Délibération de la formation restreinte n° SAN-2020-009 du 18 novembre 2020 concernant la société CARREFOUR BANQUE

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

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

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

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

Vu les décisions no 2019-081C du 24 avril 2019 et no 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 la société CARREFOUR BANQUE ;

Vu la décision de la vice-présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 29 novembre 2019 ;

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

Vu les observations écrites versées par le conseil de la société CARREFOUR BANQUE 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 BANQUE reçues le 24 août 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 BANQUE :

- […] ;

- […] ;

- […] ;

- […] ;

- […] ;

- […] ;

- […].

La société CARREFOUR BANQUE ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La société CARREFOUR BANQUE est une filiale détenue à 40 % par la société BNP PARIBAS S.A. et à 60 % par la société CARREFOUR S.A., maison-mère du groupe CARREFOUR.

2. Créé en 1959, le groupe CARREFOUR (ci-après le groupe), dont le siège est au 93 avenue de Paris à Massy (91300), a pour activité principale la grande distribution. Il intervient également dans d'autres domaines comme le secteur bancaire et assurantiel, le commerce en ligne et les agences de voyages. En 2018, il employait environ 360 000 salariés et avait réalisé un chiffre d'affaires de 76 milliards d'euros.

3. Sise au 1 place Copernic Courcouronnes à Évry Courcouronnes (91080), la société CARREFOUR BANQUE (ci-après la société) est un établissement bancaire ayant pour activités principales le crédit à la consommation, la gestion de portefeuilles, le courtage en assurance ainsi que les services d'investissement. En 2018, elle employait environ 300 salariés et avait réalisén produit net bancaire de 308 millions d'euros.

4. Dans le cadre de ses activités, la société édite le site web www.carrefour-banque.fr (ci-après le site carrefour-banque.fr). Elle commercialise également une carte de paiement destinée aux clients du groupe Carrefour (ci-après la carte Pass), qui peut être rattachée au programme de fidélité du groupe.

5. En application des décisions no 2019-081C du 24 avril 2019 et no 2019-102C du 6 juin 2019 de la présidente de la Commission, les services de la CNIL ont procédé à un contrôle en ligne, le 5 juillet 2019, relatif au site carrefour-banque.fr et aux traitements mis en œuvre à partir de ce site ainsi qu'à un contrôle sur place dans les locaux de la société CARREFOUR S.A., le 9 juillet 2019, relatif aux traitements concernant la carte Pass.

6. Ces missions avaient pour objet de vérifier, notamment, 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 no 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après la loi informatique et libertés).

7. Dans le cadre du contrôle sur place, les représentants du groupe CARREFOUR ont précisé à la délégation que la société CARREFOUR BANQUE est responsable de traitement des deux programmes paiement (débit et crédit) de la carte Pass tandis que la société CARREFOUR FRANCE est responsable de traitement du troisième programme permettant le rattachement de la carte Pass à la base de données SIEBEL qui met en œuvre le programme de fidélité Carrefour.

8. Le 19 juillet 2019, la société a transmis à la délégation de contrôle les documents demandés dans le cadre du contrôle sur place du 9 juillet 2019 et notamment le comptage du nombre de cartes Pass rattachées au programme de fidélité Carrefour.

9. Aux fins d'instruction de ces éléments, la vice-présidente de la Commission a désigné Monsieur Éric PÉRÈS en qualité de rapporteur, le 29 novembre 2019, sur le fondement de l'article 22 de la loi informatique et libertés .

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

11. 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 et 13 du Règlement et de 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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 deuxième report de la séance de la formation restreinte, prévue le 21 avril 2020.

17. 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.

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

19. 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.

20. 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 L 151-1 du code du commerce.

21. 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.

22. Le 24 août 2020, la société a produit de nouvelles observations en réponse à celles du rapporteur.

23. 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 traiter les données de manière loyale

24. Aux termes de l'article 5, paragraphe 1, a), du RGPD : Les données à caractère personnel doivent être: a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) .

25. Il ressort des constatations effectuées par la délégation de contrôle que lorsqu'un souscripteur d'une carte de paiement (carte Pass) souhaite également adhérer au programme de fidélité Carrefour, la société CARREFOUR BANQUE fait plusieurs requêtes à la société CARREFOUR FRANCE dont, notamment, une demande d'adhésion au programme de fidélité Carrefour.

26. En effet, lors du contrôle en ligne, la délégation a constaté que s'il veut adhérer au programme de fidélité Carrefour, le souscripteur de la carte Pass doit notamment cocher la case située au bas de la page intitulée Ma fidélité récompensée au soutien de laquelle figure la mention suivante : Je souhaite rattacher mon compte Fidélité Carrefour à ma carte Pass (ou à défaut le créer et le rattacher). Pour cela, j'accepte que Carrefour Banque communique à Carrefour Fidélité mon nom, prénom et email. Carrefour Banque s'engage à ne transmettre aucune autre information à Carrefour Fidélité .

27. Il ressort des pièces remises à la délégation lors du contrôle sur place que la société CARREFOUR BANQUE transmet également à la société CARREFOUR FRANCE, en plus des nom, prénom et adresse électronique du souscripteur de la carte Pass mentionnés ci-avant, son adresse postale ainsi que son ou ses numéros de téléphone. Lorsqu'elle dispose de ces informations, elle renseigne aussi la société CARREFOUR FRANCE sur le nombre d'enfants déclarés par le souscripteur.

28. Le rapporteur considère ainsi que la société a manqué au principe de loyauté dès lors qu'elle transmettait à la société CARREFOUR FRANCE plus de données à caractère personnel concernant les souscripteurs de la carte Pass que celles limitativement énumérées dans le cadre du parcours de souscription en ligne.

29. La société répond, tout d'abord, que la notion de loyauté n'étant pas définie dans le Règlement, le rapporteur ne saurait demander à la formation restreinte d'en sanctionner la violation.

30. Elle relève, par ailleurs, que le principe de loyauté peut tout au plus être rattaché à l'obligation de transparence, prévue à l'article 12 du Règlement. En l'occurrence, elle avance s'être conformée à cette exigence de transparence dès lors que la mention d'information mise en cause par le rapporteur informe les personnes de l'existence du traitement, de sa finalité ainsi que du transfert de ces données à des tiers.

31. Elle soutient, enfin, que les pratiques dénoncées pourraient d'autant moins être qualifiées de déloyales qu'elles ne résulteraient que d'un défaut de mise à jour de son web, dû à une erreur de communication entre les différents services des deux sociétés.

32. La formation restreinte rappelle que le principe de loyauté est un principe autonome prévu à l'article 5, paragraphe 1, a), du RGPD dont la violation par un responsable de traitement est susceptible de donner lieu au prononcé d'une mesure correctrice de la part de l'autorité de contrôle.

33. Elle relève, à cet égard, que cette disposition doit être interprétée à la lumière du considérant 60 du Règlement, aux termes duquel : le principe de traitement loyal et transparent exige que la personne concernée soit informée de l'existence de l'opération de traitement et de ses finalités. Le responsable du traitement devrait fournir à la personne concernée toute autre information nécessaire pour garantir un traitement équitable et transparent, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées .

34. En l'occurrence, la formation restreinte considère que l'information fournie dans cette mention était à la fois imprécise et trompeuse.

35. Tout d'abord, la formation restreinte relève que la société CARREFOUR BANQUE mentionne Carrefour Fidélité comme destinataire des données communiquées alors mêmeque ce service, rattaché à la société CARREFOUR FRANCE, n'avait, avant cette mention, jamais été présenté aux souscripteurs de la carte Pass. Ainsi, les personnes concernées ne pouvaient

comprendre d’elles-mêmes que leurs données à caractère personnel étaient en fait communiquées à une société tierce, la société CARREFOUR FRANCE.

36. Ensuite, la formation restreinte considère que l’information fournie aux personnes concernées était trompeuse et déloyale dès lors que la société avait expressément indiqué, dans cette même mention d’information, qu’elle s’engage[ait] à ne transmettre aucune autre information à Carrefour Fidélité que les noms, prénoms et adresse électronique des souscripteurs à la carte Pass alors même que tel n’était précisément pas le cas.

37. La formation restreinte considère donc qu’un manquement à l’article 5, paragraphe 1, a), du RGPD était constitué.

38. Elle relève, néanmoins, qu’au jour de la séance, la société avait entièrement refondu le parcours de souscription en ligne à la carte Pass et, notamment, réécrit la mention d’information contestée. Les souscripteurs de la carte Pass souhaitant être rattachés au programme de fidélité Carrefour sont désormais informés du fait que des données à caractère personnel les concernant sont transmises à la société CARREFOUR FRANCE et sont également renseignés sur la nature exacte des données effectivement transmises.

B. Sur le manquement relatif à l’information des personnes

39. L’article 12 du Règlement 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 […] .

40. L’article 13 de ce même Règlement dresse la liste des informations devant être communiquées aux personnes concernées lorsque les données à caractère personnel sont collectées auprès d’elles.

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

41. En premier lieu, le rapporteur considère que, tel qu’il ressort des constations effectuées par la délégation lors du contrôle en ligne, l’information mise à disposition des utilisateurs du site carrefour-banque.fr par le biais de différents canaux, n’était pas aisément accessible au sens de l’article 12 du Règlement.

42. Pour prendre connaissance de l'information fournie quant au traitement de ses données à caractère personnel, l'utilisateur pouvait tout d'abord cliquer sur l'onglet Protection des données bancaires figurant en pied de page du site. Alternativement, il pouvait également cliquer sur le lien Mentions légales figurant en pied de page du site, parvenir au point 3 de ces mentions, intitulé 3 - Protection et confidentialité des données personnelles traitées par Carrefour Banque et, enfin, cliquer sur le lien Pour en savoir plus sur notre politique de protection des données personnelles consultez notre page dédiée , lequel renvoyait à la politique de confidentialité de la société intitulée Protection et confidentialité des données personnelles traitées par Carrefour Banque , sans qu'aucune autre information n'ait été préalablement fournie à l'utilisateur avant d'atteindre cette politique de confidentialité.

43. La société soutient qu'elle était parfaitement fondée à insérer un lien renvoyant vers sa politique de confidentialité dans ses mentions légales et qu'en tout état de cause, cette information était fournie directement via l'onglet Protection des données bancaires figurant en pied de page du site.

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

45. Elle relève, à cet égard, que cette disposition doit être interprétée à la lumière du considérant 61 du Règlement, aux termes duquel : les informations sur le traitement des données à caractère personnel relatives à la personne concernée devraient lui être fournies au moment où ces données sont collectées auprès d'elle .

46. En ce sens, elle partage la position du G29 présentée dans les lignes directrices sur la transparence au sens du Règlement, adoptées dans leur version révisée le 11 avril 2018 (ci-après les lignes directrices sur la transparence), qui rappelle que la personne concernée ne devrait pas avoir à rechercher les informations mais devrait pouvoir tout de suite y accéder .

47. Pour illustrer comment il est possible de satisfaire à ce critère d'accessibilité, ces mêmes lignes directrices précisent, s'agissant d'un environnement en ligne que, chaque entreprise disposant d'un site internet devrait publier une déclaration ou un avis sur la protection de la vie privée sur son site. Un lien direct vers cette déclaration ou cet avis sur la protection de la vie privée devrait être clairement visible sur chaque page de ce site internet sous un terme communément utilisé (comme Confidentialité, Politique de confidentialité ou Avis de protection de la vie privée). Les textes ou liens dont la mise en page ou le choix de couleur les rend moins visibles ou difficiles à trouver sur une page web ne sont pas considérés comme aisément accessibles .

48. En l’espèce, la formation restreinte considère, d’abord, que l’imprécision de l’intitulé de l’onglet Protection des données bancaires figurant en pied de page du site, évoquant les données bancaires et non les données à caractère personnel, ne pouvait permettre aux personnes concernées de comprendre aisément qu’en cliquant sur ce lien elles allaient être redirigés vers la politique de confidentialité du site, comportant les informations relatives au traitement de leurs données à caractère personnel. En effet, pour le grand public, une part importante des données traitées (adresse, nombre d’enfants, etc.) ne relève pas des données bancaires .

49. Ensuite, s’agissant du second canal d’information, les utilisateurs du site carrefour-banque.fr ne pouvaient deviner d’eux-mêmes que le lien renvoyant vers la politique de confidentialité du site était inséré dans les mentions légales du site. Ainsi, pour parvenir jusqu’à cette politique de confidentialité, les utilisateurs devront, dans un certain nombre de cas, entreprendre préalablement plusieurs actions, comme, par exemple, cliquer sur les liens Accessibilité ou Conditions générales de vente figurant également en pied de la page d’accueil, avant de cliquer finalement sur le lien Mentions légales .

50. Il en résulte que l’information fournie aux utilisateurs du site carrefour-banque.fr n’était pas aisément accessible .

51. En deuxième lieu, le rapporteur estime que l’information relative à la carte Pass fournie dans le cadre du parcours de souscription en ligne sur le site carrefour-banque.fr et telle que constatée lors du contrôle en ligne n’était pas non plus aisément accessible dès lors que les souscripteurs de cette carte ne disposaient pas d’une information complète relative au traitement de leurs données sur la page de présentation du parcours de souscription et qu’ils n’étaient pas, non plus, invités à prendre connaissance d’une information plus complète, par exemple par le biais d’un lien hypertexte renvoyant vers des mentions d’information complémentaires.

52. La société soutient qu’un tel lien existait déjà à travers l’onglet Protection des données bancaires figurant en pied de page du site.

53. La formation restreinte souligne que selon le principe de transparence, tel que notamment rappelé dans le considérant 61 du RGPD, les informations doivent être communiquées aux personnes au moment où les données sont collectées.

54. A titre d’exemple, les lignes directrices sur la transparence du G29 mentionnent que, dans un contexte en ligne, il convient qu’ un lien vers la déclaration ou l’avis sur la protection de la vie privée soit fourni au point de collecte des données à caractère personnel, ou que ces

informations soient consultables sur la même page que celle où les données à caractère personnel sont collectées .

55. En l'espèce, il ressort des constatations que la société a fait le choix d'adopter une information à plusieurs niveaux.

56. A cet égard, si la société fournissait bien, dans la page de présentation du parcours de souscription à la carte Pass les mentions attendues au titre d'une information de premier niveau, à savoir l'identité du responsable de traitement, les finalités principales du traitement et la description des droits Informatique et Libertés , la formation restreinte relève en revanche que la société avait négligé de compléter ces mentions en permettant aux personnes de prendre connaissance d'une information complète en insérant, par exemple, un lien hypertexte renvoyant vers une information de deuxième niveau, en l'occurrence, vers la politique de confidentialité de la société, censée détailler l'ensemble des mentions d'informations exigées par l'article 13 du Règlement.

57. S'agissant de l'onglet Protection des données bancaires mis en avant par la société, la formation restreinte relève que cet onglet ne figurait pas en pied de page du parcours de souscription en ligne à la carte Pass et rappelle qu'en tout état de cause son intitulé n'aurait pas permis aux personnes concernées de comprendre aisément qu'en cliquant sur ce lien elles allaient être redirigées vers la politique de confidentialité de la société.

58. De la sorte, les personnes concernées n'étaient pas informées, au moment de la collecte de leurs données à caractère personnel, de toutes les informations afférentes au traitement. Il en résulte que toutes les informations fournies aux souscripteurs de la carte Pass sur le site carrefour-banque.fr n'étaient pas aisément accessibles .

59. La formation restreinte considère donc que la société a méconnu les dispositions de l'article 12 du Règlement.

60. Elle relève, néanmoins, qu'au jour de la séance, la société avait entièrement refondu son site web et que l'information aujourd'hui fournie tant aux utilisateurs du site qu'aux souscripteurs de la carte Pass satisfait désormais aux exigences de l'article 12 du Règlement.

2. S'agissant du contenu de l'information

61. Le rapporteur considère que la politique de confidentialité de la société, intitulée Protection et confidentialité des données personnelles traitées par Carrefour Banque et

accessible selon les modalités rappelées ci-avant, était à la fois imprécise et lacunaire s'agissant des mentions relatives aux durées de conservation. Ainsi, d'une part, la politique d'information comportait des formulations trop vagues, ne permettant pas d'identifier des durées définies et, d'autre part, la société ne donnait aucune information concernant certaines données qu'elle indiquait pourtant collecter, telles que les données de comportement, d'habitudes et de préférences de consommation en ligne collectées par les cookies déposés sur le terminal des utilisateurs à partir de son site web. Par ailleurs, la société ne précisait pas si elle archivait ou non les données des personnes concernées.

62. La société conteste le caractère imprécis de ses mentions d'information relatives aux durées de conservation et fait valoir que l'information relative aux cookies était disponible dans un autre développement de ses Mentions légales .

63. La formation restreinte rappelle qu'aux termes de l'article 13, paragraphe 2, a) du Règlement, le responsable du traitement fournit à la personne concernée les informations relatives à la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée .

64. A titre d'éclairage, les lignes directrices sur la transparence précitées recommandent que la durée de conservation [soit] formulée de manière à ce que la personne concernée puisse évaluer, selon la situation dans laquelle elle se trouve, quelle sera la période de conservation s'agissant de données spécifiques ou en cas de finalités spécifiques. Le responsable du traitement ne peut se contenter de déclarer de façon générale que les données à caractère personnel seront conservées aussi longtemps que la finalité légitime du traitement l'exige. Le cas échéant, différentes périodes de stockage devraient être mentionnées pour les différentes catégories de données à caractère personnel et/ou les différentes finalités de traitement, notamment les périodes à des fins archivistiques .

65. En l'espèce, la formation restreinte souligne, tout d'abord, que l'emploi de formules vagues et non définies telles que lesdélais de prescription légale applicables ou la conservation de vos données par Carrefour Banque varie selon les réglementations et lois applicables ou encore des expressions à titre d'exemple ou de l'adverbe notammentrendaient nécessairement confuse pour les personnes concernées la compréhension de l'étendue et de la nature des données conservées ainsi que des durées de conservation appliquées à ces données.

66. Elle ajoute, ensuite, que l'information était également incomplète dans la mesure où la société négligeait de préciser les durées de conservation applicables à toutes les données traitées ou ne précisait pas les critères utilisés pour déterminer ces durées. Ainsi, la société ne précisait pas qu'elle archivait les données contractuelles pendant cinq ans, durée de la prescription légale applicable, en cas de contentieux. Par ailleurs, elle ne précisait pas les durées de conservation des données collectées par les cookies, dès lors que si les Mentions

légales du site comportaient bien un paragraphe relatif aux cookies, ce dernier ne précisait pas les durées de conservation des données collectées par ces cookies.

67. La formation restreinte considère donc qu'un manquement à l'article 13 du Règlement était constitué.

68. Elle relève, néanmoins, qu'au jour de la séance, la société avait complété ses mentions d'information et que sa politique de confidentialité satisfait désormais aux exigences de l'article 13 du Règlement.

C. Sur le manquement relatif aux cookies

69. 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 leur équipement. Tout dépôt de cookie ou autre traceur doit donc être précédé de l'information et du consentement des utilisateurs. 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 .

70. Le rapporteur considère que la société ne respectait pas ces dispositions dès lors qu'il a été constaté lors du contrôle en ligne qu'en arrivant sur le site web carrefour-banque.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.

71. La société ne conteste pas ces éléments.

72. La formation restreinte relève, en l'espèce, que le dépôt de trente et un cookies était automatique dès l'arrivée sur la page d'accueil du site et avant toute action de l'utilisateur.

73. La formation restreinte observe que cinq de ces cookies (les cookies MUIDB , GPS et gid , _ga et _gat_trackerBanque) n'avaient ni pour finalité exclusive de permettre ou de faciliter la communication par voie électronique, ni n'étaient strictement nécessaires à la fourniture d'un service expressément demandé par l'utilisateur.

74. S’agissant, d’abord, des trois cookies gid , _ga et _gat_trackerBanque , 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 .

75. S’agissant, ensuite, des cookies MUIDB et GPS , la formation restreinte relève que ces deux cookies sont des cookies de traçage, le premier permettant de suivre un utilisateur se rendant sur différents noms de domaine appartenant à la société Microsoft, le second enregistrant un identifiant sur le terminal de l’utilisateur afin de le géolocaliser. Dès lors, le dépôt de ces cinq cookies aurait dû obliger la société à recueillir préalablement le consentement de l’utilisateur.

76. La formation restreinte considère donc qu’un manquement à l’article 82 de la loi informatique et libertés était constitué.

77. Elle relève, néanmoins, qu’au jour de la séance, la société avait entièrement refondu sa politique en matière de cookies. 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 4 mars 2020.

III. Sur les mesures correctrices et la publicité

78. Aux termes du III de l’article 20 de la loi informatique et libertés :

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.

79. 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.

80. En premier lieu, concernant la proposition de sanction, la société soutient que dès lors que les manquements à la loyauté et à l'information ne seraient pas caractérisés, le prononcé d'une amende administrative n'apparaît pas nécessaire.

81. Elle avance qu'il conviendrait en tout état de cause de réduire le montant de l'amende proposée, dans la mesure où les manquements reprochés sont dénués de gravité et qu'elle a opéré, depuis le début de la procédure de sanction, un important travail de mise en conformité.

82. Au regard des critères pertinents prévus à l'article 83 du Règlement, la formation restreinte considère, au contraire, que le prononcé d'une amende administrative s'avère nécessaire.

83. En l'occurrence, s'agissant, premièrement, de la nature, de la gravité et de la durée de la violation, la formation restreinte note que ce critère est caractérisé pour le manquement lié à la loyauté dès lors que la société a fourni à ses clients une information contraire à la réalité des traitements mis en œuvre.

84. Deuxièmement, s’agissant du nombre de personnes concernées, la formation restreinte souligne que le manquement relatif aux cookies a concerné un nombre important de personnes dès lors que les cookies permettaient de suivre de la même façon, sans distinction, le comportement en ligne des souscripteurs de la carte Pass et des prospects éventuels de la société mais également de tous les internautes susceptibles de naviguer sur son site web.

85. Par ailleurs, les manquements à la loyauté et à l’information ont concerné aussi l’ensemble des souscripteurs de la carte Pass rattachés ou non au programme de fidélité Carrefour lesquels, selon les éléments relevés par la délégation de contrôle, s’élèvent à au moins […] de personnes.

86. Troisièmement, s’agissant des mesures prises par le responsable du traitement pour atténuer le dommage subi par les personnes concernées et du degré de coopération avec l’autorité de contrôle, 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 les trois manquements ont été corrigés à ce jour.

87. S’agissant du montant de l’amende administrative, la formation restreinte rappelle qu’en 2018 la société a réalisé un produit net bancaire de 308 millions d’euros et qu’en application des dispositions de l’article 83, paragraphe 5, elle encourt une sanction financière d’un montant maximum de 20 millions d’euros.

88. Dès lors, au regard des capacités financières de la société et des critères pertinents de l’article 83, paragraphe 2, du Règlement évoqués ci-avant, la formation restreinte estime que le prononcé d’une amende de 800 000 €, qui ne représenterait donc que 0,25% de ce produit net bancaire, apparaît à la fois effectif, proportionné et dissuasif, conformément aux exigences de l’article 83, paragraphe 1, de ce Règlement.

89. En deuxième lieu, concernant le prononcé d’une injonction, la société soutient que dans la mesure où elle a remédié à l’ensemble des manquements qui lui sont reprochés, les demandes formulées au titre de l’injonction proposée sous astreinte perdent tout fondement.

90. La formation restreinte relève en effet que, dès lors que la société a corrigé l’ensemble des manquements relevés dans le rapport de sanction, le prononcé d’une injonction ne se justifie plus.

91. En troisième lieu, concernant la publicité de la présente décision, la société soutient qu'une telle mesure ne respecterait pas le principe constitutionnel de nécessité des peines dès lors qu'elle se serait déjà inscrite dans une démarche consistant à renforcer la conformité de sa situation aux exigences de la règlementation sur la protection des données. Elle ajoute que la publicité aurait des conséquences particulièrement dommageables en ce qu'elle risquerait d'affecter sa réputation de manière durable.

92. La formation restreinte considère que la publicité de la présente décision se justifie au regard de la gravité des manquements sanctionnés et du nombre de personnes concernées.

93. Elle estime que cette mesure permettra d'informer l'ensemble des clients et des prospects potentiels de la société de l'existence de différents manquements sanctionnés et notamment des manquements à la déloyauté et aux cookies.

94. Enfin, la mesure n'est pas disproportionnée dès lors que la décision n'identifiera plus nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

95. 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 800 000 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 BANQUE une amende administrative d'un montant de 800 000 (huit cent mille) euros pour les manquements aux articles 5, paragraphe 1, a), 12 et 13 du RGPD et à l'article 82 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