation restreinte relève, tout d'abord, que la société reconnaît un retard dans la mise en œuvre de son programme d'effacement des données mais souligne les efforts importants fournis depuis l'engagement de la procédure pour se mettre en conformité. La formation restreinte note que la délégation de contrôle a constaté la présence de données concernant des clients inactifs depuis plus de quatre ans, et notamment plus de vingt-huit millions de clients membres du programme fidélité inactifs depuis cinq à dix ans. S'agissant des utilisateurs du site carrefour.fr, la formation restreinte souligne qu'étaient conservées les données de plus de 750 000 utilisateurs dont l'acte d'achat remontait de cinq à dix ans, et près de 20 000 utilisateurs dont le dernier achat remontait à plus de dix ans.

35. La formation restreinte considère donc, au vu de ces éléments, qu'un manquement à l'article 5-1-e) du RGPD est constitué.

36. La formation restreinte souligne cependant les moyens très importants, tant organisationnels que financiers, déployés par la société et constate, au jour de la séance, la conformité au Règlement des pratiques de la société. Cette dernière démontre en effet avoir mis en place un système automatisé de suppression des données de ses clients (tant du programme fidélité que du site carrefour.fr) inactifs depuis plus de trois ans.

2. Les pièces d'identité conservées dans le cadre de l'exercice des droits

37. Le rapporteur reproche à la société d'avoir conservé pendant une durée d'un à six ans les pièces d'identité qui lui étaient communiquées par les personnes concernées dans le cadre de l'exercice d'un droit. Il considère que cette durée est excessive, les données étant conservées au-delà de la durée nécessaire pour l'atteinte de la finalité pour laquelle elles sont traitées.

38. Sur ce point, la société souligne la modification de ces pratiques depuis la notification du rapport de sanction, les titres d'identité n'étant plus conservés que pendant la durée relative au traitement de la demande en question.

39. La formation restreinte relève que la délégation de contrôle a effectivement constaté que des copies de cartes nationales d'identité de requérants étaient conservées par la société pendant une durée pouvant aller d'un à six ans.

40. Or, elle considère que, dès qu'il a été fait droit à la demande, la société n'a plus besoin de conserver une copie de la pièce d'identité du requérant. La fourniture de ce document a en effet pour seul but de justifier de l'identité de la personne dont émane la demande et il n'est pas nécessaire de le conserver une fois l'identité confirmée.

41. La formation restreinte estime également que, pour démontrer qu'elle a effectivement fait droit à la demande, la société peut, au titre d'un archivage intermédiaire à des fins contentieuses, ne conserver que le courrier de réponse favorable, élément dont la conservation présente, au demeurant, un risque moindre pour la personne concernée.

42. Elle considère donc, au vu de ces éléments, qu'un manquement à l'article 5-1-e) du RGPD est constitué.

43. Elle souligne néanmoins les modifications apportées dès la notification du rapport et observe que les nouvelles pratiques de la société sont, au jour de la séance, en conformité avec le Règlement. Il a en effet été démontré que les pièces d'identité sont désormais supprimées dès qu'il a été fait droit à la demande.

B. Sur le manquement relatif aux modalités d'exercice des droits

44. L'article 12 du Règlement dispose, d'une part, que *le responsable du traitement facilite l'exercice des droits conférés à la personne concernée au titre des articles 15 à 22. Dans les cas visés à l'article 11, paragraphe 2, le responsable de traitement ne refuse pas de donner suite à la demande de la personne concernée d'exercer les droits que lui confèrent les articles 15 à 22, à moins que le responsable du traitement ne démontre qu'il n'est pas en mesure d'identifier la personne concernée* et que *lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande visée aux articles 15 à 21, il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée* .

45. Il dispose, d'autre part, que *le responsable du traitement fournit à la personne concernée des informations sur les mesures prises à la suite d'une demande formulée en application des articles 15 à 22, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes. Le responsable du traitement informe la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande.*

46. **En premier lieu**, le rapporteur a relevé que, sauf dans les cas d'opposition au traitement des données à des fins de prospection commerciale, la société demandait un justificatif d'identité de manière systématique lors de l'exercice d'un droit.

47. La société a souligné, lors de ses échanges avec le rapporteur, que cette pratique a été abandonnée dès le 23 octobre 2019.

48. La formation restreinte relève que la société ne réservait pas la demande d'un justificatif d'identité aux seuls cas où existait un doute raisonnable sur l'identité de la personne, cette demande étant systématique. Elle souligne que la présence (constatée lors des contrôles) des justificatifs d'identité accompagnant les demandes, comme les courriers en réponse de la société communiqués à la CNIL par les plaignants, ont démontré l'existence de cette pratique. En effet, la CNIL a été informée d'une demande en ce sens s'agissant de Messieurs […], […], […], […], […] et […] et de Madame […] sans que la société justifie de doutes raisonnables quant à l'identité de la personne.

49. La formation restreinte considère que le caractère systématique des demandes de justificatifs d'identité, reconnu par la société, suffit à démontrer que ces demandes n'étaient pas limitées aux situations où la société avait *des doutes raisonnables quant à l'identité de la personne physique présentant la demande* .

50. Elle considère donc, au vu de ces éléments, qu'un manquement à l'article 12 du RGPD est constitué.

51. Elle souligne néanmoins les modifications apportées par la société et constate que les nouvelles pratiques de la société sont, au jour de la séance, en conformité avec le Règlement. Il est en effet démontré que les courriers de réponse aux demandes d'exercice de droit n'exigent plus de justificatif d'identité de manière systématique.

52. **En second lieu**, le rapporteur reproche à la société le délai dans lequel il était répondu aux demandes d'exercice de droit. Il souligne que les délais de réponse varient mais peuvent atteindre neuf mois, sans qu'aucune information ne soit communiquée dans l'attente aux personnes concernées. Il estime que ces retards de traitement sont récurrents. À titre d'illustration, la demande de suppression et d'opposition de Madame […] a été reçue le 4 juillet 2018. Le retrait de son consentement à la prospection publicitaire a été retranscrit en base de données le 15 avril 2019, soit plus de neuf mois plus tard. La demande d'accès de Monsieur […] a été reçue le 7 novembre 2018 et une réponse lui a été apportée le 10 juin 2019, soit plus de sept mois plus tard. La demande d'accès et d'opposition de Monsieur […] a été enregistrée dans l'outil JIRA le 10 janvier 2019. Il ressort pourtant des documents communiqués à la CNIL par le plaignant que la société a accusé réception de sa première demande dès le 9 novembre 2018. Une réponse a été apportée à sa demande concernant l'opposition à la prospection le 11 juin 2019, soit plus de sept mois plus tard.

53. Sur ce point, la société reconnaît, tant dans sa deuxième réponse aux observations du rapporteur que lors de la séance de la formation restreinte, un retard chronique dans le traitement des demandes au moment du contrôle. Elle souligne cependant les efforts particulièrement importants déployés depuis les opérations de contrôle, la restructuration en profondeur de l'organisation des équipes travaillant sur ces questions, et la transformation de leurs méthodes de travail, avec notamment le développement de nouveaux outils *ad hoc* qui améliorent l'attribution et le traitement des demandes d'exercice de droit, réduisant leur délai de traitement ainsi que le risques d'erreur.

54. La formation restreinte observe que l'organisation de la société entraînait, structurellement, un retard dans le traitement des demandes et prend note que la société indique que cette défaillance structurelle trouvait son origine dans une mauvaise appréciation des conséquences du RGPD. L'entrée en application de ce texte a augmenté le nombre de demandes auxquelles elle a dû faire face, dans des proportions inattendues (passant, avant l'entrée en application du RGPD, d'une à deux demandes par jour à parfois plus de 75 demandes par jour après le 25 mai 2018).

55. La formation restreinte constate que ce défaut d'anticipation a eu des conséquences directes pour les personnes exerçant leurs droits, les contraignant parfois à formaliser plusieurs relances face au silence gardé par la société. La formation restreinte considère donc, au vu de ces éléments, qu'un manquement à l'article 12 du RGPD est constitué.

56. Elle souligne néanmoins les modifications profondes et efficaces apportées par la société et constate que les nouvelles pratiques de la société sont, au jour de la séance, en conformité avec le Règlement. La société démontre aujourd'hui un délai moyen de réponse aux demandes inférieur à quinze jours, parfois même inférieur à dix jours. Elle démontre également que

plus aucune réponse n'a été envoyée hors délai depuis le changement de ses processus internes et le développement de nouveaux outils.

C. Sur le manquement relatif à l'information des personnes

57. L'article 12 du RGPD dispose que *le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 […] 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 […]* . Les articles 13 et 14 dressent la liste des informations devant être communiquées aux personnes concernées lorsque les données à caractère personnel sont collectées directement auprès d'elles et indirectement.

1. S'agissant de l'accessibilité de l'information

58. **En premier lieu**, le rapporteur considère que l'information délivrée n'était pas aisément accessible.

59. S'agissant d'abord de l'information communiquée sur le site carrefour.fr, il relève en effet que la multiplicité des pages à consulter, des liens présents dans les différentes pages, ainsi que la redondance des informations ne permettent pas de considérer que les informations pertinentes pour les personnes sont aisément accessibles.

60. S'agissant ensuite de l'information communiquée aux personnes adhérant en ligne au programme fidélité, le rapporteur estime que les informations n'étaient pas aisément accessibles puisqu'elles étaient insérées à l'intérieur des conditions générales d'utilisation de la carte Carrefour.

61. S'agissant enfin de l'information délivrée aux personnes adhérant au programme fidélité à l'aide d'un bulletin papier, le rapporteur relève que les informations n'étaient pas non plus aisément accessibles. Il relève en effet que le bulletin résumait les mentions essentielles et renvoyait pour des mentions plus complètes, vers la page d'accueil du site carrefour.fr sans plus de précisions.

62. Sur ces points, la société avance qu'une page dédiée à la protection des données était directement accessible par un lien hypertexte en pied de page, et qu'elle a modifié les mentions d'information sur son site web le 22 novembre 2019, soit préalablement à l'ouverture de la procédure de sanction et à la notification du rapport. Ces modifications importantes ont notamment consisté en la fusion de l'ensemble des mentions d'information dans un document unique, la conservation d'une page dédiée à l'exercice des différents droits, et une reformulation de l'information communiquée afin de la rendre plus lisible, plus précise et plus simple.

63. La formation restreinte relève que la société a fait le choix d'une information en plusieurs niveaux, comme le lui permet le Règlement.

64. Dans cette configuration, la formation restreinte estime particulièrement important que l'information demeure aisément accessible , comme l'exige l'article 12 du Règlement. La présentation de l'information en plusieurs niveaux augmente en effet le risque que l'information soit plus difficile à trouver. Or, le considérant 39 du RGPD souligne que *le principe de transparence exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples* . Le considérant 58 dispose également que *le principe de transparence exige que toute information adressée au public ou à la personne concernée soit concise, aisément accessible et facile à comprendre, et formulée en des termes clairs et simples et, en outre, lorsqu'il y a lieu, illustrée à l'aide d'éléments visuels.*

65. En l'espèce, la formation restreinte considère, d'une part, que l'accès aux mentions d'information sur le site carrefour.fr était malaisé, puisque ces dernières étaient regroupées dans l'article 3 des conditions générales d'utilisation du site carrefour.fr que l'utilisateur devait donc parcourir. Il en va de même pour les mentions d'information relatives au programme de fidélité qui figuraient dans l'article 10 des conditions générales d'utilisation de la carte Carrefour.

66. Or ces deux documents étaient d'une longueur telle que l'utilisateur était contraint de faire défiler un grand nombre de pages et de lire plusieurs dizaines de paragraphes (une quinzaine dans les conditions générales d'utilisation du site carrefour.fr, plus de soixante-dix dans les conditions générales d'utilisation de la carte Carrefour) avant de pouvoir trouver les informations relatives à la protection de ses données à caractère personnel. La formation restreinte considère en conséquence que l'accès à ces informations n'était pas aisé et que l'utilisateur devait faire preuve d'une détermination particulière pour accéder aux informations sur ces questions. Elle rappelle que l'information doit être présentée de manière efficace et succincte afin d'éviter de noyer l'information à délivrer parmi d'autres contenus informatifs.

67. La difficulté d'accès à ces informations était en outre renforcée par leur redondance. En effet, les informations relatives à la protection des données à caractère personnel étant dispersées et morcelée entre plusieurs documents (conditions générales d'utilisation, conditions générales de vente, page relative à la protection des données personnelles , page dédiée à l'exercice des droits), certaines informations n'étaient présentes que sur certaines pages, alors que d'autres étaient présentées plusieurs fois.

68. Afin que l'utilisateur n'ait pas à chercher les informations pertinentes, la formation restreinte considère que celles-ci devraient être regroupées dans un document unique distinct des conditions générales d'utilisation. Elle partage ici la position développée par le G29 dans les lignes directrices sur la transparence au sens du Règlement adoptée dans leur version révisée le 11 avril 2018 (ci-après les lignes directrices sur la transparence) qui estime que *la personne concernée ne doit pas avoir à chercher activement les informations couvertes par ces articles parmi d'autres informations telles que les conditions d'utilisation d'un site internet* .

69. Elle estime, d'autre part, que lorsqu'un responsable de traitement fait le choix de communiquer aux personnes concernées une information en plusieurs niveaux, il importe non seulement que le deuxième niveau d'information détaille l'ensemble des mentions relatives au traitement mais également que le premier niveau d'information en présente les caractéristiques essentielles. Cette exigence d'accessibilité, telle qu'éclairée par le considérant 39 du RGPD, est notamment rappelée dans les lignes directrices sur la transparence. Le G29 préconise notamment que *le premier niveau/la première modalité inclut les détails de la finalité du traitement, l'identité du responsable du traitement et une description des droits des personnes concernées* .

70. Or, la formation restreinte relève que le premier niveau d'information présent sur le site carrefour.fr, accessible à partir du lien données personnelles , ne fournissait pas ces informations essentielles mais uniquement quelques informations d'ordre général comme la possibilité, pour les personnes concernées, de *consulter les données personnelles qui [les] concernent* ou d' *exercer les différents droits* dont elles bénéficient, ou l'une des finalités du traitement (la présentation d'offres personnalisées).

71. Concernant les personnes adhérant au programme fidélité par le bulletin papier, la formation restreinte considère que, en renvoyant ces personnes vers le site carrefour.fr sans plus de précisions, la société n'a pas rendu l'information aisément accessible. La société aurait dû, *a minima*, préciser la page ou l'adresse URL à laquelle ces informations étaient disponibles. La formation restreinte relève que ce défaut d'accessibilité par un simple renvoi sur la page d'accueil du site était aggravé par les défauts précédemment soulignés concernant le site carrefour.fr.

72. **En second lieu**, le rapporteur considère que l'information délivrée n'était pas rédigée en des termes clairs et simples.

73. Il considère que l'ensemble des mentions d'informations (dans les conditions générales d'utilisation du site carrefour.fr, les formulaires papiers d'adhésion au programme fidélité et pour l'adhésion au même programme par l'espace client du site carrefour.fr) utilisaient des termes imprécis et peu clairs et n'étaient pas aisément compréhensibles en raison de leur mise en page.

74. Sur ce point, la société met en avant les modifications importantes apportées aux mentions d'information préalablement à l'ouverture de la procédure de sanction. Elle indique avoir, dès le mois de novembre 2019, mis en lignes une page d'information spécifique à la protection des données personnelles, séparée des conditions générales d'utilisation, accessible directement depuis la page d'accueil par un lien hypertexte.

75. La formation restreinte relève que les mentions d'information présentes sur le site carrefour.fr (tant dans les conditions générales d'utilisation que dans le processus d'adhésion au programme fidélité) et sur les bulletins d'inscription papier comportaient, au moment du contrôle le 24 mai 2019, des formulations peu claires, ambigües, ou imprécises. L'utilisation, de manière quasiment systématique notamment dans les conditions générales d'utilisation du site carrefour.fr et du programme fidélité, de termes tels que *ces traitements incluentnotamment* , *pour l'une ou plusieurs des raisons suivantes* ou *vos données sont susceptibles d'être utilisées* ne permettent pas aux personnes concernées d'appréhender pleinement les traitements mis en œuvre. De la même manière, des formules telles que *vous disposez également d'un droit d'obtenir la limitation d'un traitement et d'un droit à la portabilité des données que vous avez pu fournir, qui trouveront à s'appliquer dans certains cas* (conditions générales d'utilisation de la carte Carrefour) ne délivrent pas une information complète aux personnes concernées, dès lors que ces dernières ne peuvent comprendre, à leur lecture, les situations dans lesquelles ces droits leurs sont ouverts et les modalités pour les faire appliquer.

76. Les conditions générales d'utilisation du site carrefour.fr et du programme de fidélité ne comprenaient, dans la majorité des cas, que des exemples relatifs aux données collectées (*nous pouvons éventuellement disposer de données de l'open Data*), aux opérations réalisées ou aux finalités poursuivies (*vos données pourront faire l'objet d'un traitement pour l'une ou plusieurs des raisons suivantes*), ou des formulations générales et évasives. Or la formation restreinte rappelle que le considérant 39 du RGPD souligne l'importance du principe de transparence, précisant que *les personnes physiques devraient être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement*. La formation restreinterappelle que l'information communiquée présente une importance capitale, puisque sa conformité conditionne la validité de l'engagement de la personne et sa volonté de permettre le traitement de données à caractère personnel par un responsable de traitement déterminé. La personne concernée devrait être en mesure, à la lecture des informations qui lui sont communiquées, de comprendre la portée générale du traitement, ce qui n'est pas le cas en l'espèce.

77. Les formulations utilisées, souvent inutilement compliquées, rendaient la lecture des mentions d'information particulièrement fastidieuse, même pour une personne éclairée. Par exemple, une phrase comme *vous pouvez demander à exercer votre droit d'opposition pour motif pour des raisons tenant à votre situation particulière, à un traitement de données personnelles vous concernant lorsque le traitement est fondé sur l'intérêt légitime du responsable de traitement y compris le profilage* extraite des conditions générales du site carrefour.fr ne permet pas à un utilisateur profane de comprendre ni l'existence, ni la portée, ni les conditions d'exercice de son droit d'opposition. Il en va de même pour la phrase *vos données pourront peut-être transmises à tout ou partie des destinataires suivantes : […] les marques partenaires, mais dans ce cas ces derniers n'ont pas accès ni directement ni indirectement aux données vous concernant et seuls [sic] des données liées à votre profil sans qu'il soit possible de vous identifier directement ou indirectement, aux sociétés du groupe Carrefour pour les finalités susvisées* s'agissant des destinataires des données.

78. La formation restreinte rappelle que l'information présentée était destinée à l'ensemble des utilisateurs des services de la société, qui peuvent avoir des profils très divers. La société aurait dû adopter un style permettant d'être compris par le plus grand nombre. La formation restreinte considère que tel n'était pas le cas en l'espèce.

79. D'une manière générale, la formation restreinte rappelle que les mentions d'information doivent s'attacher, autant que faire se peut, à utiliser un vocabulaire simple, faire des phrases courtes et employer un style direct, mais aussi éviter les termes juridiques ou techniques, les termes abstraits ou ambigus et les formules telles que *nous pourrions utiliser vos données* , *une possible utilisation de vos données* , *quelques données vous concernant sont utilisées* , etc.

80. Au demeurant, la formation restreinte relève que, malgré le nombre très important d'informations communiquées, ces dernières n'étaient ni hiérarchisées, ni ordonnées. L'information prenait la forme d'une longue énumération portant sur les différents points du Règlement. Elle considère qu'une telle présentation ne permet pas aux personnes concernées de trouver facilement l'information qu'elle cherche, la contraignant à lire l'ensemble des mentions d'information. Elle estime donc que la présentation utilisée ne respectait pas l'exigence d'accessibilité posée par l'article 12 du Règlement, éclairée par les lignes directrices sur la transparence déjà citées.

81. La formation restreinte note que la combinaison des articles 12 et 13 du Règlement impose au responsable de traitement que l'information fournie soit à la fois complète et aisément compréhensible. Cet équilibre peut être difficile à atteindre lorsque, comme en l'espèce, les données traitées, les finalités poursuivies et les durées de conservations sont nombreuses et différentes. Pour autant, elle considère que la qualité de l'information fournie est centrale dans la décision des personnes concernées d'engager une relation commerciale. À ce titre, la formation restreinte estime que la société aurait dû porter à l'information communiquée une attention toute particulière et aboutir, avant même les contrôles opérés, à un résultat plus lisible pour les personnes.

2. S'agissant du contenu de l'information

82. Le rapporteur considère que l'information communiquée aux personnes est incomplète à plusieurs titres.

83. Premièrement, il indique que le responsable de traitement n'est pas correctement identifié sur le site carrefour.fr.

84. Deuxièmement, le rapporteur souligne que la base juridique des traitements n'est pas indiquée dès lors que la société se contente d'indiquer que les données à caractère personnel peuvent être traitées en raison du consentement de l'utilisateur, de l'exécution du contrat ou de l'intérêt légitime du responsable de traitement, sans plus de précisions.

85. Troisièmement, le rapporteur considère que l'information relative aux pays où peuvent être transférées les données n'est pas complète, les garanties entourant le transfert n'étant pas précisées, de même que le moyen d'obtenir copie de ces garanties.

86. Quatrièmement, il considère que les personnes ne sont pas informées, pour l'ensemble de leurs données, de la durée pendant laquelle elles peuvent être conservées.

87. Sur l'ensemble de ces points, la société a indiqué avoir apporté des modifications antérieurement et postérieurement à la notification du rapport et visant à sa mise en conformité. Elle avance qu'elle fournissait, au jour des contrôles, des informations complètes sur plusieurs points, et notamment les coordonnées de son délégué à la protection des données, les destinataires des données, l'existence de droits. Sur les points où elle reconnaît l'insuffisance de l'information qu'elle délivrait, elle indique avoir modifié ses mentions d'information conformément aux demandes du rapporteur pendant la procédure, notamment quant à l'identité du responsable de traitement, les finalités et bases légales des traitements opérés, les durées de conservation et le transfert de données à caractère personnel hors de l'Union européenne.

88. Sur le premier point, il ressort des constatations de la délégation de contrôle que la société CARREFOUR HYPERMARCHÉS était indiquée comme étant responsable des traitements mis en œuvre à travers le site carrefour.fr. Les sociétés CARREFOUR HYPERMARCHÉS, CARREFOUR SUPERMARCHÉS FRANCE, CARREFOUR PROXIMITÉ FRANCE, CARREFOUR DRIVE et OOSHOP étaient désignées dans les mentions d'information comme responsables de traitement conjoints pour le programme de fidélité.

89. La formation restreinte considère, sur le premier point, que la responsabilité des traitements mis en œuvre à partir du site carrefour.fr incombe à la société CARREFOUR FRANCE, qui détermine seule la politique marketing commune à tous les formats des magasins en France. Cette interprétation est conforme à l'analyse de la société CARREFOUR FRANCE, qui se considère également responsable de traitement comme elle l'a indiqué à la délégation de contrôle le 28 mai 2019.

90. En conséquence, la formation restreinte considère que les mentions portées sur le site carrefour.fr comme dans les conditions générales d'utilisation de la carte Carrefour étaient erronées.

91. Sur le deuxième point, la formation restreinte rappelle que les personnes concernées doivent être informées de la base légale du ou des traitements mis en œuvre. Cette exigence ne saurait être satisfaite de la seule référence faite aux bases légales existantes lorsque plusieurs traitements sont mis en œuvre. Dans cette hypothèse, les personnes ne sont en effet pas informées de la base légale applicable à chacun des traitements réalisés.

92. La formation restreinte considère que l'indication de la base légale applicable à chaque traitement présente une importance particulière. D'une part, elle permet à la personne concernée d'avoir une appréciation globale sur le traitement réalisé, notamment sur son origine. Elle doit ainsi être en mesure de savoir si les données traitées le sont sur le fondement du consentement qu'elle a donné (et qu'elle pourrait donc retirer), ou en vertu d'un contrat qu'elle aurait passé avec le responsable de traitement, d'une obligation légale de ce dernier ou encore de son intérêt légitime. D'autre part, et surtout, la base légale applicable peut avoir des conséquences directes sur les droits des personnes. Par exemple, l'article 20 du RGPD prévoit que le droit à la portabilité des données s'applique lorsque le traitement est fondé sur le consentement. Dès lors, la société avait l'obligation de préciser la base légale applicable à chaque traitement mis en œuvre.

93. En raison de l'absence de telles précisions, la formation restreinte considère que les mentions portées sur le site carrefour.fr étaient incomplètes.

94. Sur le troisième point, la formation restreinte souligne que l'article 13 du Règlement impose, en son point 1.f), que le responsable de traitement informe la personne concernée de *l'existence ou l'absence d'une décision d'adéquation rendue par*

la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition .

95. La formation restreinte constate que ces informations n'étaient pas communiquées aux personnes concernées au moment des constations effectuées par la délégation de contrôle. La formation restreinte considère que les mentions portées sur le site carrefour.fr étaient incomplètes.

96. Sur le quatrième point, la formation restreinte relève que l'article 13-2-a) du Règlement impose que les personnes soient informées de *la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée* . Les lignes directrices sur la transparence, venant éclairer les dispositions de l'article 13, précisent que *la période de conservation (ou les critères pour la déterminer) […] devrait être formulée de manière à ce que la personne concernée puisse évaluer […] quelle sera la période de conservation s'agissant de données spécifiques ou en cas de finalités spécifiques* . La formation restreinte relève que les mentions d'information n'indiquaient pas les durées de conservation (ou les critères utilisés pour l'établir) de manière systématique pour l'ensemble des données ou des finalités, notamment les données de navigation ou les données relatives aux achats effectués. Il en résulte que les personnes ne pouvaient pas estimer, pour nombre de données, les durées de conservation établies par le responsable de traitement.

97. En raison de l'absence de telles précisions, la formation restreinte considère que les mentions portées sur le site carrefour.fr étaient incomplètes.

98. Il ressort de l'ensemble de ces éléments que l'information communiquée aux personnes à travers le site carrefour.fr et à travers les bulletins papier d'adhésion au programme fidélité n'était pas aisément accessible et était incomplète. La formation restreinte considère donc qu'un manquement aux articles 12 et 13 du RGPD est constitué.

99. Elle souligne néanmoins l'important travail de mise en conformité apporté par la société s'agissant des mentions d'information présentes sur son site web et sur ses bulletins papier. Elle constate que les nouvelles pratiques de la société sont, au jour de la séance, en conformité avec le Règlement. La société démontre aujourd'hui une information claire, transparente, aisément accessible et complète sur l'ensemble de ses supports.

D. Sur le manquement relatif au droit d'accès

100. L'article 15 du RGPD dispose que les personnes concernées ont le droit d'obtenir du responsable de traitement la confirmation que des données à caractère personnel les concernant sont traitées ainsi qu'un certain nombre d'informations parmi lesquelles toute information disponible quant à l'origine des données, lorsque celles-ci ne sont pas collectées directement par le responsable de traitement (article 15-1-g).

101. Dans la saisine n^{o} 19001627 du 21 janvier 2019, Monsieur […] expliquait avoir reçu, le 8 novembre 2018, un courrier de prospection électronique sans avoir communiqué ses coordonnées au groupe CARREFOUR par le passé. Il indiquait avoir demandé le jour même l'origine des données personnelles le concernant détenues par la société. Le 15 novembre 2018, la société lui avait répondu en vue d'obtenir une copie de la pièce d'identité du plaignant qui a été communiqué au responsable de traitement le 21 novembre. Monsieur […] expliquait que, malgré plusieurs relances les 4 et 18 janvier 2019, aucune réponse n'a été apportée à sa demande, seule son opposition à recevoir de la prospection ayant été prise en compte.

102. Il ressort des constatations effectuées le 12 juin 2019 que ce plaignant était un ancien client de la société OOSHOP, dont le site a, par la suite, été intégré au site carrefour.fr.

103. La société CARREFOUR FRANCE reconnaît ne pas avoir, dans un premier temps, communiqué au plaignant l'origine des données qu'elle détenait le concernant, considérant qu'elle traitait ces données personnelles dans le cadre d'une collecte directe, et non indirecte, et que l'origine des données figure parmi les informations devant être communiquées sur le fondement de l'article 15 du Règlement seulement en cas de collecte indirecte des données à caractère personnel.

104. Sur ce point, la formation restreinte relève que le plaignant avait précédemment créé un compte sur le site web ooshop. C'est à cette occasion que les données à caractère personnel le concernant avaient été collectées par la société OOSHOP. La formation restreinte considère que la fusion ultérieure entre le site web ooshop et le site carrefour.fr ne donne pas à la société CARREFOUR FRANCE la qualité de primo-collectant des données à caractère personnel. En effet, les données à caractère personnel ont été transmises à la société CARREFOUR FRANCE par la société OOSHOP, ce qui correspond au cas d'une collecte indirecte, les données n'ayant pas été collectées par CARREFOUR FRANCE auprès de la personne concernée. Dès lors, la formation restreinte considère que CARREFOUR FRANCE était tenu d'informer le plaignant de l'origine des données dans le cadre de sa demande d'accès, conformément à l'article 15-1-g) du RGPD.

105. La formation restreinte rappelle que le fait que le plaignant ait été informé de la fusion entre le site ooshop et le site carrefour.fr préalablement à sa demande à la société ne dispensait pas le responsable de traitement de son obligation d'information sur l'origine des données, formulée par le plaignant dans le cadre de l'exercice de ses droits.

106. Il ressort de ces éléments qu'un manquement à l'article 15 du Règlement est constitué.

107. La formation restreinte souligne néanmoins que la société a fait droit à la demande du plaignant le 19 juin 2019, après le contrôle réalisé mais avant l'engagement de la procédure de sanction, et que le manquement n'était donc plus constitué au jour de la séance.

E. Sur le manquement relatif au droit à l'effacement

108. L'article 17 du Règlement définit les conditions dans lesquelles les personnes concernées ont droit à l'effacement de leurs données à caractère personnel. L'article 17-1-c), notamment, offre ce droit lorsque les données ne sont plus nécessaires au

regard des finalités du traitement ou lorsque la personne s'oppose au traitement mis en œuvre à des fins de prospection.

109. La Commission a été saisie de plusieurs plaintes relatives aux difficultés rencontrées dans le cadre de l'exercice de ce droit.

110. Par la saisine n° 18011774 du 8 juin 2018, Monsieur […] a saisi la CNIL, expliquant avoir demandé l'effacement de ses données sans obtenir de réponse favorable à sa demande, qui portait notamment sur l'effacement de son adresse de courrier électronique, utilisée par la société à des fins de prospection commerciale.

111. Les constatations opérées pendant le contrôle du 12 juin 2019 ont permis de constater la présence de l'adresse de courrier électronique du plaignant dans les bases de données de la société.

112. En défense, la société a expliqué que l'adresse électronique sert de clef d'entrée de la base en question et qu'elle ne peut donc être supprimée. Elle a en outre indiqué que la situation n'a entraîné aucun préjudice pour le plaignant, son opposition à la prospection ayant été prise en compte.

113. La formation restreinte souligne tout d'abord que la demande d'effacement de Monsieur […] du 28 mai 2018 était large et explicite : *je vous demande de supprimer toutes les données que vous pourriez avoir sur moi. Ces données seront rattachées à l'adresse mail* […]@[…]*.com.*

114. La formation restreinte constate que la société a fait le choix d'utiliser comme clef d'entrée de sa base de données l'adresse électronique des personnes, donc une donnée à caractère personnel. Cette décision purement pratique, sans que la conservation de la donnée en question soit justifiée par une quelconque finalité légitime au regard des éléments du dossier, ne saurait lui permettre de s'exonérer de ses obligations en matière d'exercice des droits. La formation restreinte estime que Monsieur […] pouvait légitimement, sur le fondement de l'article 17-1 c) du Règlement, exiger l'effacement de ses données utilisées à des fins de prospection commerciale et il revenait dès lors à la société d'accéder à cette demande et de mettre en place un système d'organisation de sa base de données qui ne portait pas atteinte à ce droit. En l'espèce, la formation restreinte relève que la société n'a pas respecté ses obligations résultant de l'article 17 du Règlement.

115. La formation restreinte observe néanmoins que la société a modifié l'architecture de ses bases postérieurement à la notification du rapport de sanction. Le nouveau mode de fonctionnement n'utilise plus de donnée à caractère personnel comme clef d'entrée de la base, et il a été fait droit à la demande de Monsieur […].

116. Par la saisine n° 18013824 du 7 juillet 2018, Madame […] a saisi la CNIL, expliquant avoir demandé à la société l'effacement de toutes les données à caractère personnel la concernant sans obtenir de réponse favorable à sa demande.

117. Les constatations opérées pendant le contrôle ont permis de constater la présence du nom, du prénom, de la date de naissance et du numéro de téléphone portable de la plaignante dans les bases de données de la société.

118. En défense, la société a expliqué que la présence de ces données résultait d'une erreur ponctuelle et qu'elle n'avait pas entraîné de conséquences pour la plaignante, son opposition à recevoir de la prospection commerciale ayant été prise en compte.

119. La formation restreinte considère que Madame […] pouvait légitimement, sur le fondement de l'article 17-1 c) du Règlement, exiger l'effacement de ses données utilisées à des fins de la prospection commerciale. Un manquement à l'article 17 du Règlement est donc constitué.

120. La formation restreinte relève néanmoins que la société a fait droit à la demande de Madame […] le 12 mai 2020.

121. Par la saisine n° 19001602 du 19 janvier 2019, Monsieur […] a saisi la CNIL, expliquant avoir sollicité à deux reprises l'effacement de ses données et continuer néanmoins à recevoir de la prospection commerciale.

122. Les constatations opérées pendant le contrôle ont permis de constater la présence du nom, du prénom, de la date de naissance et des adresses postale et électronique du plaignant dans les bases de données de la société.

123. La société explique que les données relevées n'étaient pas intégrées à une base servant à la prospection commerciale. Elle avance que, dans le cas d'une opposition à la prospection, elle fait droit à cette demande mais n'efface pas les données des bases n'étant pas dédiées à la prospection.

124. La formation restreinte relève que la demande de Monsieur […], portant sur l'arrêt de la prospection commerciale et l'effacement des données, était dénuée de toute ambiguïté Dans un premier courriel adressé à la société, le plaignant expliquait *Je souhaite obtenir la clôture de mon compte ainsi conformément aux articles 38 et suivants de la loi informatique et libertés du 6 janvier 1978 modifiée, je vous remercie de supprimer l'ensemble de mes données personnelles rattachées à ce compte* . Dans un second courrier, il précisait *Ainsi, je réitère ma demande : en application des articles 21.1 et 17.1.c du Règlement général sur la protection des données (RGPD), je vous remercie de supprimer les données personnelles me concernant sur les sites suivants : carrefour.fr et courses-en-ligne.carrefour.fr* . Monsieur […] étant fondé à solliciter une telle suppression sur le fondement de l'article 17-1 c), il revenait à la société, sauf justification de cette dernière à conserver les données pour une finalité légitime, de faire droit à cette demande. Un manquement à l'article 17 du Règlement est donc constitué.

125. La formation restreinte relève néanmoins que, tout en contestant l'appréciation du rapporteur, la société a fait droit à la demande de Monsieur […] en procédant à l'effacement de toutes les données le concernant.

126. Par la saisine n° 19006872 du 6 avril 2019, Monsieur […] a saisi la CNIL, expliquant avoir demandé à la société l'effacement de son adresse postale sans obtenir de réponse favorable à sa demande.

127. Les constatations opérées pendant le contrôle ont permis de constater la présence du nom, du prénom, de la date de naissance, des numéros de téléphone fixe et mobile et des adresses postale et électronique du plaignant dans les bases de données de la société.

128. La société explique que la présence de l'adresse postale du plaignant résulte d'une erreur ponctuelle et n'a pas entraîné de conséquence, son opposition à recevoir de la prospection commerciale ayant été prise en compte.

129. La formation restreinte estime que Monsieur […] pouvait légitimement, sur le fondement de l'article 17-1 c) du Règlement, exiger l'effacement de ses données. Un manquement à l'article 17 du Règlement est donc constitué.

130. La formation restreinte constate néanmoins que la société a rectifié son erreur dès qu'elle en a été informée, à la suite du contrôle réalisé le 11 juin 2019.

131. **En conclusionsur ces manquements**, la formation restreinte considère que si, après une demande d'effacement, certaines données personnelles des clients peuvent être conservées, notamment au titre des obligations légales ou à des fins probatoires ou lorsque que la société dispose d'un motif légitime impérieux, les données personnelles non nécessaires dans le cadre du respect de ces autres obligations ou finalités doivent être supprimées après l'exercice de ce droit dès lors que les conditions posées par l'article 17 du RGPD sont remplies. Elle relève à cet égard que tel était le cas pour le traitement ayant pour finalité la prospection et qu'il ne ressort pas des éléments de la procédure que la conservation des données en question était légitime sur un autre fondement.

132. Au demeurant, la formation restreinte rappelle que le responsable de traitement a l'obligation de se rapprocher de la personne concernée lorsqu'il estime que les demandes qu'il reçoit ne comportent pas tous les éléments lui permettant de procéder aux opérations qui lui sont demandées (article 142 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, anciennement article 94 du décret n° 2005-1309 du 20 octobre 2005). Dès lors, la formation restreinte estime que, si la société CARREFOUR FRANCE estimait que les demandes d'effacement étaient trop larges et qu'elle ne pouvait y faire droit sur le fondement d'un intérêt légitime supérieur ou parce que l'effacement n'était pas possible sur le fondement de l'article 17 du RGPD, il lui revenait de prendre l'attache des personnes concernées, ce qu'elle n'a pas fait en l'espèce.

133. En conséquence, dans chacun des cas précités, la société n'a pas respecté ses obligations résultant de l'article 17 du Règlement et qu'un manquement est caractérisé.

F. Sur le manquement relatif au droit d'opposition au traitement des données personnelles à des fins de prospection commerciale

134. Le deuxième paragraphe de l'article 21 du Règlement dispose que *lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection* .

135. Par la saisine n° 18019816 du 1er octobre 2018, Monsieur […] a saisi la CNIL, expliquant avoir continué à recevoir des SMS publicitaires de la part de la société malgré une opposition précédemment exprimée au traitement de ses données personnelles à des fins de prospection commerciale.

136. Les constatations opérées pendant le contrôle du 11 juin 2019 ont permis de constater que l'opposition du plaignant n'avait pas été retranscrite dans les bases de données de la société, ne permettant ainsi pas sa prise en compte effective.

137. La société explique que cette erreur, ponctuelle, est due à une carence de son prestataire qui ne lui avait pas transmis l'opposition en question.

138. La formation restreinte relève qu'il ressort des constatations opérées lors du contrôle, comme des pièces communiquées par la société, que le prestataire […] communique à la société les oppositions exprimées par les personnes au fil de l'eau . Ces transmissions sont également compilées lors d'un envoi mensuel, seul pris en compte par la société pour retranscrire les oppositions en base de données, tel qu'elle l'a indiqué dans le cadre de la procédure. Il ressort des pièces communiquées par la société durant la procédure que l'opposition de Monsieur […] n'avait pas été transmise dans un envoi compilé au jour du contrôle, le 11 juin 2019. Pour autant, la formation restreinte souligne que la société avait reçu cette opposition dans le cadre de la transmission au fil de l'eau et qu'elle aurait donc dû cesser toute prospection commerciale envers le plaignant. En tout état de cause, la délégation a constaté que cette opposition n'avait pas été prise en compte au jour du contrôle.

139. Dès lors, un manquement à l'article 21 du Règlement est constitué.

140. La formation restreinte note néanmoins que cette erreur a été corrigée par la société lors du contrôle réalisé le 11 juin 2019. Elle souligne surtout que la société a déployé d'importants moyens pour revoir en profondeur la répercussion des oppositions exprimées par SMS dans ses bases de données dans le cadre de la présente procédure. Elle constate que les oppositions sont désormais directement reçues, traitées et retranscrites en base, assurant un meilleur respect des droits.

141. Par la saisine n° 18023308 du 22 novembre 2018, Monsieur […] a saisi la CNIL, expliquant avoir continué à recevoir des SMS publicitaires de la part de la société malgré plusieurs oppositions précédemment exprimées.

142. Les constatations opérées pendant le contrôle ont permis de constater que l'opposition du plaignant n'avait pas été retranscrite dans les bases de données de la société.

143. La société explique que cette absence de retranscription provient d'une erreur humaine interne.

144. La formation restreinte considère en conséquence que la société n'avait pas respecté ses obligations résultant de l'article 21 du Règlement.

145. Elle note néanmoins que l'opposition du plaignant a été prise en compte et retranscrite en base de données lors du contrôle réalisé le 11 juin 2019.

146. **En conclusion sur ces manquements**, la formation restreinte considère que dans chacun des cas précités, la société n'a pas respecté ses obligations résultant de l'article 21 du Règlement et qu'un manquement était caractérisé au jour du contrôle dès lors que, si elle avait offert aux personnes concernées un moyen d'exercer leur droit d'opposition, celui-ci n'était pas systématiquement pris en compte. Elle souligne cependant que l'ensemble des plaintes ont été traitées par la société dans le cours de la procédure, soit immédiatement lors des contrôles, soit à la suite de ses échanges avec le rapporteur.

G. Sur le manquement relatif au droit d'opposition à la prospection par voie électronique

147. Le premier paragraphe de l'article L34-5 du code des postes et des communications électroniques dispose qu' *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.* Le quatrième paragraphe du même article pose cependant une exception à ce principe d'interdiction *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* .

148. Par la saisine n° 19000325 du 4 janvier 2019, Monsieur […] a saisi la CNIL, expliquant avoir reçu de la prospection commerciale sans que le courriel lui permette de s'y opposer. En effet, le lien de désabonnement de la liste de diffusion le renvoyait, pour pouvoir s'opposer, à une page de connexion à un compte client. Or le plaignant ne disposait pas d'un tel compte, et ne pouvait donc pas s'opposer à la prospection commerciale.

149. Le rapporteur considère que la société a manqué à ses obligations découlant de l'article L.34-5 du code des postes et des communications électroniques dès lors qu'elle n'a pas systématiquement offert aux destinataires de ses courriels de prospection un moyen simple et effectif de se désabonner dans les courriels en question.

150. La société reconnaît cette erreur mais estime qu'un manquement ne saurait être caractérisé à partir de cette unique occurrence.

151. Il ressort des explications fournies par la société lors du contrôle réalisé le 11 juillet 2019 qu'une telle erreur est effectivement intervenue dans un courriel de prospection adressé à plus de 350 000 personnes. La société indique que le lien de désinscription intégré au courriel de prospection renvoyait vers l'espace personnel du site carrefour.fr permettant aux personnes disposant d'un compte client de se désinscrire. Par erreur, des personnes ne possédant pas de compte client ont été ciblées par cette campagne de prospection. Lorsque ces personnes ont cliqué sur le lien de désinscription, il leur a été demandé, pour pouvoir se désinscrire, de se connecter à un compte client dont elles ne disposaient pas.

152. La société explique avoir immédiatement repéré l'erreur parce qu'elle a reçu un grand nombre de plaintes de clients ne pouvant pas exercer correctement leurs droits. Elle affirme donc que cette erreur n'est intervenue qu'une fois, puisqu'elle n'a pas reçu d'autres réclamations similaires.

153. La formation restreinte considère que les personnes ne disposant pas d'un compte client n'ont pas pu s'opposer simplement à l'utilisation de leurs données personnelles à des fins de prospection commerciale. En conséquence, un manquement à l'article L.34-5 du code des postes et des communications électroniques est constitué dès lors qu'aucun moyen de s'opposer à la prospection par voie électronique n'a été offert à ces personnes.

154. La formation restreinte relève néanmoins que la société a mis en place un lien de désinscription unique ne nécessitant pas de passer par le compte client pour se désinscrire. Dès lors, elle estime que la société a mis en œuvre les mesures nécessaires pour que les droits des personnes soient respectés à l'avenir.

H. Sur le manquement relatif à la sécurité des données à caractère personnel

155. L'article 32 du RGPD dispose que *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* .

156. Le rapporteur fait grief à la société de ne pas avoir mis en place les mesures nécessaires à la protection des données à caractère personnel qu'elle traite après avoir eu connaissance de l'existence d'une vulnérabilité sur son site web.

157. Il ressort des déclarations de la société faites lors du contrôle du 11 juillet 2019 que, lors d'un achat sur le site carrefour.fr, une facture est mise à disposition du client sur son espace personnel après la livraison de la commande ou le retrait en magasin. Cette facture est accessible par une adresse URL fixe. Toute personne disposant de cette adresse peut accéder à la facture émise sans qu'il soit nécessaire de s'authentifier et de se connecter à son espace client.

158. La société a identifié cette vulnérabilité technique le 16 novembre 2018, consignée dans le registre des incidents de sécurité sous le numéro 415342. Pour pallier cette vulnérabilité, la société a décidé du développement de deux mesures : l'ajout d'une chaîne de caractères aléatoire et un mécanisme d'authentification préalable obligatoire. La première mesure

devait, en augmentant le nombre d'adresses URL potentielles, réduire le risque d'une déduction de l'adresse par incrémentation permettant d'accéder aux factures. La seconde mesure empêchait totalement l'accès aux factures par toute personne autre que la personne concernée.

159. La première mesure a été mise en place très rapidement par la société. Au jour du contrôle réalisé, soit presque huit mois après la découverte de la vulnérabilité, la seconde mesure n'avait toujours pas été déployée, et l'accès à une facture demeurait possible par toute personne disposant de son adresse URL.

160. Sur ce point, la société indique qu'elle avait déjà déployé, au jour du contrôle, une première mesure suffisante réduisant fortement le risque d'accès aux documents, et que la seconde mesure était en cours de déploiement.

161. La formation restreinte considère que l'ajout d'une chaîne de caractères aléatoire ne suffit pas, à elle seule, à empêcher un accès indu aux données à caractère personnel de tiers. Cette mesure permet de réduire le risque mais ne le fait pas disparaitre, l'accès demeurant possible. Elle rappelle que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) alerte depuis 2013 sur cette vulnérabilité liée aux adresses URL, même *dans le cas d'URL composées de plusieurs dizaines de caractères parfaitement aléatoires* (Recommandations pour la sécurisation des sites web, 13 août 2013, p. 16). La formation restreinte souligne que la société avait identifié la mesure adéquate à mettre en place dès novembre 2018 puisqu'elle avait prévu, dès cette date, le déploiement d'une authentification préalable obligatoire.

162. En conséquence, la formation restreinte considère que l'absence de mise en place de l'authentification préalable obligatoire à la suite de la découverte de la vulnérabilité – alors que cette mesure avait été identifiée et qu'elle est la seule mesure permettant d'empêcher complètement le risque – constitue un manquement à l'article 32 du Règlement.

163. La formation restreinte constate cependant que la société a mis en place une authentification obligatoire le 17 juillet 2019.

I. Sur le manquement relatif à la notification des violations de données à caractère personnel

164. L'article 33 du Règlement dispose qu' *en cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques* .

165. Le rapporteur estime que la société a manqué à son obligation de notifier les violations de données à caractère personnel, cette obligation ressortant des circonstances de la violation et des données concernées.

166. Il ressort des constatations effectuées lors du contrôle du 11 juillet 2019 que la société a identifié et consigné une attaque informatique dont elle avait été victime le 1er juillet 2019. Cette attaque, utilisant le service d'authentification de l'application mobile du groupe, a pris la forme de 800 000 tentatives de connexion à partir de 10 000 adresses IP. Elle a abouti à 4 000 authentifications réussies et à 275 accès effectifs aux comptes de clients. Cette violation n'a pas été notifiée à la CNIL.

167. En défense, la société a indiqué que la violation était peu susceptible d'engendrer un risque pour les droits et libertés des personnes. Elle précise également que les personnes concernées n'ont subi aucun préjudice financier puisqu'aucun point de fidélité n'a été soustrait. Elle souligne qu'en toute hypothèse, les conditions générales d'utilisation de la carte Carrefour prévoient le remboursement des cagnottes des personnes concernées en cas d'attaque par des tiers.

168. La formation restreinte rappelle qu'en cas de violation de données à caractère personnel, le principe est celui de la notification à l'autorité de contrôle. L'absence de notification n'est possible que par exception, lorsque la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes. En l'espèce, la formation restreinte considère que l'analyse des risques liés à cette violation n'amène pas à faire application de cette exception à l'obligation de notification. En effet, la gravité de la violation découle de l'origine à l'évidence malveillante de cette attaque, du grand nombre de personnes concernées et de la combinaison de plusieurs données personnelles auxquelles l'attaque a permis d'accéder et qui permettent l'identification et le contact direct des personnes concernées (les comptes clients pouvant comporter notamment l'identité des personnes, leur numéro de téléphone, leur adresse électronique et leur adresse physique).

169. La formation restreinte relève que les 4 000 comptes pour lesquels aucun accès effectif n'a été constaté mais qui ont fait l'objet d'une authentification réussie doivent être regardés comme participant à l'appréciation du risque. En effet, la formation restreinte rappelle que de nombreuses personnes utilisent une combinaison d'adresse électronique et de mot de passe identique sur un très grand nombre de sites web. Il existait donc un risque sérieux que les attaquants ayant identifié un couple adresse électronique/mot de passe valide essaient de le réutiliser sur d'autres sites web (technique appelée *credential stuffing*). Le risque existait également que, disposant désormais de plusieurs informations sur les personnes concernées et leurs relations avec les sociétés du groupe Carrefour, les attaquants tentent d'usurper l'identité d'une de ces sociétés dans des courriels malveillants et trompeurs (hameçonnage). Ces comptes doivent donc être considérés comme concernés par la violation.

170. En conséquence, la formation restreinte considère qu'un manquement à l'article 33 du RGPD est constitué.

171. Elle souligne néanmoins que, malgré une divergence d'appréciation avec le rapporteur et dans un objectif de conformité, la société a notifié la violation à la CNIL le 19 juillet 2020 et était ainsi en conformité au jour de la séance.

J. Sur le manquement relatif aux cookies

172. L'article 82 de la loi informatique et libertés (article 32.II dans une rédaction identique au jour des constatations) impose que les utilisateurs soient informés et que leur consentement soit recueilli avant toute opération d'accès ou d'inscription à des informations déjà stockées dans son équipement. Tout dépôt de cookie ou autres traceurs doit donc être précédé de

l'information et du consentement des personnes. Cette exigence ne s'applique pas aux cookies ayant *pour finalité exclusive de permettre ou faciliter la communication par voie électronique* ou étant *strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur* .

173. Le rapporteur considère que la société ne respectait pas ces dispositions dès lors qu'il ressort du contrôle en ligne du 24 mai 2019 qu'en arrivant sur le site web carrefour.fr plusieurs cookies ne rentrant pas dans les deux cas rappelés ci-avant étaient déposés sur le terminal de l'utilisateur dès la connexion à la page d'accueil du site et avant toute action de sa part.

174. La société ne conteste pas ces éléments.

175. La formation restreinte relève qu'en l'espèce, le dépôt de trente-neuf cookies était automatique dès l'arrivée sur la page d'accueil du site, et avant tout action de l'utilisateur. Parmi ces trente-neuf cookies, trois appartenaient à la solution Google Analytics (cookies _gid , _ga et _gat_gtag_UA_3928615_46).

176. S'agissant de ces trois cookies, dits *Google analytics,* la formation restreinte souligne qu'il ne fait pas débat que les données collectées par ces cookies peuvent être recoupées avec des données issues d'autres traitements pour poursuivre des finalités différentes que celles limitativement prévues par l'article 82 de la loi informatique et libertés , notamment pour mener à bien de la publicité personnalisée. En effet, il ressort du guide pratique Association des comptes Analytics et Google Ads , mis en ligne sur un des sites de la société Google, que *l'intégration de Google Analytics dans Google Ads (…) permet [aux annonceurs] de savoir précisément dans quelle mesure [leurs] annonces se traduisent par des conversions, puis d'ajuster rapidement les créations et les enchères en conséquence. [Les annonceurs peuvent] également combiner les produits afin d'identifier [leurs] segments les plus intéressants, puis susciter l'intérêt de ces utilisateurs à l'aide de messages personnalisés* .

177. Dès lors, ces cookies n'ont pas pour finalité exclusive de permettre ou de faciliter la communication par voie électronique et ne sont pas strictement nécessaires à la fourniture du service. Leur dépôt aurait donc dû obliger la société à recueillir préalablement le consentement des utilisateurs.

178. La formation restreinte considère, en conséquence, qu'un manquement à l'article 82 de la loi n° 78-17 du 6 janvier 1978 est constitué. Elle considère également que ce manquement a concerné un grand nombre de personnes, à savoir tous les visiteurs du site carrefour.fr.

179. La formation restreinte souligne néanmoins que la société a apporté d'importantes modifications sur son site web durant la procédure de sanction. Ces modifications ont amené, notamment, à l'arrêt du dépôt automatique de cookies à l'arrivée sur la page d'accueil du site depuis le 5 février 2020.

III. Sur les mesures correctrices et la publicité

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

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.

181. L'article 83 du RGPD prévoit :

1. Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives.

2. Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j). Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants :

a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ;

b) le fait que la violation a été commise délibérément ou par négligence ;

c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ;

d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32 ;

e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant ;

f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs ;

g) les catégories de données à caractère personnel concernées par la violation ;

h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation ;

i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures ;

j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42 ; et

k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

182. **Sur les injonctions et la conformité**, la formation restreinte souligne que la société a corrigé l'ensemble des manquements relevés dans le rapport de sanction au cours de la procédure. Sa conformité étant démontrée à ce jour, la formation restreinte considère qu'aucune injonction ne se justifie.

183. **Sur le prononcé d'une amende et son montant**, la formation restreinte estime que, dans le cas d'espèce, les manquements précités justifient que soit prononcée une amende administrative à l'encontre de la société.

184. Concernant l'amende proposée par le rapporteur, la société soutient d'abord que le montant de l'amende proposée est excessif, plusieurs manquements n'étant, selon elle, pas constitués. Sur ce point, la formation restreinte considère que l'ensemble des manquements relevés par le rapporteur sont caractérisés en l'espèce, comme elle l'a détaillé précédemment dans les motifs de la décision.

185. La société soutient ensuite que les facteurs d'atténuation posés par l'article 83 du Règlement doivent amener à réduire le montant proposé par le rapporteur et que l'important travail de mise en conformité opéré doit être pris en compte.

186. La formation restreinte analyse les critères dressés par l'article 83 de la manière suivante.

187. S'agissant de la nature, de la gravité et de la durée de la violation, elle considère que ce critère est particulièrement caractérisé pour plusieurs manquements, notamment ceux relatifs aux durées de conservation des données personnelles, aux modalités d'exercice de droit et au dépôt de cookies. S'agissant du manquement relatif au droit à l'effacement et à l'opposition à la prospection, la formation restreinte relève le caractère résiduel de ces cas au regard du nombre important de demandes d'effacement auxquelles le responsable de traitement a fait face depuis l'entrée en application du RGPD. Elle souligne que le nombre de plaintes reçues par la Commission est limité et résulte, à chaque fois, de défaillances isolées. Elle reconnaît les modifications apportées par la société pour se mettre en conformité sur ce point ainsi que pour internaliser la prise en compte de l'opposition des personnes et améliorer le traitement des demandes et le respect des droits. S'agissant du manquement relatif à la sécurité des données, la formation restreinte estime que la gravité de ce manquement est atténuée par la mise en œuvre rapide de mesures limitant pour partie la survenance du risque. S'agissant enfin de l'opposition à la prospection par voie électronique, la formation restreinte note que l'incident était ponctuel. Concernant le nombre de personnes concernées, ce critère est particulièrement aggravant pour le manquement relatif à la durée de conservation des données, qui a concerné plusieurs millions de personnes, pour l'information, puisque chaque personne ayant adhéré au programme fidélité ou ayant créé un compte sur le site carrefour.fr a été concernée, et pour le manquement relatif aux cookies, puisque des cookies ont été déposés sans consentement sur le terminal des 1,7 millions de visiteurs unique du site. Ce critère est, en revanche atténuant s'agissant des difficultés rencontrées lors de l'exercice du droit d'accès (trois personnes concernées), du droit à l'effacement des données (quatre personnes concernées), du droit d'opposition (deux personnes concernées) et de l'opposition à la prospection par voie électronique (350 personnes concernées sur les 350 000 personnes ciblées par la campagne). Sur l'ensemble des manquements, la formation restreinte considère le niveau de dommage subi comme peu important.

188. La formation restreinte relève que la plupart des manquements résultent de négligences, d'erreurs ponctuelles ou d'un manque d'anticipation des conséquences de l'entrée en application du Règlement.

189. S'agissant des mesures prises par le responsable du traitement pour atténuer le dommage subi par les personnes concernées, la formation restreinte note la parfaite coopération de la société tout au long de la procédure de sanction et les efforts très importants engagés afin d'atteindre une conformité totale au jour de la séance. Elle relève que l'ensemble des manquements ont été corrigés à ce jour.

190. S'agissant du degré de coopération avec l'autorité de contrôle, la formation restreinte constate la parfaite coopération de la société, tant dans la facilitation des investigations de la CNIL que dans la prise en compte, avant même la décision de la formation restreinte, des observations du rapporteur. Elle relève également que la société s'est conformée à l'analyse juridique du rapporteur sur l'ensemble des manquements relevés, même dans les cas où une divergence d'opinion demeurait.

191. S'agissant des catégories de données à caractère personnel concernées, la formation restreinte relève qu'aucune donnée sensible n'était concernée par les traitements.

192. S'agissant de la manière dont l'autorité de contrôle a eu connaissance de la violation, la formation restreinte relève que des plaintes sont, pour nombre de manquements, à l'origine de son action.

193. S'agissant des avantages tirés des manquements, la formation restreinte estime que la société n'en a tiré aucun avantage financier. Elle a démontré notamment que, même lorsque les durées de conservation des données étaient dépassées, elles ne pouvaient pas être utilisées à des fins de prospection. Elle a en outre engagé des moyens financiers conséquents pour se mettre en conformité pendant la procédure de sanction.

194. En conclusion, la formation restreinte relève le nombre et la gravité des manquements à certaines obligations essentielles d'un responsable de traitement, comme l'information ou le respect des droits des personnes. Elle relève également que certains manquements étaient structurels. Tel était le cas, par exemple, du sous-dimensionnement des moyens engagés pour répondre aux demandes d'exercice de droit, entraînant de manière récurrente des délais de réponse anormalement longs sans que les personnes soient informées du traitement de leur demande, ou le retard pris dans la purge des données à caractère personnel dont la durée de conservation était expirée. Sur ces points, la formation restreinte souligne également le nombre particulièrement important de personnes concernées au regard des plusieurs dizaines de millions de clients dont les données personnelles figurent dans les bases de données de la société. La formation restreinte note enfin que les manquements ont été portés à son attention en raison d'un grand nombre de plaintes reçues par la CNIL concernant ce responsable de traitement. Ce volume important de plaintes est d'ailleurs à l'origine de la décision de diligenter un contrôle à l'encontre de cette société.

195. Dès lors, la formation restreinte considère qu'une amende doit être prononcée.

196. **Sur l'assiette de l'amende**, la société conteste en outre le mode de calcul de l'assiette de la sanction.

197. Sur ce point, la formation restreinte rappelle que l'article 83-5 du Règlement dispose que le montant des amendes prononcées pour les manquements retenus peut s'élever *dans le cas d'une entreprise,jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent* . Elle souligne que le considérant 150 du Règlement précise que *lorsque des amendes administratives sont imposées à une entreprise, ce terme doit, à cette fin, être compris comme une entreprise conformément aux articles 101 et 102 du traité sur le fonctionnement de l'Union européenne* . La formation restreinte considère donc que le Règlement fait une référence directe et explicite, dans le contexte particulier de la détermination du montant des amendes, au droit de la concurrence que concernent les articles 101 et 102 du traité sur le fonctionnement de l'Union européenne (ci-après le TFUE). La formation restreinte rappelle que les lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement 2016/679, adoptées le 3 octobre 2017 par le G29, précisent à ce sujet que *pour infliger des amendes effectives, proportionnées et dissuasives, les autorités de contrôle s'en remettront à la définition de la notion d'entreprise fournie par la CJUE aux fins de l'application des articles 101 et 102 du traité FUE, à savoir que la notion d'entreprise doit s'entendre comme une unité économique pouvant être formée par la société mère et toutes les filiales concernées. Conformément au droit et à la jurisprudence de l'Union, il y a lieu d'entendre par entreprise l'unité économique engagée dans des activités commerciales ou économiques, quelle que soit la personne morale impliquée (considérant 150).*

198. La formation restreinte considère que les filiales détenues par la société CARREFOUR FRANCE et bénéficiant des traitements doivent être considérées comme concernées au sens des lignes directrices précitées. En effet, dans le contexte du droit de la concurrence auquel le considérant 150 du Règlement fait directement référence, une entreprise *doit être comprise comme désignant une unité économique même si, du point de vue juridique, cette unité économique est constituée de plusieurs personnes physiques ou morales* (arrêt du 12 juillet 1984, Hydrotherm, 170/83, Rec. p. 2999, point 11 , repris dans l'arrêt Confederación Española de Empresarios de Estaciones de Servicio, ECLI:EU:C:2006:784, point 40).

199. La formation restreinte rappelle également que les amendes prononcées doivent avoir un caractère dissuasif. Au regard de cette exigence, il a été jugé que *une imputation de la responsabilité au successeur économique est justifiée aux fins de la mise en œuvre efficace des règles de la concurrence. En effet, si la Commission ne disposait pas d'une telle faculté, il serait aisé pour des entreprises de pouvoir échapper à des sanctions par des restructurations, des cessions ou d'autres changements juridiques ou organisationnels. L'objectif de réprimer les comportements contraires aux règles de la concurrence et d'en prévenir le renouvellement au moyen de sanctions dissuasives serait ainsi compromis* (arrêt du Trib. UE, 29 février 2016, Schenker contre Commission européenne, affaire T-265/12, point 193).

200. La formation restreinte considère que l'organisation juridique du groupe, et notamment de la société CARREFOUR FRANCE et de ses filiales, rendrait *de facto* sans effet toute amende qui serait prononcée sur le seul chiffre d'affaires de la société CARREFOUR FRANCE. La formation restreinte rappelle que la société CARREFOUR FRANCE a réalisé, en 2019, un chiffre d'affaires d'environ 14 millions d'euros et un résultat net déficitaire de 1,6 milliards d'euros. Ces chiffres étaient du même ordre en 2018 (chiffre d'affaires d'environ 25 millions d'euros et résultat net déficitaire de 1,4 milliards d'euros). CARREFOUR FRANCE appartient pourtant à un groupe dont l'activité économique est d'un ordre de grandeur totalement différent, présentant un chiffre d'affaires d'environ 80 milliards d'euros (environ 40 milliards d'euros en France) pour un résultat net ajusté, part du groupe, bénéficiaire d'environ 900 millions d'euros en 2019. Certaines filiales de la société CARREFOUR FRANCE réalisent un chiffre d'affaires particulièrement important. À titre d'exemple, la société CARREFOUR HYPERMARCHÉS (détenue à 81,73% par la société CARREFOUR FRANCE) a réalisé, en 2019, un chiffre d'affaires de 14,3 milliards d'euros et la société CARREFOUR PROXIMITÉ FRANCE (détenue à 99% par la société CARREFOUR FRANCE) a réalisé en 2019 un chiffre d'affaires de 636 millions d'euros.

201. En conséquence, la formation restreinte considère que, pour apprécier la notion d'entreprise conformément aux articles 101 et 102 du TFUE, il convient de prendre en compte le chiffre d'affaires réalisé par la société CARREFOUR FRANCE et par les filiales qu'elle détient et qui ont bénéficié des traitements. Il ressort des déclarations de la société lors du contrôle réalisé le 28 mai 2019 que les sociétés CARREFOUR HYPERMARCHÉS et CARREFOUR PROXIMITÉ FRANCE profitent du programme de mutualisation des données. Le service Marketing France de la société CARREFOUR FRANCE traite en effet les données mutualisées des clients de ces sociétés (nom, prénom, adresse physique et électronique, numéro de téléphone, historique d'achat) afin de leur adresser des publicités personnalisées pour les produits vendus dans ces enseignes. La formation restreinte souligne aussi que ces sociétés participent à la collecte des données à caractère personnel, puisque l'adhésion au programme fidélité est possible directement en magasin au travers de formulaires papier.

202. En conclusion, la formation restreinte retient que le chiffre d'affaires de l'entreprise, au sens d'unité économique, servant de base au calcul de l'assiette de l'amende s'élève à 14,9 milliards d'euros en 2019.

203. La formation restreinte considère néanmoins que la détermination du montant de l'amende doit prendre en compte la spécificité du modèle économique du secteur concerné, celui de la grande distribution, caractérisé par un chiffre d'affaires particulièrement élevé au regard des résultats nets dégagés par l'activité, celle-ci se distinguant par des volumes extrêmement importants et des marges faibles.

204. Dès lors, elle estime qu'une amende d'un montant de 2 250 000 euros est justifiée et proportionnée aux manquements relevés et à la situation de la société CARREFOUR FRANCE.

205. **Sur la publicité de la décision,** la société estime que la publicité de la sanction ne se justifie pas.

206. La formation restreinte considère, premièrement, que la gravité de certains manquements justifie, par elle-même, la publicité de la présente décision.

207. La formation restreinte rappelle, deuxièmement, que les manquements relatifs à la durée de conservation des données, aux modalités d'exercice des droits ou à l'information délivrée ont concerné un très grand nombre de personnes. Elle considère que la publicité de sa décision est le meilleur moyen d'informer les personnes de l'existence passée de ces manquements. Elle note que les personnes ne peuvent avoir connaissance de certains manquements (comme celui relatif à la durée de conservation) que grâce à cette publicité de sa décision.

208. Il résulte de tout ce qui précède et de la prise en compte des critères fixés à l'article 83 du règlement qu'une amende administrative à hauteur de 2 250 000 euros ainsi qu'une sanction complémentaire de publication pour une durée de deux ans sont justifiées et proportionnées.

PAR CES MOTIFS

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

· **prononcer à l'encontre de la société CARREFOUR FRANCE une amende administrative d'un montant de 2 250 000 (deux millions deux cent cinquante mille) euros pour les manquements aux articles 5-1 e), 12, 13, 15, 17, 21, 32 et 33 du RGPD, à l'article L34-5 du code des postes et des communications électroniques et à l'article 82 (anciennement 32.II) de la loi informatique et libertés ;**

· **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.