Délibération SAN-2023-008 du 8 juin 2023

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Date de publication sur Légifrance : Jeudi 15 juin 2023
Etat juridique : En vigueur

Délibération de la formation restreinte no SAN-2023-008 du 8 juin 2023 concernant la société KG COM

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

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

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 la décision n° 2020-267C du 20 octobre 2020 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par la société KG COM ou pour son compte ;

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 23 décembre 2021 ;

Vu le rapport de Madame Sophie LAMBREMON, commissaire rapporteure, notifié à la société KG COM le 7 juillet 2022 ;

Vu les observations écrites versées par la société KG COM le 8 août 2022 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 15 septembre 2022 :

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

En qualité de représentants de la société KG COM :

- […]

La société KG COM ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La société KG COM (ci-après " KG COM " ou " la société ") est une société par actions simplifiée, immatriculée au registre du commerce et des sociétés de Lyon sous le numéro 538 563 917, dont le siège social est situé 40 rue de Bruxelles, à

Villeurbanne (69100). La société exploite plusieurs sites web afin de proposer à ses clients des consultations de voyance par chat ou par téléphone, dont le site web http://www.voyance-en-direct.tv/. La société emploie six salariés.

2. En 2019, le chiffre d'affaires net de la société s'élevait à […] euros et son résultat net était de […] euros. En 2020, son chiffre d'affaires net s'élevait à […] euros avec un résultat net déficitaire de […] euros.

3. Le 1er octobre 2020, un article de presse, paru sur le site web du média Numerama, a révélé l'existence d'une violation de données à caractère personnel concernant les données conservées sur le serveur de KG COM. Selon cet article, la base de données de la société ne faisant pas l'objet de mesures de sécurité particulières, celle-ci était librement accessible sur Internet jusqu'au 23 juillet 2020. De nombreuses données, dont des données d'identification et des données de contact, auraient ainsi été exposées.

4. Le 21 janvier 2021, une délégation de contrôle de la Commission nationale de l'informatique et des libertés (ci-après " CNIL " ou " Commission ") a procédé à un contrôle sur pièces en adressant un questionnaire à la société, auquel cette dernière a répondu par un courrier reçu le 25 mars 2021.

5. Un contrôle en ligne a également été effectué le 15 avril 2021 sur le site web www.voyance-en-direct.tv, édité par la société. Le procès-verbal n° 2020-267/1, dressé à l'issue du contrôle, a été notifié à l'organisme le 26 avril 2021. La société a fourni à la délégation des éléments complémentaires par courriels des 17 mai et 18 juin 2021.

6. Un contrôle sur place a été effectué le 15 juillet 2021. Le procès-verbal n° 2020-267/2, dressé à l'issue du contrôle, a été notifié à l'organisme le 21 juillet 2021. Par la suite, la société a fourni à la délégation des éléments complémentaires par courriels des 26 août, 20 septembre, 19 octobre et 3 novembre 2021.

7. La base de données de KG COM comporte les adresses électroniques de […] clients et […] prospects, comme cela ressort des observations en réponse de la société.

8. Conformément à l'article 56 du RGPD, la CNIL a informé l'ensemble des autorités de contrôle européennes de sa compétence pour agir en tant qu'autorité de contrôle chef de file concernant les traitements transfrontaliers mis en œuvre par KG COM, résultant de ce que son établissement unique se trouve en France. Après échanges entre la CNIL et les autorités de protection des données européennes dans le cadre du mécanisme de guichet unique, la Belgique, le Luxembourg, l'Italie, l'Espagne, le Portugal, la Bulgarie, Berlin et l'Irlande se sont déclarées concernées par le traitement.

9. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 23 décembre 2021, désigné Madame Sophie LAMBREMON en qualité de rapporteure, sur le fondement de l'article 22 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après " loi Informatique et Libertés ").

10. Le 7 juillet 2022, la rapporteure a fait notifier à la société KG COM un rapport détaillant les manquements aux dispositions du RGPD et de la loi Informatique et Libertés qu'elle estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de prononcer à l'encontre de la société une amende administrative. Il proposait également que la décision soit rendue publique mais qu'il ne soit plus possible d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

11. Le 2 août 2022, KG COM a sollicité un délai pour répondre au rapport de la rapporteure. Par courrier du 4 août 2022, le président de la formation restreinte a avisé la société de sa décision de ne pas faire droit à cette demande.

12. La société a répondu au rapport de sanction par des observations écrites en date du 8 août 2022.

13. Par courrier du 16 août 2022, la rapporteure a informé le conseil de la société que l'instruction était close, en application de l'article 40, III, du décret modifié n°2019-536 du 29 mai 2019.

14. Le 22 août 2022, le conseil de la société a été informé que le dossier était inscrit à l'ordre du jour de la formation restreinte du 15 septembre 2022.

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

II. Motifs de la décision

16. En application de l'article 60, paragraphe 3, du RGPD, le projet de décision adopté par la formation restreinte a été transmis le 4 mai 2023 aux huit autorités de contrôle européennes qui se sont déclarées concernées.

17. Au 1er juin 2023, aucune des autorités de contrôle concernées n'avait formulé d'objection pertinente et motivée à l'égard de ce projet de décision, de sorte que, en application de l'article 60, paragraphe 6, du RGPD, ces dernières sont réputées l'avoir approuvé.

A. Sur le manquement relatif à l'obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données à caractère personnel traitées en application de l'article 5-1-c du RGPD

18. L'article 5, paragraphe 1, c) du RGPD dispose que les données à caractère personnel doivent être " adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ".

19. En premier lieu, la rapporteure relève que la société enregistre systématiquement l'intégralité des appels téléphoniques passés entre les téléopérateurs et les prospects, ainsi qu'entre les voyants et les clients, à des fins de contrôle de la qualité du service, de preuve de la souscription du contrat et dans la perspective de réquisitions judiciaires. La rapporteure considère que cela conduit à collecter des données non limitées à ce qui est nécessaire au regard des finalités poursuivies.

20. En défense, la société indique avoir cessé de proposer à ses clients des consultations de voyance par téléphone.

21. Afin de justifier les faits passés, elle indique que ces enregistrements lui permettaient de contrôler les propos tenus par les voyants lors des consultations, notamment pour apprécier leurs compétences. Selon elle, l'enregistrement d'un échantillon des consultations ne permettrait pas de répondre à ses besoins.

22. La formation restreinte prend note de l'arrêt des consultations de voyance par téléphone, ce qui implique l'arrêt des enregistrements des appels téléphoniques passés entre les téléopérateurs et les prospects et ceux passés entre les voyants et les clients.

23. Toutefois, la formation restreinte relève qu'au jour des contrôles, la société enregistrait systématiquement et intégralement ces appels téléphoniques à des fins de contrôle de la qualité du service, de preuve de la souscription du contrat et dans la perspective de réquisitions judiciaires.

24. La formation restreinte note que la société ne donne pas de justification, pour le passé, concernant la nécessité d'enregistrer systématiquement l'intégralité des conversations téléphoniques, d'une part, entre les téléopérateurs et les prospects, et d'autre part, entre les voyants et les clients, à des fins de contrôle qualité, de preuve de la souscription du contrat et dans la perspective de réquisitions judiciaires.

25. Or, un responsable de traitement ne peut pas mettre en place un traitement de données à caractère personnel sans s'assurer que celui-ci est nécessaire à ses besoins, a fortiori lorsqu'il repose sur un dispositif particulièrement intrusif pour les salariés.

26. S'agissant de l'enregistrement intégral et systématique des appels téléphoniques à des fins de contrôle de la qualité du service, la formation restreinte considère que la finalité visant à contrôler la qualité du service fourni par les téléopérateurs et les voyants peut être atteinte par un moyen moins intrusif.

27. À cet égard, elle relève que la mise en place d'un enregistrement ponctuel et aléatoire de seulement quelques conversations téléphoniques permet à la personne chargée du suivi du contrôle qualité de disposer des éléments nécessaires à l'évaluation de la qualité des services proposés par la société.

28. Dès lors que le contrôle de la qualité du service peut être réalisé par échantillonnage, la formation restreinte considère que l'instauration d'un dispositif d'enregistrement systématique des appels téléphoniques passés, d'une part, entre les téléopérateurs et les prospects, et d'autre part, entre les voyants et les clients, est excessive au regard de la finalité poursuivie.

29. La formation restreinte rappelle qu'elle a déjà considéré, dans sa délibération n°SAN-2020-003 du 28 juillet 2020, à l'égard d'une société qui procédait à l'enregistrement des conversations téléphoniques reçus par les salariés du service clients d'une société à des fins de formation que " la société ne justifie pas de la nécessité d'enregistrer l'intégralité des conversations téléphoniques passées par le service client, au regard de la finalité du traitement, à savoir la formation des salariés. (…) Si le nombre d'enregistrements peut varier en fonction de chaque salarié et des circonstances, en particulier des besoins de formation de celui-ci, (…) la société ne démontre pas avoir mis en place, pour le passé et l'avenir, un enregistrement des conversations téléphoniques des salariés limité à ce qui est nécessaire au regard de la finalité poursuivie. Or, un responsable de traitement ne peut mettre en place un traitement de données à caractère personnel sans s'assurer que celui-ci est nécessaire à ses besoins, a fortiori lorsqu'il repose sur un dispositif particulièrement intrusif pour les salariés. La formation restreinte considère donc, au vu de ces éléments, qu'un manquement à l'article 5-1-c) du RGPD est constitué ".

30. S'agissant de l'enregistrement intégral et systématique des appels téléphoniques à des fins de de preuve de la souscription du contrat, la formation restreinte relève qu'en l'espèce, les prospects communiquent leurs numéros de téléphone à la société via l'un des sites web qu'elle édite afin d'obtenir des renseignements sur les prestations de voyance

proposées. À la suite de cette demande d'information, les téléconseillers de la société appellent les prospects afin de leur fournir ces informations et le cas échéant, fixer un rendez-vous avec un voyant.

31. La formation restreinte considère qu'un responsable du traitement qui souhaite enregistrer des conversations téléphoniques à des fins probatoires doit démontrer qu'il ne dispose pas d'autres moyens moins intrusifs pour prouver que le contrat conclu à distance a bien a été conclu avec la personne concernée.

32. La formation restreinte considère qu'en l'espèce, l'existence du contrat conclu à distance peut être prouvée par un autre moyen moins intrusif.

33. En effet, l'article L.221-16 du code de la consommation prévoit que, lorsque le professionnel contacte un consommateur par téléphone en vue de conclure un contrat portant sur la vente d'un bien ou sur la fourniture d'un service, ce dernier n'est engagé par cette offre qu'après l'avoir signée et acceptée sur un support durable.

34. La formation restreinte considère donc que, dès lors que la preuve de la souscription d'un contrat conclu à distance, à la suite d'un démarchage téléphonique, peut être apportée par la confirmation écrite de l'offre, l'enregistrement des conversations téléphoniques, passées entre les téléopérateurs et les prospects, à des fins de preuve de la formation du contrat, n'apparaît pas nécessaire.

35. Par ailleurs, la formation restreinte note qu'aucun contrat n'est conclu lors des appels téléphoniques passés entre les voyants et les clients, de sorte que l'enregistrement de ces conversations n'est pas justifié à des fins de preuve de la souscription d'un contrat.

36. S'agissant de l'enregistrement intégral et systématique des appels téléphoniques dans la perspective de réquisitions judiciaires, la formation restreinte relève que s'il est nécessaire que les responsables du traitement fassent droit aux réquisitions judiciaires qu'ils reçoivent concernant les données qu'ils traitent pour leurs propres besoins, ils n'ont en revanche pas à organiser, à l'avance, la collecte de données à caractère personnel dans la perspective de répondre à une potentielle réquisition judiciaire.

37. Dès lors, la formation restreinte considère que l'enregistrement des appels téléphoniques passés, d'une part, entre les téléopérateurs et les prospects, et d'autre part, entre les voyants et les clients, afin de répondre à des réquisitions judiciaires, n'est pas justifié.

38. La formation restreinte considère donc, au vu de ces éléments, qu'un manquement à l'article 5, paragraphe 1, c) du RGPD est constitué. Elle relève que la société a cessé de proposer à ses clients des consultations par téléphone, ce qui implique l'arrêt des enregistrements téléphoniques à tout le moins entre les voyants et les clients, mais cela ne saurait exonérer la société de sa responsabilité pour le passé.

39. En second lieu, la rapporteure relève que lors des appels téléphoniques entre les téléopérateurs et les clients, ces derniers sont invités à communiquer leurs coordonnées bancaires. Elle considère que l'enregistrement sonore de la partie de la conversation relative à la collecte des données bancaires des clients ne saurait être justifié à des fins de suivi de la démarche qualité ou à des fins probatoires.

40. En défense, la société justifie, pour le passé, la collecte des données bancaires de ses clients par la réservation de rendez-vous avec un voyant, la simplification du règlement des consultations ultérieures, le paiement d'abonnements et la lutte contre la fraude.

41. Elle indique également que la mise en place d'une mesure permettant d'interrompre un enregistrement lors de la communication des données bancaires suppose le développement d'outils complexes faisant peser sur elle un coût financier et humain particulièrement lourd.

42. La formation restreinte relève qu'au jour des contrôles, la société enregistrait les appels passés entre les téléopérateurs et les prospects à des fins de suivi de la démarche qualité ou à des fins probatoires (souscription du contrat et réquisitions judiciaires). Lors de ces appels téléphoniques, les téléopérateurs collectaient les données bancaires des prospects (numéro de carte bancaire, date d'expiration et cryptogramme) et leur indiquaient que cette collecte leur permettait de " participer à la sécurisation de la ligne pour un euro symbolique seulement ".

43. La formation restreinte relève que la société n'a pas mis en place de mesure spécifique permettant d'interrompre l'enregistrement de la conversation téléphonique lors de la collecte des données bancaires des clients. Or, elle considère que l'enregistrement sonore des données bancaires des clients n'est pas utile pour la société dans le cadre du contrôle qualité, à des fins probatoires ou de sécurité.

44. À titre d'exemple, la formation restreinte rappelle qu'elle a déjà considéré, dans sa délibération n°SAN-2020-003 du 28 juillet 2020, à l'égard d'une société qui, lors de l'enregistrement de conversations téléphoniques à des fins de formation,

enregistrait les coordonnées bancaires des clients qui passaient des commandes par téléphone que " les coordonnées bancaires sont des données qui compte tenu de leur nature et des risques de fraude associés doivent faire l'objet d'une protection renforcée de la part des responsables de traitement. (…) leur utilisation par des tiers non autorisés, dans le cadre de paiement frauduleux, est susceptible d'entraîner un préjudice pour les personnes concernées. La formation restreinte constate que la société enregistrait et conservait des données dont elle n'avait aucun usage au regard de la finalité poursuivie par le traitement en cause, à savoir la formation des salariés. Elle considère donc, au vu de ces éléments qu'un manquement à l'article 5-1-c) du RGPD est constitué ".

45. Par ailleurs, la formation restreinte considère que l'enregistrement sonore des données bancaires n'est pas non plus pertinent au regard des finalités invoquées par la société lors de la procédure : la réservation de rendez-vous avec un voyant, la simplification du règlement des consultations ultérieures, le paiement d'abonnements et la lutte contre la fraude.

46. Par conséquence, elle considère, au vu de ces éléments, qu'un manquement à l'article 5, paragraphe 1, c) du RGPD est constitué, dès lors que la société collecte des données excessives au regard des finalités poursuivies.

B. Sur le manquement relatif à l'obligation de définir et de respecter une durée de conservation proportionnée à la finalité du traitement en application de l'article 5-1-e du RGPD

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

48. La rapporteure relève, par une lecture combinée de la politique de durées de conservation et de la politique de confidentialité de la société, que la durée de conservation des données des clients, à des fins de gestion de la relation commerciale et de suivi de la clientèle, est fixée à trois ans à compter de la fin de la relation commerciale.

49. Elle observe que, lors de la procédure de contrôle, la société a pourtant indiqué que figurent dans sa base de données, en base active, des données à caractère personnel de […] clients n'ayant pas eu de consultation avec un voyant depuis plus de trois ans, dont au moins […] clients n'ont pas eu de consultation avec un voyant depuis plus de cinq ans.

50. Elle fait grief à la société de conserver les données de ses clients pour une durée excessive.

51. En défense, la société conteste la volumétrie visée par la rapporteure. Elle considère qu'elle comporte des doublons. Elle indique, à titre d'exemple, qu'une personne qui recourt à une consultation par chat pour dix minutes gratuites, puis une consultation par chat payante, et enfin une consultation par téléphone, est comptabilisée trois fois dans la base de données.

52. Par ailleurs, la société reproche à la rapporteure de se référer à la dernière consultation d'un client avec un voyant pour apprécier la durée de conservation des données, sans prendre en compte le fait qu'un client peut consommer son crédit sans limite de temps.

53. En outre, elle justifie la durée de conservation des données de ses clients pendant trois ans à compter de la fin de la relation commerciale par le fait qu'un client peut recontacter un voyant plusieurs années après la dernière consultation et qu'il est nécessaire pour le voyant de pouvoir reconnaître un client qui n'aurait pas recouru à ses services depuis longtemps.

54. Elle indique qu'après la notification du rapport, elle a mis en place un mécanisme de purge afin de ne conserver les données de ses clients qu'un an à compter de la fin de la relation contractuelle.

55. La formation restreinte relève que, lors du contrôle sur pièces, la société conservait en base active les données personnelles de […] clients n'ayant pas eu de consultation depuis plus de trois ans, dont […] clients n'ayant pas eu de consultation depuis plus de cinq ans.

56. La formation restreinte note que, si cette volumétrie comporte des doublons, selon la société, cette dernière n'a pour autant pas communiqué à la CNIL le nombre de clients uniques dont les données étaient conservées depuis plus de trois et cinq ans, depuis leur dernier rendez-vous.

57. Elle note, par ailleurs, que la société justifie cette conservation des données, notamment par le fait que les clients ont la possibilité de consommer leur crédit sans limite de temps. Pour autant, la société n'a pas indiqué à la CNIL, lors de la procédure, que les […] clients n'ayant pas eu de consultation depuis plus de trois ans, dont […] clients depuis plus de cinq ans, correspondent bien à des clients qui bénéficient encore d'un crédit.

58. Enfin, la formation restreinte relève que la société conservait, au jour des contrôles, les données de ses clients pendant trois ans à compter de la fin de la relation commerciale et, au jour de la séance de la formation restreinte, pendant un an à compter de la fin de la relation commerciale. La formation restreinte note que la société justifie cette durée de conservation par le besoin de réidentifier un client qui n'a pas recouru à ses services depuis longtemps afin de lui assurer un suivi personnalisé le jour où il souhaite bénéficier d'une nouvelle consultation.

59. La formation restreinte relève que la société n'a pas indiqué à la CNIL, lors de la procédure, que ces données sont conservées en archivage intermédiaire.

60. La formation restreinte considère qu'à l'issue de la relation commerciale, la conservation des données à caractère personnel des clients en base active, pour la finalité susvisée, n'est pas justifiée. En revanche, elle considère qu'à l'issue de cette durée, certaines données des clients peuvent être conservées pour cette finalité en archivage intermédiaire.

61. À titre illustratif, dans son référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales du 23 septembre 2021, la CNIL indique que " les données nécessaires à l'exécution des contrats sont conservées pendant la durée de la relation contractuelle. Au terme du contrat, elles doivent être conservées en archivage intermédiaire et pour un délai raisonnable, si le responsable du traitement en a l'obligation légale (par exemple, pour répondre à des obligations comptables ou fiscales) ou s'il souhaite se constituer une preuve en cas de contentieux, et dans la limite du délai de prescription applicable. Il conviendra de prévoir à cet effet une base de données d'archives dédiée ou une séparation logique dans la base de données active, après avoir opéré un tri des données pertinentes à archiver. (…) "

62. Par conséquent, la formation restreinte considère que ces faits constituent un manquement aux dispositions de l'article 5, paragraphe 1, e) du RGPD.

C. Sur le manquement relatif à l'obligation de traiter les données de façon licite en application de l'article 6 du RGPD

63. Selon l'article 6 du RGPD, " le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;

b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. "

64. La rapporteure note que dans le cadre des consultations par chat, la société conserve les données bancaires de ses clients, au-delà du temps strictement nécessaire à la réalisation de la transaction, pour faciliter les paiements ultérieurs, et ce, sans recueillir leur consentement préalable, par exemple sur le formulaire de collecte de données.

65. En défense, la société considère que la conservation des données bancaires de ses clients a pour finalité l'achat de crédits et repose sur le contrat qui la lie à ses clients. Elle considère également que la conservation de ces données à des fins de lutte contre la fraude repose sur son intérêt légitime.

66. La formation restreinte rappelle que la base légale du traitement des données bancaires peut varier notamment en fonction de la finalité poursuivie.

67. En l'espèce, en premier lieu, s'agissant de la finalité relative à la lutte contre la fraude, la formation restreinte considère que la base légale de la conservation des données bancaires est, conformément à ce que soutient la société, l'intérêt légitime de celle-ci, ce qui n'est pas contesté par la rapporteure.

68. À cet égard, la Commission indique, dans sa délibération n° 2018-303 du 6 septembre 2018 portant adoption d'une recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou

de fourniture de services à distance, que " la conservation des données relatives à la carte de paiement au-delà de la réalisation d'une transaction à des fins de lutte contre la fraude à la carte de paiement ne rentre pas dans le cadre du contrat. Elle considère en effet que ce traitement relève de l'intérêt légitime du responsable de traitement, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés des personnes en application de l'article 6-1-f du RGPD, en garantissant notamment le respect des principes de transparence et l'effectivité de l'exercice de leurs droits par les personnes concernées ".

69. S'agissant en second lieu de la finalité relative au re-créditage, la formation restreinte considère que les données bancaires des clients sont conservées pour offrir un service supplémentaire aux clients, en l'occurrence ne pas avoir à ressaisir leur numéro de carte lors de l'achat de crédit supplémentaire, ce qui va au-delà de l'exécution du contrat conclu.

70. Dès lors, elle considère que le traitement des données bancaires des clients à cette fin ne peut pas reposer sur le contrat conclu entre le client et la société et nécessite que soit recueilli le consentement préalable des clients.

71. La formation restreinte rappelle, à titre illustratif, que la Commission estime, dans sa délibération susvisée, qu'à des fins de paiement unique, " le numéro de carte bancaire ne peut être collecté et traité que pour permettre la réalisation d'une transaction dans le cadre de l'exécution du contrat conclu par la personne concernée conformément à l'article 6-1-b du RGPD (exécution contractuelle). Ainsi, en cas de contrat impliquant un paiement unique, la Commission estime que les données n'ont donc pas vocation à être conservées au-delà du temps de transaction commerciale ".

72. Toujours à titre illustratif, dans la délibération susvisée, la Commission indique que " la conservation du numéro de la carte du client afin de faciliter ses éventuels paiements ultérieurs, et éventuellement pouvoir procéder à un achat en " un clic " sur le site du commerçant, va au-delà de l'exécution du contrat conclu. Elle retient que cette faculté constitue une option indépendante de l'acte initial ayant conduit à la collecte des coordonnées bancaires et rappelle qu'un tel traitement nécessite que soit recueilli au préalable le consentement libre, spécifique, éclairé et univoque des personnes, en application de l'article 6-1-a du RGPD ".

73. La formation restreinte rappelle également que dans sa décision du 10 décembre 2020, n° 429571, le Conseil d'état a retenu que " la CNIL a pu à bon droit estimer que, de façon générale, devait être soumise au consentement explicite de la personne concernée la conservation des numéros de cartes bancaires des clients des sites de commerce en ligne pour faciliter des achats ultérieurs. Il suit de là que le moyen tiré de la méconnaissance par la délibération litigieuse du règlement du 27 avril 2016 doit être écarté ".

74. En conséquence, la formation restreinte considère qu'un manquement à l'article 6, paragraphe 1, du RGPD est constitué, dès lors que la société conserve les données bancaires de ses clients, au-delà de la réalisation de la transaction, afin de faciliter l'achat de crédit supplémentaire, sans recueillir au préalable leur consentement.

D. Sur le manquement relatif à l'obligation de recueillir le consentement préalable à la collecte de catégories particulières de données en application de l'article 9 du RGPD

75. En vertu de l'article 9 du RGPD, le traitement des données à caractère personnel qui révèle des données concernant la santé ou l'orientation sexuelle d'une personne physique est interdit sauf s'il relève d'une des conditions prévues à l'article 9-2-a) à j) du RGPD.

76. La rapporteure constate que les voyants ont la possibilité de rédiger des commentaires sur les fiches clients de la société après une consultation. Elle note que, parmi ces commentaires, figurent des informations révélées par les clients concernant leur santé et leur orientation sexuelle. Elle relève que, lors de la création du compte utilisateur, la société ne recueille pas l'accord de la personne concernée sur l'utilisation de ces données.

77. En défense, la société fait valoir que le simple fait pour une personne de s'adresser à un voyant et de communiquer spontanément des données sensibles lors de l'échange constitue un acte positif clair de transmettre certaines données et donc un consentement.

78. En outre, la société soutient que les commentaires des voyants ne permettent pas, pour la plupart, d'identifier la personne concernée, les données étant pseudonymisées.

79. La formation restreinte note, tout d'abord, que, lors des consultations, les clients peuvent communiquer aux voyants des données relatives à leur état de santé et à leur orientation sexuelle. À l'issue des consultations, les voyants formulent des commentaires sur les fiches de leurs clients. Ces fiches sont conservées dans leur outil métier. La formation restreinte observe que, dans le cadre de leurs commentaires, les voyants mentionnent les informations relatives à l'état de santé et à l'orientation sexuelle des clients qu'ils ont collectées lors de la consultation.

80. La formation restreinte considère que les mesures prises par la société ne correspondent pas à une anonymisation des données des clients mais à une simple pseudonymisation, dans la mesure où l'identifiant, associé au commentaire, et les

informations qu'il comporte, permettent de réidentifier le client concerné.

81. La formation restreinte relève, ensuite, qu'en l'absence d'autres conditions mobilisables au cas d'espèce au titre de l'article 9-2-b) à j) du RGPD, un tel traitement ne peut être mis en œuvre que sur la base du consentement explicite de la personne concernée au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques, en application de l'article 9-2-a) du RGPD. La formation restreinte rappelle que le caractère explicite du consentement s'analyse au cas par cas et dépend du contexte du traitement des données sensibles. Lorsque le service demandé par l'utilisateur implique nécessairement le traitement de données sensibles, il est cependant nécessaire que l'utilisateur ait pleinement conscience de ce que ses données sensibles seront traitées et parfois conservées par le responsable de traitement, ce qui implique en principe une information explicite sur ce point lors du recueil du consentement.

82. La formation restreinte rappelle que selon l'article 4, alinéa 11, du RGPD, la notion de consentement s'entend comme toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

83. D'une part, la formation restreinte considère que le caractère explicite du consentement prévu à l'article 9, paragraphe 2, a), du RGPD suppose de permettre à la personne concernée de manifester, par une action positive, son assentiment au traitement de données sensibles, attestant de la matérialité de son consentement.

84. À titre d'éclairage, la formation restreinte rappelle que dans ses lignes directrices sur le consentement au sens du règlement 2016/679 du 10 avril 2018, le Comité européen de la protection des données (ci-après " CEPD ") indique que " le RGPD stipule qu'une " déclaration ou un acte positif clair " est une condition sine qua non d'un consentement " standard ". Dès lors que les exigences pour un consentement " standard " dans le RGPD sont déjà portées à un niveau supérieur à celles de la directive 95/46/CE, il convient de préciser quels efforts complémentaires un responsable du traitement devrait entreprendre afin d'obtenir le consentement explicite d'une personne concernée conformément au RGPD. Le terme explicite se rapporte à la façon dont le consentement est exprimé par la personne concernée. Il implique que la personne concernée doit formuler une déclaration de consentement exprès. Une manière évidente de s'assurer que le consentement est explicite serait de confirmer expressément le consentement dans une déclaration écrite. Le cas échéant, le responsable du traitement pourrait s'assurer que la déclaration écrite est signée par la personne concernée afin de prévenir tout doute potentiel et toute absence potentielle de preuve à l'avenir. Une telle déclaration signée n'est toutefois pas la seule façon d'obtenir le consentement explicite […] " (lignes directrices 2016/679 WP259 rev.01 du 10 avril 2018, page 21).

85. La formation restreinte souligne qu'elle a, à plusieurs reprises, adopté des mesures correctrices à l'encontre de responsables de traitement ne recueillant pas le consentement explicite des personnes pour collecter et traiter leurs données " sensibles ", notamment dans ses délibérations n° 2016-405 du 15 décembre 2016 et n° 2016-406 du 15 décembre 2016 ainsi que dans sa délibération n° SAN-2017-006 du 27 avril 2017 dans laquelle elle a considéré que " le renseignement spontané de telles données n'exonère pas la société de l'obligation de recueillir le consentement exprès des personnes qui doivent être en mesure de manifester par une action positive leur assentiment au traitement de données sensibles, attestant ainsi que le consentement est donné en toute connaissance de cause ".

86. La formation restreinte relève donc que la simple volonté de recevoir une prestation de voyance et le fait de livrer spontanément des informations sensibles ne constituent pas un consentement explicite des personnes concernées.

87. Elle considère que la société aurait dû mettre à la disposition des personnes auprès desquelles elle collecte des catégories particulières de données un moyen afin de s'assurer qu'elles y consentent de manière explicite par un acte positif clair.

88. D'autre part, le consentement recueilli au titre de l'article 9, paragraphe 2, a) précité, du RGPD doit se lire à la lumière de la définition posée à l'article 4, paragraphe 11, précité, du RGPD, ce qui implique qu'en l'espèce, pour consentir valablement, la personne concernée soit, au préalable, pleinement éclairée sur le caractère particulier des données qu'elle communique, notamment en ce que celles-ci peuvent révéler son état de santé et son orientation sexuelle, ainsi que sur l'usage qui sera fait de ces données.

89. La formation restreinte note que la société ne délivre pas d'information spécifique aux personnes concernées concernant la collecte et le traitement de leurs données de santé et informations relatives à leur orientation sexuelle.

90. Elle considère que la société aurait dû fournir aux personnes concernées une information spécifique, par exemple, lors de la création de leur compte utilisateur.

91. Par conséquent, la formation restreinte considère que la société ne recueille pas le consentement explicite des personnes concernées, de sorte qu'elle ne peut pas se prévaloir de l'exception à l'interdiction de collecter et traiter des catégories particulières de données, prévue à l'article 9, paragraphe 2, a), du RGPD.

92. En conséquence, la formation restreinte considère qu'en l'absence de recueil du consentement préalable et explicite des clients à la collecte de leurs données de santé et d'informations relatives à leur orientation sexuelle, un manquement à l'article 9 du RGPD est constitué.

E. Sur le manquement relatif à l'obligation de transparence en application de l'article 12 du RGPD

93. L'article 12, paragraphe 1, du RGPD dispose que " le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique ".

94. La rapporteure fait grief à la société de ne pas fournir aux personnes concernées les informations visées à l'article 13 du RGPD de manière suffisamment accessible lors de la collecte de données à caractère personnel en vue de la création d'un compte utilisateur.

95. En défense, la société soutient qu'aucune disposition légale ne prescrit les modalités pratiques que le responsable du traitement se doit de respecter pour informer ses utilisateurs du traitement de données à caractère personnel. Elle indique, par ailleurs, que la séparation de sa politique de confidentialité et des " conditions générales de vente " est en cours.

96. La formation restreinte rappelle que l'information est aisément accessible, au sens de l'article 12 du RGPD, si elle est fournie à l'utilisateur, sans que celui-ci ait besoin de la rechercher activement.

97. D'une part, la formation restreinte note que le formulaire de création d'un compte utilisateur ne comporte pas les informations relatives aux traitements de données à caractère personnel mis en œuvre par la société, ni de lien renvoyant vers de telles informations.

98. Elle relève que, pour accéder à ces informations, l'utilisateur doit quitter le processus d'inscription afin de retourner sur la page d'accueil, la faire défiler jusqu'en bas, cliquer sur les conditions générales de vente de la société et rechercher activement dans ce document les informations relatives à la protection des données à caractère personnel.

99. Dès lors qu'un parcours de plusieurs actions est nécessaire à l'utilisateur pour obtenir une information exhaustive relative à la protection des données, la formation restreinte considère que l'information n'est pas aisément accessible.

100. D'autre part, la formation restreinte constate que les informations se situent dans un document qui s'intitule " CGV ", qui comporte à la fois des informations générales sur les " conditions de vente ", les conditions d'utilisation du site web et des informations concernant les traitements de données à caractère personnel que la société met en œuvre.

101. Dès lors que l'information se situe dans un document qui n'est pas facilement identifiable comme relatif à la protection des données à caractère personnel, la formation restreinte considère que l'information n'est pas aisément accessible.

102. La formation restreinte rappelle également, à titre illustratif, que dans ses lignes directrices sur la transparence du 11 avril 2018, le CEPD estime que " le critère " aisément accessible " signifie que la personne concernée ne devrait pas avoir à rechercher les informations mais devrait pouvoir tout de suite y accéder : par exemple, ces informations pourraient être communiquées aux personnes concernées directement ou au moyen d'un lien qui leur serait adressé […] ". Il recommande à titre de bonne pratique que " dans un contexte en ligne, 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 ". Ces lignes directrices précisent également que les informations " devraient être clairement différenciées des autres informations non liées à la vie privée telles que des clauses contractuelles ou des modalités d'utilisation générale ". Les lignes directrices indiquent également que "la personne concernée ne doit pas avoir à chercher activement les informations couvertes par [les articles 13 et 14] parmi d'autres informations telles que les conditions d'utilisation d'un site […] ".

103. Par conséquent, la formation restreinte considère que, sur le site web www.voyance-en-direct.tv, les modalités de délivrance de l'information relative à la protection des données à caractère personnel ne répondent pas aux exigences de transparence prévues à l'article 12 du RGPD.

F. Sur le manquement relatif à l'obligation d'information en application de l'article 13 du RGPD

104. L'article 13 du RGPD impose au responsable de traitement de fournir à la personne concernée différentes informations relatives notamment à son identité et ses coordonnées, aux finalités du traitement mis en œuvre, sa base juridique, les

destinataires ou les catégories de destinataires des données, au fait que le responsable du traitement a l'intention d'effectuer un transfert de données vers un pays tiers. En outre, la réglementation impose, lorsque cela apparaît nécessaire pour garantir " un traitement équitable et transparent " des données personnelles en l'espèce, d'informer les personnes sur la durée de conservation des données, l'existence des différents droits dont bénéficient les personnes, l'existence du droit de retirer son consentement à tout moment et le droit d'introduire une réclamation auprès d'une autorité de contrôle.

105. La rapporteure observe que certaines informations mentionnées à l'article 13 ne sont pas communiquées aux utilisateurs sur le site web www.voyance-en-direct.tv, notamment la durée de conservation des données, leur droit à la portabilité et leur droit d'introduire une réclamation auprès d'une autorité de contrôle.

106. Par ailleurs, elle relève que l'échantillon des enregistrements communiqués à la délégation montre que, lors des appels téléphoniques, les personnes ne sont pas informées du fait que la conversation est enregistrée, de leur droit de s'y opposer, ni du fait que les données collectées lors de l'appel seront traitées par la société.

107. En défense, la société indique être en cours de mise en conformité concernant l'insertion des mentions obligatoires manquantes dans sa politique de confidentialité. S'agissant de l'absence d'information lors des appels téléphoniques, la société indique avoir cessé de proposer des prestations de voyance par téléphone.

108. La formation restreinte prend acte de la mise en conformité en cours de la société concernant l'information des personnes et de l'arrêt des consultations par téléphone.

109. Toutefois, elle relève qu'il n'est pas contesté, qu'au jour des contrôles, certaines informations obligatoires au titre de l'article 13 du RGPD n'étaient pas communiquées aux utilisateurs du site web www.voyance-en-direct.tv et que les prospects n'étaient pas informés, lors des appels, de l'enregistrement des conversations téléphoniques, de la possibilité de s'y opposer et des traitements qui étaient mis en œuvre à partir des données collectées à cette occasion.

110. Par conséquent, la formation restreinte considère qu'un manquement à l'article 13 du RGPD est constitué, compte tenu, d'une part, de l'absence de complétude de l'information fournie aux utilisateurs, tant que la société n'a pas modifié la mention d'information sur son site web, et d'autre part, du défaut d'information des prospects au jour des contrôles.

G. Sur le manquement relatif à l'obligation d'encadrer la relation entre le responsable du traitement et le sous-traitant en application de l'article 28 du RGPD

111. L'article 28, paragraphe 3, du RGPD prévoit que le traitement effectué par un sous-traitant pour un responsable de traitement est régi par un contrat qui définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel, les catégories de personnes concernées, ainsi que les obligations et les droits du responsable de traitement. Ce contrat prévoit en outre les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement.

112. La rapporteure relève que parmi les contrats et annexes de sous-traitance communiqués par la société, deux ne sont pas signés par les prestataires et d'autres ne comportent pas l'ensemble des mentions obligatoires.

113. En défense, la société ne conteste pas l'absence de signature par ses prestataires de deux des contrats de sous-traitance, ni l'absence de certaines mentions obligatoires devant figurer dans les contrats de sous-traitance communiqués. Elle demande toutefois à la formation restreinte de noter l'existence de ces accords, impliquant sa volonté d'être conforme à l'article 28 du RGPD.

114. La formation restreinte note, tout d'abord, que l'annexe du contrat d'infogérance, qui lie la société avec le sous-traitant à l'égard duquel elle impute la responsabilité de l'incident de sécurité, ne comporte pas l'ensemble des informations prévues à l'article 28, paragraphe 3, du RGPD et n'est pas signé par le prestataire.

115. Ensuite, elle relève que le contrat conclu entre la société KG COM et le prestataire en charge de la téléphonie ne comporte pas de clause de sous-traitance, au sens de l'article 28, paragraphe 3, du RGPD.

116. Elle relève, enfin, que les annexes aux contrats conclus entre la société KG COM et les partenaires d'affiliation comportent une clause de sous-traitance qui n'est pas conforme à l'article 28, paragraphe 3, du RGPD, puisqu'elle ne vise pas l'ensemble des mentions obligatoires, notamment l'obligation pour le sous-traitant de traiter les données à caractère personnel uniquement sur instruction documentée du responsable du traitement. Elle note, par ailleurs, que l'une de ces annexes n'est pas signée par le partenaire d'affiliation.

117. La formation restreinte considère que ces faits ne permettent pas d'assurer une protection efficace des données à caractère personnel traités par le biais de garanties contractuelles.

118. En conséquence, la formation restreinte considère que ces faits constituent un manquement à l'article 28, paragraphe 3, du RGPD, ce que la société ne conteste pas au demeurant.

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

119. Aux termes de l'article 32 du RGPD, " 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

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

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

[…] ".

120. En premier lieu, la rapporteure relève que, lors de la création d'un compte utilisateur sur le site web www.voyance-en-direct.tv, les personnes peuvent choisir un mot de passe comportant un seul caractère. Par ailleurs, l'accès à l'outil CRM de la société s'effectue à partir d'un identifiant et d'un mot de passe créé soit par le président de la société et le salarié concerné, sans règles particulières concernant la complexité des mots de passe, ni modification automatique du mot de passe lors de la première connexion, soit par l'administrateur au moyen d'un générateur qui prévoit un mot de passe composé de neuf et douze caractères, dont des caractères alphanumériques et des caractères spéciaux.

121. En défense, la société n'apporte pas d'éléments de réponse sur le manque de robustesse des mots de passe.

122. La formation restreinte rappelle qu'en application de l'article 32 du RGPD, pour assurer la protection des données à caractère personnel, il incombe au responsable de traitement de prendre des " mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ".

123. La formation restreinte considère que des règles de complexité des mots de passe trop permissives, qui autorisent l'utilisation de mots de passe insuffisamment robustes, peuvent conduire à des attaques par des tiers non autorisés, telles que des attaques par " force brute " ou " par dictionnaire ", qui consistent à tester successivement et de façon systématique de nombreux mots de passe et conduisent, ainsi, à une compromission des comptes associés et des données à caractère personnel qu'ils contiennent.

124. Elle relève, à cet égard, que la nécessité d'un mot de passe fort est recommandée tant par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) que par la Commission dans sa délibération n° 2017-012 du 19 janvier 2017, exigence confirmée dans sa délibération n° 2022-100 du 21 juillet 2022.

125. La formation restreinte souligne qu'elle a, à plusieurs reprises, adopté des sanctions pécuniaires où la caractérisation d'un manquement à l'article 32 du RGPD est le résultat de mesures insuffisantes pour garantir la sécurité des données traitées. Les délibérations n° SAN-2019-006 du 13 juin 2019, n° SAN-2019-007 du 18 juillet 2019 et n° SAN-2022-018 du 8 septembre 2022 visent notamment l'insuffisante robustesse des mots de passe.

126. En l'espèce, la formation restreinte relève que les mots de passe des utilisateurs du site web www.voyance-en-direct.tv peuvent être composés d'un seul caractère.

127. Elle considère que le risque encouru par les personnes concernées est réel : un tiers ayant eu accès au mot de passe pourrait accéder aux données à caractère personnel présentes dans le compte de la personne concernée, consulter l'historique de sa consommation de crédit, et/ou changer le mot de passe de son compte, à l'insu de l'utilisateur.

128. Par ailleurs, la formation restreinte relève l'absence de robustesse des mots de passe permettant aux salariés de la société d'accéder à son outil CRM, compte tenu de l'absence de règle de complexité lorsqu'ils sont créés par le président de la société et le salarié concerné, et de l'absence de mesures de sécurité complémentaire, lorsqu'ils sont créés par l'administrateur (mots de passe composés de neuf à douze caractères alphanumériques et spéciaux).

129. La formation restreinte considère également que la procédure de création des mots de passe ne permet pas d'assurer la confidentialité des données puisque lorsque le mot de passe est créé par l'administrateur, celui-ci le transmet au président de la société afin qu'il le communique au salarié concerné et lorsqu'il n'est pas créé par l'administrateur, le président de la société le créé en lien avec le salarié concerné.

130. Ces faits constituent un réel risque pour les personnes concernées : un tiers non habilité ayant eu accès au mot de passe pourrait accéder à un grand nombre de données à caractère personnel, dont des données sensibles.

131. Dès lors, la prise en compte de ces risques pour la protection des données à caractère personnel et de la vie privée des personnes conduit la formation restreinte à considérer que les mesures déployées pour garantir la sécurité des données en l'espèce sont insuffisantes.

132. Dans ces conditions, eu égard aux risques encourus par les personnes, rappelés ci-dessus, ainsi que de la sensibilité de certaines données (données de santé, données relatives à l'orientation sexuelle, données bancaires), la formation restreinte considère que l'organisme a manqué aux obligations qui lui incombent en vertu de l'article 32 du RGPD.

133. En deuxième lieu, la rapporteure relève que le mécanisme utilisé par la société pour chiffrer les données bancaires présente des vulnérabilités (détermination à l'avance du vecteur d'initialisation, réutilisation de celui-ci et obsolescence de la bibliothèque utilisée), ce qui ne permet pas, eu égard à la sensibilité de ces données, de garantir un niveau de sécurité adapté au risque.

134. En défense, la société soutient que son sous-traitant, la société […], aurait dû la conseiller sur le chiffrement des données.

135. La formation restreinte rappelle que la protection des données bancaires nécessite la mise en place de mesures de sécurité accrues eu égard à leur caractère hautement personnel, telles que le chiffrement.

136. En l'espèce, la formation restreinte relève qu'il ressort des pièces du dossier que la société […] n'était pas en charge du chiffrement des données bancaires des clients de la société KG COM mais de l'infogérance et de l'hébergement des données.

137. La formation restreinte note également qu'il ressort des pièces du dossier que la société KG COM a elle-même procédé au chiffrement des données bancaires de ses clients, et ce de manière non sécurisée.

138. En effet, la formation restreinte observe que la liste CWE (Common Weakness Enumeration) du MITRE (organisation à but non lucratif américaine intervenant notamment dans l'ingénierie des systèmes et la technologie de l'information), qui énumère les faiblesses de logiciels, identifie notamment comme des vulnérabilités le fait de générer un vecteur d'initialisation prédictible avec le mode CBC, comme en l'espèce, et le fait de réutiliser un vecteur d'initialisation. La formation restreinte note que lorsque le vecteur d'initialisation n'est pas aléatoire mais déterminé, le message clair est toujours chiffré de la même manière. Il est donc possible de comparer plusieurs messages chiffrés et d'identifier les messages clairs auxquels ils correspondent. Par ailleurs, en réutilisant le vecteur d'initialisation, celui-ci est commun à toutes les données chiffrées avec la clé unique.

139. La formation restreinte relève également que Mcrypt, bibliothèque cryptographique utilisée par la société, a été considérée comme obsolète, puis supprimée en 2017, de sorte que le recours à cette fonctionnalité est déconseillé dans la documentation PHP.

140. En conséquence, la formation restreinte considère que les faits précités constituent un manquement à l'article 32 du RGPD dès lors que le mécanisme mis en œuvre par la société KG COM pour chiffrer les données bancaires de ses clients ne permet pas d'assurer un niveau de sécurité adapté au risque.

141. En troisième lieu, la rapporteure relève que, lors des contrôles, l'accès au site web www.voyance-en-direct.tv s'effectuait à l'aide du protocole " HTTP ", y compris la page relative à la collecte des données bancaires. Or, ce protocole n'est pas un protocole sécurisé, ce qui signifie que le site est vulnérable aux attaques et permet la lecture en clair des flux contenant des données à caractère personnel, dont des données bancaires, entre le navigateur de l'utilisateur et le serveur hébergeant le site.

142. En défense, la société indique avoir modifié son protocole " HTTP " en protocole TLS sur le site web www.voyance-en-direct.tv, après la notification du rapport.

143. La formation restreinte rappelle que, en application de l'article 32 du RGPD, il incombe au responsable de traitement de prendre des " mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ".

144. La formation restreinte relève que le protocole " HTTP " est un protocole de communication qui ne permet ni l'authentification du site web, ni le chiffrement des données lors de leur transmission vers les serveurs hébergeant le site web de la société, ce qui ne permet pas de garantir l'authenticité du site consulté, ni l'intégrité et la confidentialité des données échangées, exposant les données à caractère personnel traitées par le biais de ces pages à des risques d'écoute, d'interception ou de modification à l'insu de l'utilisateur, ce qui peut conduire à porter atteinte à la vie privée des personnes concernées.

145. La formation restreinte relève à titre d'éclairage que la nécessité d'assurer la confidentialité des canaux de transmission de données à caractère personnel est soulignée par l' ANSSI depuis 2013 notamment dans ses " Recommandations pour la mise en œuvre d'un site web : maîtriser les standards de sécurité côté navigateur " qui précisent que " la mise en place de HTTPS sur un site ou une application web est une garantie de sécurité qui repose sur TLS pour assurer la confidentialité et l'intégrité des informations échangées, ainsi que l'authenticité du serveur contacté. L'absence de cette garantie peut entraîner de nombreux abus sans pour autant que l'intention soit malveillante ".

146. La formation restreinte relève également que la Commission recommande de façon constante depuis la publication de son guide " La sécurité des données personnelles " en 2018, de mettre en œuvre, à titre de précautions élémentaires, le protocole " TLS " en utilisant uniquement les versions les plus récentes et en vérifiant sa bonne mise en œuvre.

147. La formation restreinte relève en outre que les données à caractère personnel en question sont des données hautement personnelles puisqu'il s'agit de données bancaires. Dès lors, la prise en compte de ces risques pour la protection des données à caractère personnel et de la vie privée des personnes conduit la formation restreinte à considérer que les mesures déployées pour garantir la sécurité des données, en l'espèce, sont insuffisantes dès lors que ces données transitent lors de leur transmission entre le navigateur de l'utilisateur et le serveur hébergeant le site.

148. En conséquence, la formation restreinte considère, au regard des données personnelles objet du traitement (notamment, des données bancaires), que l'absence de mise en place de la mesure de sécurité de base que constitue l'utilisation du protocole " HTTPS " ou d'une autre mesure de sécurité équivalente caractérise un manquement à l'article 32 du RGPD. La formation restreinte prend note néanmoins de la modification du protocole par la société en cours de procédure. Elle rappelle toutefois que les mesures de mises en conformité effectuées ne sauraient exonérer la société de sa responsabilité pour le manquement constaté.

I. Sur le manquement relatif à l'obligation de notifier les violations de données à caractère personnel à la CNIL en application de l'article 33 du RGPD

149. L'article 4, 12) du RGPD définit la violation de données à caractère personnel comme " une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ".

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

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

152. La rapporteure relève que la société a pris connaissance de la violation de données à caractère personnel le 29 septembre 2020, lorsqu'un journaliste lui a communiqué un échantillon des données impactées, ou au plus tard le 30 septembre 2020, à l'issue de son enquête interne.

153. Selon elle, la violation de données était susceptible de présenter un risque pour les droits et libertés des personnes concernées, notamment compte tenu de la durée de la violation (deux mois et quatre jours) et du nombre potentiel de personnes concernées ([…] clients et prospects dans la base de données).

154. Par conséquent, elle considère que l'existence de la violation de données à caractère personnel aurait dû être notifiée à la CNIL par la société, le cas échéant de manière échelonnée.

155. En défense, la société reconnaît avoir appris l'existence de l'incident de sécurité le 29 septembre 2020. Elle indique toutefois que l'accès au serveur en cause était fermé depuis le 10 juillet 2020, ce qui a mis fin à l'incident de sécurité.

156. Elle impute la responsabilité de cet incident de sécurité à son sous-traitant, en charge de l'infogérance. En effet, elle indique qu'après avoir demandé à son sous-traitant de donner l'accès à son serveur à son développeur, son sous-traitant a agi en dehors de ses instructions en rendant le serveur accessible à des tiers non autorisés.

157. Enfin, la société conteste la volumétrie avancée par la rapporteure concernant les clients et prospects inscrits dans sa base de données. Elle considère que celle-ci comporte les adresses électroniques de […] clients et […] prospects.

158. La formation restreinte rappelle que, conformément à l'article 33 du RGPD, 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.

159. La formation restreinte rappelle également qu'en cas de violation de données à caractère personnel susceptible d'engendrer un risque pour les droits et libertés des personnes, le responsable du traitement est tenu de notifier cette violation à l'autorité de contrôle dans les meilleurs délais, et, si possible, 72 heures au plus tard après en avoir pris connaissance.

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

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

162. Toujours à titre d'illustration, le CEPD précise qu'" après avoir été informé d'une possible violation par un individu, par une organisation médiatique (…), le responsable du traitement peut mener une brève enquête afin de déterminer si une violation s'est effectivement produite. Lors de cette période d'enquête, le responsable du traitement peut ne pas être considéré comme ayant pris " connaissance ". Cette période d'enquête initiale devrait cependant débuter aussi rapidement que possible et déterminer avec un degré de certitude raisonnable si une violation s'est produite. Une enquête plus détaillée pourra alors suivre. "

163. En l'espèce, la formation restreinte note que l'accès au serveur en cause a été fermé par le sous-traitant de la société, sur demande de celle-ci, le 10 juillet 2020, car il n'était pas adapté à ses besoins.

164. La formation restreinte relève que la société a été alertée par courriel, le 29 septembre 2020, par un journaliste, de l'existence d'un incident de sécurité dû à l'ouverture d'un port de ce serveur qui n'aurait pas dû l'être. Elle note également que le journaliste a communiqué à la société, dans le cadre de son courriel, un échantillon de la base de données qui aurait été divulguée, à savoir des données d'identification et de contact.

165. Elle relève que la société a mené une brève enquête interne, le 30 septembre 2020, à l'issue de laquelle la société a conclu que l'incident de sécurité était imputable à son sous-traitant, en charge de l'infogérance, qui a ouvert accidentellement un port du serveur.

166. Elle note que la société a répertorié l'incident de sécurité dans son registre des violations de données et identifié comme conséquences probables de la violation, " la revente des données entraînant la prospection sans consentement des personnes concernées par la violation ".

167. La formation restreinte relève que la société n'a pourtant pas procédé à une notification auprès de la CNIL. La société le justifie par le fait qu'elle n'aurait pas été en mesure de constater la violation de données puisque l'alerte du journaliste est intervenue après la fermeture du serveur et que son sous-traitant, en charge de l'infogérance, n'a pas conservé les logs de connexion au serveur concerné.

168. Selon la formation restreinte, la société n'a pas mis en œuvre toutes les mesures appropriées pour établir immédiatement l'existence de la violation de données à caractère personnel.

169. En effet, la formation restreinte estime que même si la société a été alertée de l'incident de sécurité après la fermeture du serveur, elle était en mesure d'identifier l'existence d'une violation de données, en confrontant l'échantillon des données communiqué par le journaliste à sa propre base de données.

170. Par ailleurs, la formation restreinte relève la tardiveté de la demande de communication des logs de connexion au sous-traitant puisque celle-ci n'est intervenue que le 25 novembre 2020, soit deux mois après l'alerte du journaliste.

171. Compte tenu des éléments évoqués ci-dessus, la formation restreinte considère que, au plus tard le 30 septembre 2020, date de l'enquête interne, la société avait un degré de certitude raisonnable de l'existence d'une violation de

données engendrant un risque pour les droits et libertés des personnes concernées, notamment compte tenu de la durée de la violation (deux mois et quatre jours) et du nombre potentiel de personnes concernées, à savoir […] clients et prospects.

172. La formation restreinte relève que la société, en qualité de responsable du traitement, avait l'obligation de notifier la survenance d'une violation de données même si la violation avait pour origine une erreur imputable au sous-traitant.

173. Par conséquent, la formation restreinte considère que la société a manqué à ses obligations en ne notifiant pas la violation de données à la CNIL.

174. Il résulte de ce qui précède que la formation restreinte considère qu'un manquement à l'article 33 du RGPD est caractérisé.

J. Sur le manquement relatif à l'article 82 de la loi Informatique et Libertés

175. L'article 82 de la loi Informatique et Libertés dispose que " tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :

1° De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;

2° Des moyens dont il dispose pour s'y opposer […] ".

Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son consentement qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle (…) Ces dispositions ne sont toutefois pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur : 1° Soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ; 2° Soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur ".

176. Ces dispositions transposent en droit français l'article 5, paragraphe 3, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (dite " directive e-Privacy ").

177. En premier lieu, la rapporteure note que la délégation a constaté, lors du contrôle en ligne du 15 avril 2021, l'absence de bandeau ou d'interface d'information et consentement aux cookies lors de l'accès au site web www.voyance-en-direct.tv alors que certains cookies étaient déposés sur les terminaux des utilisateurs.

178. Elle relève que, lors du contrôle sur place du 15 juillet 2021, la délégation a constaté la présence d'un bandeau cookies lors de l'accès à ce site web.

179. Elle considère toutefois que l'information délivrée n'est pas satisfaisante et ne permet pas d'éclairer le consentement de la personne concernée puisqu'aucune information n'est fournie concernant la manière de refuser les traceurs, les conséquences qui s'attachent à un refus et l'existence du droit de retirer son consentement.

180. En défense, la société fait valoir que, depuis la notification du rapport, elle a édité un bandeau cookies conforme sur son site web.

181. La formation restreinte rappelle qu'il résulte des dispositions combinées des articles 82 de la loi Informatique et Libertés et 4 du RGPD que les traceurs nécessitant un recueil du consentement ne peuvent, sous réserve des exceptions prévues par ces dispositions, être utilisés en écriture ou en lecture qu'à condition que l'utilisateur ait manifesté à cette fin son consentement, de manière libre, spécifique, univoque et éclairée, par une action positive.

182. La formation restreinte considère que la validité du consentement est donc notamment liée à la qualité de l'information reçue.

183. À titre d'éclairage, la formation restreinte indique que dans les lignes directrices relatives à l'application de l'article 82 de la loi Informatique et Libertés aux opérations de lecture et écriture dans le terminal d'un utilisateur, la Commission précise, s'agissant du caractère éclairé du consentement, qu' " a minima, la fourniture des informations suivantes aux utilisateurs, préalablement au recueil de leur consentement, est nécessaire pour assurer le caractère éclairé de ce dernier :

- l'identité du ou des responsables de traitement des opérations de lecture ou écriture ;

- la finalité des opérations de lecture ou écriture des données ;

- la manière d'accepter ou de refuser les traceurs ;

- les conséquences qui s'attachent à un refus ou une acceptation des traceurs ;

- l'existence du droit de retirer son consentement ".

184. La Commission précise, dans sa recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux cookies et autres traceurs du 17 septembre 2020, qu' " en pratique, afin de concilier les exigences de clarté et de concision des informations avec la nécessité d'identifier l'ensemble des responsables du ou des traitements, les informations spécifiques sur ces entités (identité, lien vers leur politique de traitement des données à caractère personnel), régulièrement mises à jour, peuvent par exemple être fournies à un second niveau d'information. Elles peuvent ainsi être mises à disposition depuis le premier niveau via, par exemple, un lien hypertexte ou un bouton accessible depuis ce niveau ". L'information relative à l'identité du ou des responsables de traitement des opérations de lecture ou d'écriture peut donc être fournie à un second niveau d'information.

185. La formation restreinte relève également que la Commission indique, à titre d'illustration, dans les questions-réponses sur les lignes directrices modificatives et la recommandation " cookies et autre traceurs " de la CNIL du 4 novembre 2022 qu' " afin que le consentement de l'utilisateur soit éclairé, l'ensemble des informations rappelées à l'article 2 des lignes directrices " cookies et autres traceurs " doit être disponible au moment de recueillir son choix. Il est recommandé, sur le premier niveau d'information, d'indiquer clairement les finalités des cookies, de permettre à l'utilisateur d'accéder à la liste des responsables du ou des traitements via, par exemple, un lien hypertexte ou un bouton accessible depuis le premier niveau d'information, de l'informer sur la possibilité de retirer le consentement à tout moment et, lorsque c'est pertinent, des conséquences découlant d'un refus des cookies ".

186. La formation restreinte note qu'au jour du contrôle en ligne, le site web www.voyance-en-direct.tv ne comportait pas de bandeau d'information concernant les cookies déposés sur les terminaux des utilisateurs lors de leur accès au site web. Les utilisateurs n'étaient donc ni informés des opérations réalisées, ni en capacité d'y consentir préalablement, tel qu'exigé par l'article 82 de la loi Informatique et Libertés éclairé par l'article 4 du RGPD.

187. La formation restreinte relève que ce n'est que lors du contrôle sur place, le 15 juillet 2021, que la délégation a constaté, lors de l'accès à ce site web, la présence du bandeau cookies suivant: " Nous utilisons des cookies et d'autres technologies de suivi pour améliorer votre expérience de navigation sur notre site, pour vous montrer un contenu personnalisé et des publicités ciblées, pour analyser le trafic de notre site et pour comprendre la provenance de nos visiteurs " comportant les boutons " J'accepte " et " Changer mes préférences ".

188. Elle relève également qu'après avoir cliqué sur le bouton " Changer mes préférences ", l'utilisateur accède à l'information suivante : " Vous pouvez modifier vos préférences et refuser l'enregistrement de certains types de cookies sur votre ordinateur lors de la navigation sur notre site. Vous pouvez également supprimer les cookies déjà stockés sur votre ordinateur, mais gardez à l'esprit que leur suppression peut vous empêcher d'utiliser des éléments de notre site web ".

189. La formation restreinte relève que, lors du contrôle sur place, le 15 juillet 2021, le premier niveau d'information fourni aux utilisateurs ne leur permettait pas d'être informés de la possibilité et la manière de refuser les traceurs, ainsi que des conséquences qui s'attachent à un refus, ni du droit de retirer son consentement.

190. La formation restreinte note qu'au jour de la séance de la formation restreinte, lors de l'accès au site web www.voyance-en-direct.tv, le bandeau cookies présent sur le site web comportait la mention suivante et les boutons " J'accepte ", " Je refuse " et " Changer mes préférences " : " Nous utilisons des cookies et d'autres technologies de suivi pour améliorer votre expérience de navigation sur notre site, pour vous montrer un contenu personnalisé et des publicités ciblées, pour analyser le trafic de notre site et pour comprendre la provenance de nos visiteurs ".

191. En conséquence, la formation restreinte considère que les faits précités constituent un manquement à l'article 82 de la loi Informatique et Libertés, dès lors qu'au moment du contrôle en ligne et jusqu'à la modification du bandeau cookies, lors de l'accès au site web www.voyance-en-direct.tv, les utilisateurs n'étaient pas informés de l'existence d'opérations permettant l'accès ou l'inscription d'informations dans leur terminal, conformément à l'article 82 de la loi Informatique et Libertés et l'article 4 du RGPD et donc en mesure d'y consentir de manière éclairée.

192. En deuxième lieu, la rapporteure relève que la délégation a constaté, lors du contrôle en ligne du 15 avril 2021, que trois cookies, soumis au recueil préalable du consentement des utilisateurs, sont déposés sur les terminaux des utilisateurs dès leur accès au site web www.voyance-en-direct.tv, avant toute action de sa part, sans que leur consentement soit préalablement recueilli.

193. En défense, la société fait valoir que, depuis la notification du rapport, aucun cookie non indispensable au fonctionnement du site n'est déposé sur le terminal de l'utilisateur.

194. La formation restreinte rappelle que l'article 82 de la loi Informatique et Libertés exige un consentement aux opérations de lecture et d'écriture d'informations dans le terminal d'un utilisateur mais prévoit des cas spécifiques dans lesquels certains traceurs bénéficient d'une exemption au consentement : soit lorsque celui-ci a pour finalité exclusive de permettre ou faciliter la communication par voie électronique, soit lorsqu'il est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

195. S'agissant des traceurs de mesure d'audience exemptés du recueil du consentement, la formation restreinte relève, à titre illustratif, que la Commission précise, dans ses lignes directrices du 17 septembre 2020, que " ces mesures sont dans de nombreux cas indispensables au bon fonctionnement du site ou de l'application et donc à la fourniture du service. En conséquence, la Commission considère que les traceurs dont la finalité se limite à la mesure de l'audience du site ou de l'application, pour répondre à différents besoins (mesure des performances, détection de problèmes de navigation, optimisation des performances techniques ou de l'ergonomie, estimation de la puissance des serveurs nécessaires, analyse de contenus consultés, etc.) sont strictement nécessaires au fonctionnement et aux opérations d'administration courante d'un site web (…) Afin de se limiter à ce qui est strictement nécessaire à la fourniture du service, la Commission souligne que ces traceurs doivent avoir une finalité strictement limitée à la seule mesure de l'audience sur le site ou l'application pour le compte exclusif de l'éditeur ".

196. S'agissant des traceurs à multi-finalités, la formation restreinte relève, toujours à titre illustratif, que la Commission précise, dans ses lignes directrices du 17 septembre 2020, que " l'utilisation d'un même traceur pour plusieurs finalités, dont certaines n'entrent pas dans le cadre de ces exemptions, nécessite de recueillir préalablement le consentement des personnes concernées, dans les conditions rappelées par les présentes lignes directrices. À titre d'exemple, dans le cas d'un service offert via une plate-forme nécessitant l'authentification des usagers (" univers logué "), l'éditeur du service pourra utiliser un cookie pour authentifier les utilisateurs sans demander leur consentement (car ce cookie est strictement nécessaire à la fourniture du service de communication en ligne). En revanche, il ne pourra utiliser ce même cookie pour des finalités publicitaires que si ces derniers ont effectivement consenti préalablement à cette finalité spécifique ".

197. La formation restreinte considère qu'afin de déterminer si l'inscription d'un cookie multi-finalités sur le terminal des utilisateurs nécessite le recueil préalable de leur consentement, il convient de déterminer si parmi les finalités, au moins l'une d'entre elles nécessite le recueil préalable du consentement.

198. En l'espèce, la formation restreinte note que la société procède au dépôt et à la lecture des cookies suivants sur les terminaux des utilisateurs, dès leur accès au site web www.voyance-en-direct.tv, avant toute action de leur part, sans recueil préalable de leur consentement : le cookies " test_cookie ", " .ga " et " .gid ".

199. S'agissant du cookie " test_cookie ", la formation restreinte relève qu'il poursuit une finalité publicitaire. Dès lors, il ne relève d'aucune des exceptions définies à l'article 82 de la loi Informatique et Libertés et ne peut être déposé sur le terminal de l'utilisateur sans recueil préalable de son consentement.

200. S'agissant des cookies " .ga " et " .gid ", la formation restreinte note qu'ils poursuivent plusieurs finalités, à savoir une finalité relative au suivi et à l'analyse de site web www.voyance-en-direct.tv et une finalité propre à Google concernant le maintien et la protection du service Analytics. 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. Par conséquent, ils ne relèvent d'aucune des exceptions définies à l'article 82 de la loi Informatique et Libertés et ne peuvent être déposés sur le terminal de l'utilisateur sans recueil préalable de son consentement.

201. La formation restreinte considère donc que le dépôt et la lecture de ces cookies sur le terminal de l'utilisateur nécessitent que l'utilisateur donne son consentement préalable, dans les conditions prévues par l'article 82 de la loi Informatique et Libertés, telles qu'éclairées par l'article 4, paragraphe 11, du RGPD.

202. La formation restreinte rappelle qu'elle a, à plusieurs reprises, adopté des sanctions pécuniaires pour manquement à l'article 82 de la loi Informatique et Libertés concernant le dépôt de cookies dont le recueil préalable du consentement est obligatoire, sur les terminaux des utilisateurs, avant toute action de leur part, sans recueil préalable de leur consentement (notamment délibérations SAN-2022-023 du 19 décembre 2022, SAN-2022-025, SAN-2022-026 et SAN-2022-027 du 29 décembre 2022).

203. En conséquence, la formation restreinte considère que les faits précités constituent un manquement à l'article 82 de la loi Informatique et Libertés pour les faits relevés au jour des contrôles, dès lors que des cookies soumis au recueil préalable du consentement étaient déposés sur le terminal des utilisateurs, avant toute action de leur part, sans leur consentement.

204. La formation restreinte relève qu'au cours de la procédure, la société KG COM a indiqué s'être mise en conformité avec les exigences de l'article 82 de la loi Informatique et Libertés puisqu'elle ne dépose plus de cookie non indispensable au fonctionnement du site web www.voyance-en-direct.tv.

205. En troisième lieu, la rapporteure relève que, lors du contrôle sur place du 15 juillet 2021, la délégation de contrôle a constaté que le bandeau cookies présent sur le site web www.voyance-en-direct.tv ne permettait pas de refuser les cookies aussi simplement que de les accepter.

206. En défense, la société fait valoir que son bandeau cookies comportera prochainement un bouton " refuser ".

207. La formation restreinte estime que, pour garantir la liberté du consentement, il devrait en l'espèce être aussi facile de refuser les cookies que de les accepter.

208. À titre d'éclairage, la formation restreinte indique que dans les lignes directrices relatives à l'application de l'article 82 de la loi Informatique et Libertés aux opérations de lecture et écriture dans le terminal d'un utilisateur, la Commission précise que " l'expression du refus de l'utilisateur ne doit donc nécessiter aucune démarche de sa part ou doit pouvoir se traduire par une action présentant le même degré de simplicité que celle permettant d'exprimer son consentement ".

209. La formation restreinte relève que, tel qu'il ressort des constatations effectuées lors du contrôle sur place du 15 juillet 2021, lorsqu'un utilisateur se rendait sur le site web www.voyance-en-direct.tv, il pouvait accepter le dépôt de cookies, soumis au recueil préalable du consentement, en une seule action, en cliquant sur le bouton intitulé " J'accepte " figurant sur le bandeau cookies.

210. Elle relève qu'en revanche, pour refuser ces cookies, l'utilisateur devait effectuer pas moins de cinq actions : cliquer sur le bouton " Changer mes préférences " afin d'accéder à l'interface de gestion des cookies (premier clic), cliquer sur les onglets " Cookies de fonctionnalité " (deuxième clic), " Cookies de suivi et de performance " (troisième clic), " Cookies de ciblage et de publicité " (quatrième clic) afin d'effectuer un choix sur le dépôt de ces cookies, cliquer sur le bouton " Sauvegarder mes préférences " (cinquième clic).

211. La formation restreinte considère qu'il n'était donc pas aussi simple de refuser les cookies que de les accepter et que le fait de rendre le mécanisme de refus des cookies plus complexe que celui consistant à les accepter revient en réalité à décourager les utilisateurs de refuser les cookies et à les inciter à privilégier la facilité du bouton " Tout accepter ". En effet, un utilisateur d'Internet est généralement conduit à consulter de nombreux sites. La navigation sur Internet se caractérise par sa rapidité et sa fluidité. Le fait de devoir cliquer sur " Changer mes préférences " et de devoir comprendre la façon dont est construite la page permettant de refuser les cookies est susceptible de décourager l'utilisateur, qui souhaiterait pourtant refuser le dépôt des cookies. Il n'est pas contesté qu'en l'espèce, la société offrait un choix entre l'acceptation ou le refus des cookies avant l'insertion du bouton " Tout refuser ", mais les modalités par lesquelles ce refus pouvait être exprimé, dans le contexte de la navigation sur Internet, biaisait l'expression du choix en faveur du consentement de façon à altérer la liberté de choix.

212. La formation restreinte souligne qu'elle a, à plusieurs reprises, adopté des sanctions pécuniaires pour manquement à l'article 82 de la loi Informatique et Libertés dans des cas où il n'était pas aussi simple pour les utilisateurs de refuser les cookies que de les accepter. Elle a notamment retenu dans des délibérations SAN-2022-023 du 19 décembre 2022 et SAN-2022-027 du 29 décembre 2022 que " le fait de rendre le mécanisme de refus des cookies plus complexe que celui consistant à les accepter revient en réalité à décourager les utilisateurs de refuser les cookies et à les inciter à privilégier la facilité du bouton " Accepter ". En effet, un utilisateur d'Internet est généralement conduit à consulter de nombreux sites. La navigation sur Internet se caractérise par sa rapidité et sa fluidité. Le fait de devoir cliquer sur " Plus d'options " et de devoir comprendre la façon dont est construite la page permettant de refuser les cookies est susceptible de décourager l'utilisateur, qui souhaiterait pourtant refuser le dépôt des cookies. Il n'est pas contesté qu'en l'espèce, la société offrait un choix entre l'acceptation ou le refus des cookies avant l'insertion du bouton " Tout refuser ", mais les modalités par lesquelles ce refus pouvait être exprimé, dans le contexte de la navigation sur internet, biaisait l'expression du choix en faveur du consentement de façon à altérer la liberté de choix " (également dans les délibérations SAN-2021-023 et SAN-2021-024 du 31 décembre 2021).

213. La formation restreinte note qu'au jour de la séance de la formation restreinte, lors de l'accès au site web www.voyance-en-direct.tv, le bandeau cookies présent sur le site web comportait un bouton " Je refuse ".

214. Par conséquent, la formation restreinte considère qu'un manquement aux dispositions de l'article 82 de la loi Informatique et Libertés, interprétées à la lumière du RGPD, est constitué, dans la mesure où, au moment du contrôle en ligne et jusqu'à la mise en place du bouton " Tout refuser ", l'utilisateur n'avait pas la possibilité de refuser les opérations de lecture et/ou d'écriture avec le même degré de simplicité qu'il avait de les accepter.

III. Sur la sanction et la publicité

215. 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 ".

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

217. En premier lieu, sur le principe du prononcé d'une amende, la société insiste en défense sur la responsabilité de son sous-traitant concernant les manquements relatifs à la sécurité et l'origine de l'incident de sécurité. Elle indique que les données qui ont été potentiellement accessibles ne concernent pas des données hautement personnelles ou des données sensibles. Par ailleurs, elle conteste le nombre de personnes concernées, sans pour autant communiquer une volumétrie.

218. Elle rappelle également l'absence de plaintes et considère que certains manquements sont peu préjudiciables pour les personnes concernées, notamment les manquements aux articles 12 et 28 du RGPD. Elle met également l'accent sur les efforts qu'elle a engagés pour se mettre en conformité à la suite de la notification du rapport.

219. La formation restreinte rappelle, d'abord, qu'elle doit tenir compte, pour le prononcé d'une amende administrative, des critères précisés à l'article 83 du RGPD, tels que la nature, la gravité et la durée de la violation, les mesures prises par le responsable du traitement pour atténuer le dommage subi par les personnes concernées, le degré de coopération avec l'autorité de contrôle et les catégories de données à caractère personnel concernées par la violation.

220. La formation restreinte relève, en outre, le nombre particulièrement élevé de manquements : neuf manquements au titre du RGPD (articles 5-1-c), 5-1-e), 6, 9, 12 et 13, 28, 32, 33) et un manquement au titre de la loi Informatique et Libertés (article 82). La société a ainsi fait preuve de multiples défaillances puisque les manquements constitués concernent une grande partie des règles relatives à la protection des données à caractère personnel, dont des obligations fondamentales du responsable du traitement (minimisation des données, limitation de la durée de conservation des données et d'accessibilité de l'information, licéité du traitement).

221. À titre d'exemple, l'enregistrement intégral et systématique de l'ensemble des appels téléphoniques passés entre les téléopérateurs et les prospects, ainsi qu'entre les voyants et les clients, à des fins de contrôle de la qualité du service et de preuve, constitue une pratique particulièrement intrusive pour les personnes concernées.

222. Par ailleurs, la société ne respectait pas l'article 82 de la loi Informatique et Libertés sur plusieurs aspects : défaut d'information, absence de consentement au dépôt de cookies non exemptés de consentement et déséquilibre entre les modalités offertes à l'utilisateur pour accepter ou refuser le dépôt de cookies sur son terminal. Ces faits constituent une atteinte substantielle au droit au respect à la vie privée et à la protection des données à caractère personnel des personnes concernées.

223. La formation restreinte rappelle également, à titre d'illustration, que la société n'a pas notifié à la CNIL la violation de données alors qu'elle disposait de l'ensemble des éléments permettant de vérifier son existence et qu'elle a identifié comme conséquence probable de celle-ci, la prospection commerciale non consentie.

224. La formation restreinte note, ensuite, que certains manquements concernent des catégories particulières de données soumises à un régime juridique strict (données de santé, informations sur l'orientation sexuelle) et des données hautement personnelles (données bancaires) devant faire l'objet d'une vigilance accrue compte tenu du risque de fraude.

225. La formation restreinte rappelle, également, qu'en qualité de responsable du traitement, la société est tenue de respecter ses obligations prévues au RGPD. Elle est notamment tenue d'exercer un contrôle satisfaisant et régulier sur les mesures techniques et organisationnelles mises en œuvre par son sous-traitant pour assurer la conformité au RGPD et notamment pour assurer la sécurité des données à caractère personnel traitées.

226. À cet égard, la formation restreinte relève que plusieurs mesures de sécurité élémentaires faisaient défaut en l'espèce, entrainant un risque pour les personnes concernées. La formation restreinte rappelle que les différents documents encadrant les relations contractuelles entre la société et ses sous-traitants ne comportent pas l'ensemble des mesures requises par l'article 28 du RGPD et certains documents ne sont pas signés par les prestataires. Ces faits ne sont pas de nature à assurer une protection efficace des données à caractère personnel traités par le biais de garanties contractuelles.

227. Enfin, la formation restreinte relève que les mesures de conformité qui ont été mises en place par la société à la suite de la notification du rapport, notamment concernant les cookies, n'exonère pas l'organisme de sa responsabilité pour les manquements constatés pour le passé.

228. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative pour les manquements aux articles 5-1-c) et e), 6, 9, 12, 13, 28, 32 et 33 du RGPD et à l'article 82 de la loi Informatique et Libertés.

229. En deuxième lieu, s'agissant du montant de l'amende, l'organisme insiste en défense sur le caractère déficitaire de son résultat net.

230. La formation restreinte considère que la situation financière de l'organisme doit être notamment prise en compte pour la détermination de la sanction et, en cas d'amende administrative, de son montant. Elle relève à ce titre qu'en 2020, le chiffre d'affaires net de la société KG COM s'élevait à […] euros et son résultat net déficitaire était de […] euros. La société a précisé, à titre indicatif, lors de la séance de formation restreinte que son chiffre d'affaires projeté, de janvier à août 2022, est d'environ […] euros, soit environ […] euros sur l'année 2022.

231. Dès lors, au regard des critères pertinents de l'article 83, paragraphe 2, du RGPD évoqués ci-avant, la formation restreinte considère comme justifié le prononcé d'une amende administrative d'un montant de 150 000 euros se répartissant comme suit : 120 000 euros pour les manquements au RGPD et 30 000 euros pour le manquement à la loi Informatique et Libertés.

232. En troisième lieu, s'agissant de la publicité de la sanction, l'organisme soutient qu'une telle mesure lui serait préjudiciable d'un point de vue économique.

233. La formation restreinte considère que, au regard de la pluralité des manquements relevés, de leur gravité, de la nature particulière des données traitées et du nombre de personnes concernées, la publicité de la présente décision est justifiée.

PAR CES MOTIFS

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

- prononcer à l'encontre de la société KG COM une amende administrative d'un montant de 120 000 (cent-vingt mille) euros pour manquements aux articles 5-1-c) et e), 6, 9, 12, 13, 28, 32 et 33 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données et d'un montant de 30 000 (trente mille) euros pour manquement 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 KG COM 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.