Délibération SAN-2024-020 du 5 décembre 2024

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Etat juridique : En vigueur

Date de publication sur Légifrance : Jeudi 19 décembre 2024

Délibération de la formation restreinte n° SAN-2024-020 du 5 décembre 2024 concernant la société KASPR

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Messieurs Philippe-Pierre CABOURDIN, président, Vincent LESCLOUS, vice-président, Madame Laurence FRANCESCHINI et Messieurs Bertrand DU MARAIS et Alain DRU, membres ;

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

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

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

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

Vu la décision n°2022-104C du 21 juin 2022 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par la société KASPR ;

Vu le rapport de Monsieur Fabien TARISSAN, commissaire rapporteur, notifié à la société KASPR le 3 mai 2024 ;

Vu les observations écrites versées par le conseil de la société KASPR le 13 juin 2024 ;

Vu la réponse du rapporteur à ces observations signifiée par commissaire de justice à la société KASPR le 12 juillet 2024 ;

Vu les observations écrites versées par le conseil de la société KASPR, reçues le 19 août 2024 ;

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

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 19 septembre 2024 :

- Monsieur Fabien TARISSAN, commissaire, entendu en son rapport ;

En qualité de représentants de la société KASPR :

- […].

La société KASPR ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. Créée en 2018, la société KASPR (ci-après " la société "), a son siège basé au 38 rue Dunois à Paris (75013), ses bureaux opérationnels sont situés au 198 avenue de France à Paris (75013). La société emploie 32 salariés. Elle a réalisé un chiffre d'affaires d'environ […] euros en 2021, […] euros en 2022, et […] euros en 2023.

2. La société KASPR développe et commercialise une extension (ci-après " l'extension KASPR ") disponible à partir du site " kaspr.io " et fonctionnant sur le navigateur CHROME, qui permet à ses utilisateurs d'obtenir les coordonnées professionnelles de personnes dont ils visitent le profil sur le réseau social LinkedIn.

3. Le 28 juillet 2022, faisant suite à plusieurs saisines, et en vertu de la décision n° 2022-104C du 21 juin 2022 de la présidente de la Commission nationale de l'informatique et des libertés (ci-après " la CNIL " ou " la Commission "), les services de la Commission ont effectué un contrôle sur audition des représentants de la société.

4. Ce contrôle avait pour objet de vérifier la conformité des traitements de données à caractère personnel mis en œuvre par la société KASPR aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil relatif à la protection des données à caractère personnel (ci-après " le RGPD " ou " le Règlement "), de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après " loi Informatique et Libertés ") et, le cas échéant aux dispositions des articles L251-1 et suivants du code de la sécurité intérieure.

5. Par courrier électronique du 9 août 2022, la société a fait parvenir à la CNIL plusieurs documents et éléments de réponse sollicités par les services de la Commission dans le cadre des investigations.

6. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 8 avril 2024, désigné Monsieur Fabien TARISSAN en qualité de rapporteur sur le fondement de l'article 39 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi Informatique et Libertés.

7. Le 3 mai 2024, à l'issue de son instruction, le rapporteur a fait notifier à la société un rapport détaillant les manquements au RGPD qu'il estimait constitués en l'espèce.

8. Ce rapport proposait à la formation restreinte de la Commission de prononcer une amende administrative à l'encontre de la société, ainsi qu'une injonction de mettre en conformité le traitement avec les articles 5, 6, 12, 14 et 15 du RGPD, assortie d'une astreinte à l'issue d'un délai de trois mois suivant la notification de la délibération de la formation restreinte. Il proposait également que cette décision soit rendue publique et ne permette plus d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

9. Par courrier électronique du 17 mai 2024, la société a sollicité un délai complémentaire auprès du président de la formation restreinte pour produire ses observations en réponse, qui lui a été accordé le 23 mai suivant, sur le fondement de l'article 40, alinéa 4 du décret du 29 mai 2019.

10. Le 13 juin 2024, la société a produit des observations en réponse au rapport du rapporteur.

11. Le 12 juillet 2024, le rapporteur a répondu aux observations de la société.

12. Le 19 août 2024, la société a présenté de nouvelles observations en réponse.

13. Par courrier du 6 septembre 2024, la société a reçu une convocation à la séance de la formation restreinte du 19 septembre suivant.

14. La société et le rapporteur ont présenté des observations orales lors de la séance de la formation restreinte du 19 septembre 2024.

I. Motifs de la décision

A. Sur le traitement en cause

15. L'outil KASPR est une extension pour le navigateur CHROME qui, lors de la visite du profil d'une personne sur LinkedIn, affiche les coordonnées professionnelles (numéro de téléphone et adresse électronique) de personnes physiques qui figurent dans la base de données KASPR. Pour accéder à ce service, l'utilisateur doit acheter et dépenser des " crédits " permettant d'afficher les coordonnées de la personne souhaitée (la personne cible). Le nombre de crédits dont bénéficie l'utilisateur est déterminé par le prix de son abonnement, qui peut être mensuel ou annuel.

16. En l'espèce, la formation restreinte relève que la société traite les données à caractère personnel de deux catégories distinctes de personnes :

- les personnes cibles, c'est à dire les personnes dont les coordonnées professionnelles ont été collectées par la société à partir de différentes sources, dont le réseau social LinkedIn et versées dans sa base de données ;

- les utilisateurs de l'extension KASPR, c'est-à-dire les clients de la société dont l'abonnement permet de visiter les profils LinkedIn des personnes cibles afin, notamment, d'obtenir leurs coordonnées professionnelles.

17. La finalité de l'extension KASPR est de permettre à ces utilisateurs de contacter les personnes cibles, par exemple pour de la prospection commerciale, du recrutement ou de la vérification d'identité, grâce aux coordonnées de professionnels obtenues. Les seules données pouvant être affichées par l'extension lors de la visite d'un profil LinkedIn sont le numéro de téléphone et l'adresse de courriel. Les données collectées concernant les données de contacts des personnes cibles sont les nom, prénom, adresse de courriel, numéro de téléphone, URL du profil LinkedIn ou autres réseaux sociaux, employeur, entreprise, intitulé du poste, compétences, intérêt professionnel, carrière, date d'embauche et de fin de poste, formation, lieu de travail, source de la donnée et date de la collecte

18. La formation restreinte observe que la société collecte les données par le biais de trois sources :

- des " fournisseurs " collectant eux-mêmes des données à partir de sources professionnelles publiquement accessibles comme LinkedIn, Whois, GitHub ;

- les annuaires des registres de noms de domaines, qui permettent de rechercher des informations sur un nom de domaine déjà existant et son titulaire ;

- l'import des contacts LinkedIn d'un utilisateur lors de l'activation de KASPR. Les utilisateurs KASPR synchronisent l'extension KASPR avec leur compte LinkedIn. La délégation a été informée que cela permet de récupérer les coordonnées disponibles sur LinkedIn des contacts directs des utilisateurs mais qui ne sont pas forcément visibles par l'intégralité des visiteurs du site LinkedIn. L'extension KASPR permet ainsi de rendre disponibles, dans la base de données KASPR, des données que les contacts LinkedIn des utilisateurs de KASPR souhaitaient limiter à leurs seuls contacts au sein du réseau social professionnel.

19. Environ 160 millions de contacts figurent dans la base de données constituée par la société, dont précisément […] au sein de l'Union Européenne, de la Norvège, de l'Islande et du Liechtenstein, l'origine géographique étant déterminée par l'adresse du lieu de travail.

B. Sur la compétence de la CNIL et l'application du mécanisme de cohérence

20. L'article 3, paragraphe 1 du RGPD dispose que " Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union ".

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

22. Les critères permettant de déterminer si une autorité de contrôle est concernée sont fixés par l'article 4 (22) du RGPD qui dispose qu'une autorité est " concernée par le traitement de données à caractère personnel parce que :

a) le responsable du traitement ou le sous-traitant est établi sur le territoire de l'État membre dont cette autorité de contrôle relève ;

b) des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être ; ou

c) une réclamation a été introduite auprès de cette autorité de contrôle ".

23. Le rapporteur considère qu'en application de l'article 3, paragraphe 1 du RGPD, dès lors que les activités du responsable de traitement ont lieu sur le territoire de l'Union, les obligations contenues dans le RGPD s'appliquent pour toutes les personnes concernées par ledit traitement, que celles-ci soient localisées au sein de l'Union européenne ou non.

24. Par ailleurs, le rapporteur considère que, dès lors que la délégation de la CNIL a constaté la présence dans la base de données KASPR de données à caractère personnel de personnes localisées en Suède, en Hongrie et dans le land de Saxe, ces autorités sont concernées.

25. En défense, si la société ne conteste pas la qualité d'autorité compétente de la CNIL pour connaître de la conformité au RGPD du traitement en cause, elle soutient que la CNIL n'est pas compétente pour se prononcer, en tant qu'autorité chef de file, sur la conformité au RGPD des traitements des données à caractère personnel des personnes situées en Hongrie, en Suède et dans le land de Saxe dès lors que ces autorités se sont déclarées non concernées. S'agissant ensuite du champ d'application territoriale du RGPD, la société considère que dans l'évaluation du nombre de personnes concernées par les

manquements qui lui sont reprochés, ne peuvent pas être pris en compte les personnes localisées en dehors de l'Union Européenne. La société soutient que dans son arrêt du 24 septembre 2019, la Cour de justice de l'Union européenne a considéré à l'occasion d'une question préjudicielle relative à la portée territoriale du droit au déréférencement que le RGPD ne pouvait produire d'effet que sur le territoire de l'Union européenne (CJUE, grande chambre, 24 septembre 2019, Google, n°C-507/17).

26. La formation restreinte relève que l'établissement unique de la société KASPR se trouve en France, que le traitement en cause a donc lieu dans le cadre de l'activité de cet établissement, et que la CNIL est ainsi l'autorité compétente pour connaitre de la conformité des traitements au RGPD, ce qui n'est pas contesté par la société.

27. Conformément à l'article 56 du RGPD, la CNIL a informé, le 19 septembre 2023, l'ensemble des autorités de contrôle européennes de sa compétence pour agir en tant qu'autorité de contrôle chef de file concernant les traitements transfrontaliers mis en œuvre par la société, compétence tirée par la CNIL de ce que l'établissement principal de la société se trouve en France. La formation restreinte note à ce propos que le formulaire intitulé " Article 56- Identification of LSA and CSA ", adressé à l'ensemble des autres autorités européennes de protection de données, a uniquement pour objet de permettre aux autres autorités d'avoir connaissance de l'ouverture d'un dossier par l'autorité chef de file et n'a pas pour objectif de déterminer de façon irréfragable leur qualité d'autorité concernée à ce stade. A l'inverse, la formation restreinte relève que la présence de données concernant des personnes établies sur le territoire d'un Etat membre en particulier est déterminant dans l'identification des autorités concernées.

28. En l'espèce, la délégation de contrôle de la CNIL a constaté qu'en plus de tous les autres contacts présents dans la base données, […] contacts dans la base de données KASPR sont localisés en Suède, […] contacts sont localisés en Hongrie et […] contacts sont localisés en Allemagne. Dès lors, l'ensemble des autorités européennes sont concernées au sens de l'article 4, paragraphe 22 du règlement.

29. Ainsi, la formation restreinte considère que le critère prévu au b) de l'article 4 (22) du RGPD est bien rempli en l'espèce, dès lors qu'il a été constaté que " des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être ".

30. En outre, la formation restreinte rappelle que le responsable de traitement dont l'établissement se trouve sur le territoire de l'Union est tenu de respecter le RGPD à l'égard de toutes les personnes dont il traite les données sans opérer de distinction entre les personnes selon leur localisation. La formation restreinte observe que les faits en cause dans le cas d'espèce s'écartent de ceux visés dans l'arrêt de la CJUE sur le déréférencement.

31. En effet, était en cause, la nécessaire mise en balance entre d'une part, le droit au respect de la vie privée d'une personne située sur le territoire de l'Union européenne, et d'autre part le droit à l'information d'une personne située en dehors de l'Union européenne, laquelle n'est ainsi pas une personne concernée dès lors que ses données n'étaient pas traitées. Il s'agissait d'une personne tierce au traitement. Or, en l'espèce, les personnes se trouvant hors du territoire de l'Union Européenne voient leurs données collectées et traitées par la société KASPR, laquelle est soumise au respect du RGPD. Ainsi, aux termes de l'article 83(2)(a), il convient de prendre en compte le fait que la société traite 160 millions de contacts, étant précisé qu'une même personne physique peut correspondre à plusieurs contacts.

32. En application de l'article 60, paragraphe 3 du RGPD, le projet de décision adopté par la formation restreinte a été transmis aux autres autorités de contrôle européennes compétentes, en vue de leur permettre d'effectuer des objections pertinentes et motivées sur les traitements et manquements qui les concernent, le 5 novembre 2024.

33. Au 4 décembre 2024, aucune des autorités de contrôle concernées n'avait formulé d'objection pertinente et motivée à l'égard de ce projet de décision concernant les manquements constatés, de sorte que, en application de l'article 60, paragraphe 6, du RGPD, ces dernières sont réputées l'avoir approuvé.

C. Sur le manquement à l'obligation de disposer d'une base légale (article 6 du RGPD)

34. Aux termes de l'article 6 du RGPD, " 1. 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 ".

35. Le recours à la base légale de l'intérêt légitime, en application de l'article 6, paragraphe 1, f) du RGPD, pour fonder légalement un traitement est soumis à trois conditions : l'intérêt poursuivi doit être légitime, il est nécessaire de traiter les données à caractère personnel aux fins des intérêts légitimes poursuivis et le traitement ne doit pas heurter les droits et intérêts des personnes dont les données sont traitées, compte tenu de leurs attentes raisonnables.

36. A titre d'éclairage, s'agissant de la base légale de l'intérêt légitime, le considérant 47 du RGPD énonce qu'un tel intérêt peut " constituer une base juridique pour le traitement, à moins que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent, compte tenu des attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable du traitement. Un tel intérêt légitime pourrait, par exemple, exister lorsqu'il existe une relation pertinente et appropriée entre la personne concernée et le responsable du traitement dans des situations telles que celles où la personne concernée est un client du responsable du traitement ou est à son service ".

37. Le rapporteur précise que le manquement à l'article 6 du RGPD développé dans le rapport de sanction ne vise que les données collectées via le réseau social LinkedIn - s'agissant de personnes qui ont entendu restreindre l'affichage de leurs coordonnées - et non les autres sources de collecte. Il considère que la mise à disposition des données de contact des personnes cibles par la société KASPR à ses utilisateurs alors qu'elles avaient choisi de ne pas les rendre publiques à tous, excède ce à quoi peuvent raisonnablement s'attendre les personnes qui s'inscrivent sur un réseau social professionnel tel que LinkedIn.

38. En défense, la société considère que le traitement est fondé sur la base légale de l'intérêt légitime, dès lors que les utilisateurs de LinkedIn s'inscrivent sur ce réseau social pour bénéficier d'une mise en relation avec d'autres professionnels, et qu'il n'est ainsi pas nécessaire de collecter leur consentement. Elle soutient également que la nécessité de vérification d'identité relève des attentes raisonnables des professionnels dans un contexte d'accroissement des risques quant à la validité des profils numériques. Elle estime toutefois que les risques d'hameçonnage et d'usurpation d'identité soulevés par le rapporteur manquent en fait et ne prennent pas en compte les garanties mises en place par KASPR. La société rappelle que l'extension KASPR traite des coordonnées professionnelles et est alimentée par des sources publiques professionnelles légitimes autres que LinkedIn. La société ajoute que la validité de cette base juridique au bénéfice de KASPR ne saurait se limiter qu'à la prise en compte de son seul et unique intérêt et cite une publication de la CNIL " La prospection commerciale par courrier électronique, Pour les professionnels (B to B) du 18 mai 2009 qui indique que " la prospection vers les professionnels peut (parfaitement) être fondée sur l'intérêt légitime de l'organisme ".

39. Enfin, la société relève que la collecte des données de contact est effectuée en adéquation avec les choix exprimés par les utilisateurs du réseau social LinkedIn. Elle précise dans ces dernières écritures que ces derniers ont la possibilité de rendre leurs coordonnées visibles via les paramètres de l'interface LinkedIn, en choisissant parmi quatre options : 1) " uniquement visible par moi ", 2) " Tout le monde sur LinkedIn ", 3) " relations de 1er niveau " et 4) " Relations de 1er et 2e niveau ". La société explique que ce n'est que dans ces deux dernières hypothèses où l'utilisateur rend visible son adresse électronique par ses relations de premier et de second niveau, qu'elle procède à la collecte des données. Lorsque les personnes ont choisi l'option n°1 " uniquement par moi ", leurs données ne sont pas collectées.

40. A titre liminaire, la formation restreinte précise que le manquement développé ci-dessous vise les données à caractère personnel collectées sur le réseau social LinkedIn des personnes cibles ayant fait le choix de limiter ou de masquer la visibilité de leurs coordonnées. La formation restreinte relève également en réponse à un des arguments de la société que la circonstance que la base de données en cause soit uniquement constituée des coordonnées " professionnelles " des personnes cibles demeure sans incidence sur le caractère " personnel " de ces données lorsque ces données se rapportent à des personnes physiques, selon une jurisprudence bien établie de la Cour de justice de l'Union européenne (voir, notamment, CJUE, 9 novembre 2010, Volker e. a., aff. jtes C-92/09 et C-93/09, pt. 59).

41. S'agissant de l'intérêt poursuivi - en ce qu'il présente une nature commerciale et qu'il est consubstantiel au modèle économique de la société – la formation restreinte estime qu'il peut être qualifié de légitime et que les données collectées aux fins de ces intérêts peuvent apparaitre nécessaires, intérêt pouvant également s'étendre aux clients de KASPR qui bénéficient effectivement d'un intérêt en utilisant ces contacts pour de la prospection commerciale ou le recrutement.

42. Cet intérêt légitime poursuivi par la société doit être considéré au regard de la mise en balance des intérêts, des libertés et des droits fondamentaux des personnes concernées et des intérêts légitimes poursuivis par la société, la formation

restreinte rappelle que pour fonder un traitement sur la base de l'intérêt légitime, le traitement ne doit pas heurter les droits et intérêts des personnes dont les données sont traitées, compte tenu de leurs attentes raisonnables.

43. Or, en l'espèce, la formation restreinte considère que dès lors que les personnes font usage de leur liberté de choix en restreignant la visibilité de leurs données à caractère personnel, ce choix s'impose nécessairement aux tiers. Ainsi, si un professionnel qui est inscrit sur LinkedIn choisit de limiter la visibilité de ses coordonnées, il ne peut être soutenu que la collecte de ses données par la société KASPR figure au titre des attentes raisonnables de cette personne.

44. La formation restreinte observe qu'il ressort de l'interface des paramètres LinkedIn, que si les personnes cibles qui ont choisi de restreindre la visibilité de leurs coordonnées avaient réellement souhaité que leurs coordonnées professionnelles apparaissent à tous, elles auraient choisi d'activer le paramètre permettant que leurs coordonnées soient visibles de tous les utilisateurs. Elle considère en l'espèce que le fait pour les personnes cibles d'avoir choisi de masquer leurs coordonnées équivaut à une forme d'opposition, corolaire indispensable de l'intérêt légitime, laquelle doit être prise en compte par la société qui n'a ainsi pas d'intérêt légitime pour collecter les coordonnées masquées.

45. Ainsi, en révélant les données des personnes cibles à des personnes qui leur sont inconnues alors qu'elles avaient choisi de restreindre la visibilité de leurs coordonnées (relations de 1er et/ou de 2ème niveaux), la société va directement à l'encontre de leurs " attentes raisonnables ", au sens du considérant 47 du RGPD. Par ailleurs, la formation restreinte note qu'il ressort de l'analyse d'impact de la société que dès lors que le traitement est invisible, les personnes cibles peuvent " ne pas être conscientes que KASPR ou les utilisateurs finaux des données de profil ont collecté leurs données ". Enfin, si la société soutient qu'elle a pris des mesures permettant de limiter le risque pour les personnes dans son analyse d'impact, la formation restreinte note que celle-ci n'envisage pas le cas de figure des personnes cibles dont les données sont collectées alors qu'elles avaient choisi de masquer la visibilité de leurs coordonnées. Elle n'a ainsi pris aucune mesure permettant de limiter le risque d'atteinte aux droits des personnes cibles.

46. Contrairement à ce qu'avance la société, il ne peut être soutenu que les personnes cibles, en autorisant certains de leurs contacts à prendre connaissance de leurs coordonnées, ont, par cette action, entendu autoriser la société KASPR à collecter de telles données. En ce sens, aucune " relation pertinente et appropriée " au sens du considérant précité ne lie les personnes cibles à la société, en ce qu'elles ne sont pas utilisatrices de l'extension KASPR mais simplement des contacts des clients de KASPR qui utilisent l'extension.

47. Par ailleurs, la formation restreinte remarque que plusieurs plaignants ayant été démarchés par des utilisateurs de l'extension KASPR, que ce soit par voie électronique ou par téléphone, ont fait part aux services de la Commission de leurs interrogations sur le fondement et sur la légitimité de la collecte et de la mise à disposition de leurs données à caractère personnel par la société.

48. Bien que n'étant pas réalisé par la société, ce démarchage est rendu possible par l'extension KASPR qui révèle à ses utilisateurs les coordonnées de contact des personnes cibles figurant dans sa base de données et conduit certains de ses clients utilisateurs à effectuer ce démarchage. En outre, si la société soutient que les coordonnées des personnes démarchées ont pu être collectées à partir d'autres sources que LinkedIn, cette circonstance est sans incidence sur la caractérisation du manquement en ce que la société n'était pas fondée à collecter les données des personnes qui avaient choisi de restreindre leur visibilité.

49. La formation restreinte souligne que la politique de confidentialité de LinkedIn insiste justement sur le fait que les données traitées à partir de son réseau social le soit conformément aux préférences des utilisateurs : " Toutes les données que vous incluez dans votre profil ou dans le contenu que vous publiez, ainsi que vos actions sur les réseaux sociaux (…) réalisées sur nos Services, sont visibles par d'autres personnes selon vos préférences ".

50. Au vu de tous ces éléments, la formation restreinte considère que les intérêts ou les libertés et droits fondamentaux des personnes concernées, notamment leur droit au respect de la vie privée, prévalaient sur l'intérêt légitime du responsable de traitement à traiter leurs données pour pouvoir assurer le fonctionnement de son extension, de sorte que le fondement juridique de l'intérêt légitime de la société ne peut être retenu.

51. Enfin, en ce qui concerne les autres bases légales, la formation restreinte relève que les personnes dont les données de contacts ont été aspirées n'ont jamais consenti d'une quelconque manière à l'aspiration de leurs données de contacts, ni à leur transmission à la société pour faire fonctionner l'extension KASPR.

52. Elle relève, en outre, qu'aucun contrat ne lie les personnes concernées à la société KASPR, ce qui n'est d'ailleurs pas contesté par la société.

53. Ainsi, la formation restreinte considère que ni la base légale du consentement, ni celle du contrat, ni aucune autre des bases légales (respect d'une obligation légale, sauvegarde des intérêts vitaux de la personne concernée ou exécution d'une mission d'intérêt public), n'apparaissent comme une base légale valable pour le traitement en cause.

54. Il résulte de ce qui précède que la collecte des données de contacts à travers l'import des contacts LinkedIn des utilisateurs ayant décidé de ne pas rendre visibles leurs données de contact à l'ensemble des autres utilisateurs, utilisés pour l'alimentation de la base de données de l'extension KASPR est dépourvue de base juridique, de sorte qu'un manquement à l'article 6 du RGPD est constitué.

D. Sur le manquement à l'obligation de définir et de respecter une durée de conservation des données proportionnée à la finalité du traitement (article 5-1-e du RGPD)

55. 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 (…) ".

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

57. A titre liminaire, il convient de noter que la société collecte et conserve d'une part, les données de contacts des personnes cibles et d'autre part, les données des utilisateurs de l'extension KASPR qui sont utilisées par la société à des fins de prospection commerciale.

58. Le rapporteur relève que si l'extension a été créé en 2018, lors du contrôle sur audition du 28 juillet 2022, la CNIL a été informée que la société KASPR n'avait pas encore formalisé de politique de conservation des données. Ce n'est que dans le cadre de la présente procédure contradictoire que la société a précisé avoir réfléchi à sa politique de conservation des données dès juillet 2021.

59. Le rapporteur considère, s'agissant des clients de KASPR, que, jusqu'à la redéfinition par la société de sa politique de confidentialité mise à jour en juin 2024, celle-ci conservait les données des clients à des fins de prospection commerciale de manière illimitée tant que ces derniers ne s'y étaient pas opposés. Il considère que cela est incompatible avec le principe de conservation pour une durée proportionnée.

60. Il relève ensuite s'agissant des personnes cibles que la société n'avait pas, au jour du contrôle sur audition effectué par la Commission le 28 juillet 2022, défini de politique de durée de conservation et qu'en tout état de cause, la société n'est pas fondée à conserver indéfiniment les données des personnes cibles, au risque de faire perdre irrémédiablement à ces personnes le contrôle de leurs données.

61. La société soutient, s'agissant des clients de KASPR, que le point de départ de la durée de conservation de leurs données à des fins de prospection commerciale se renouvelle automatiquement à chaque échéance d'abonnement jusqu'à la résiliation par les clients de leur abonnement. Elle précise qu'elle conserve désormais les données durant trois ans à compter de la fin de l'abonnement, et ce depuis la rédaction de la note relative à la conservation des données par KAPSR en juillet 2021.

62. La société soutient, s'agissant des personnes cibles, que la conservation de ces données est au cœur du service proposé par KASPR à travers son extension et qu'elle a désormais prévu une durée de conservation des données de cinq ans qui commence à courir à chaque mise à jour périodique des données personnelles des personnes cibles.

63. A titre liminaire, la formation restreinte souligne que le manquement à l'article 5-1-e ne concerne pas les données des personnes dont il vient d'être dit aux paragraphes 40 à 50 qu'elles étaient traitées sans base juridique valable, lesquelles n'auraient pas dû être versées et conservées dans la base de données.

64. En premier lieu, la formation restreinte relève, s'agissant des clients de KASPR, qu'au jour du contrôle, la politique de confidentialité de la société indiquait clairement que les données des clients étaient conservées à des fins de prospection commerciale jusqu'à ce que ces derniers s'y opposent. Or, la formation restreinte observe qu'une telle conservation doit être nécessairement limitée dans le temps et que la société ne peut pas se contenter d'une absence d'opposition des utilisateurs pour conserver indéfiniment leurs données après la fin de la durée de la relation commerciale.

65. La formation restreinte relève néanmoins que dans ses écritures, la société a indiqué que la politique de confidentialité en vigueur à la date des contrôles ne reflétait pas la pratique de la société. Elle produit en ce sens des documents internes aux termes desquels la société indique d'une part, appliquer une durée de conservation de trois ans à partir de la fin de la relation commerciale et d'autre part, purger les données ayant atteint cette durée de conservation.

66. La formation restreinte considère dès lors que s'agissant de la conservation des données des clients de la société, aucun manquement à l'article 5-1-e n'est caractérisé.

67. En second lieu, s'agissant des personnes cibles dont les données n'ont pas été collectées de façon illicite [c'est-à-dire les personnes qui ont choisi de laisser visibles leurs coordonnées sur LinkedIn], la formation restreinte ne conteste pas la nécessité pour la société de conserver les données des personnes cibles ne s'étant pas opposées au traitement de leurs données dans la mesure où leur divulgation aux clients de la société constitue le principe du traitement. Elle relève toutefois qu'initialement, la société indiquait dans sa politique de confidentialité qu'elle conservait les données sans limite de temps et que ce n'est qu'en 2021, soit trois ans après la mise en œuvre du traitement, que la société a commencé à redéfinir sa politique de durée de conservation.

68. En tout état de cause, la formation restreinte relève que la politique de conservation établie par la société postérieurement au contrôle prévoit que les données sont conservées pendant 5 ans à partir de chaque mise à jour des données, laquelle intervient généralement lorsqu'une personne change de poste ou d'employeur.

69. Or, la formation retreinte note que pour les personnes qui changent de poste ou d'employeur dans un intervalle de moins de 5 ans, ce renouvellement de la durée de conservation conduit à une conservation de leurs données disproportionnée.

70. La formation restreinte considère que cette conservation " dynamique " par automaticité n'est pas compatible avec le respect du principe de conservation proportionnée.

71. En effet, les personnes cibles ne sont pas utilisatrices du service proposé par KASPR et n'ont pas de relation avec le responsable de traitement. Les personnes cibles sont ainsi passives vis-à-vis du traitement et captives de celui-ci, dès lors qu'elles ne font pas le choix d'être intégrées dans la base de données.

72. La formation restreinte souligne que contrairement à des personnes qui auraient créé un compte en ligne sur un réseau social ou un site de commerce électronique et pour lesquelles il est possible de déterminer à quel moment elles sont devenues inactives il n'est, par nature, pas possible de déterminer un tel moment pour les personnes dont KASPR traite les données.

73. Si la société explique avoir mis en place depuis le 18 mai 2022 une campagne d'information par courriel qui permet aux personnes de s'opposer au traitement de leurs données et donc, d'y mettre fin, la formation restreinte relève que pour les personnes se trouvant dans le cas de figure décrit au point 70, l'envoi de ce message constituait à ce jour la seule occasion pour elles de faire part de leur volonté de ne plus figurer dans la base de données de la société. Dans les cas de figure où les personnes ne s'opposeraient pas au traitement à l'occasion de la réception de ce message, la société conservera leurs données indéfiniment.

74. Ainsi, la formation restreinte estime qu'il conviendrait que la société cesse le renouvellement dynamique automatique de la conservation des données à caractère personnel des personnes cibles afin que KASPR ne conserve pas leurs données de manière indéterminée et illimitée, mais au plus pendant cinq ans.

75. Il résulte de ce qui précède que la politique de conservation des durées définie par la société n'est pas proportionnée au regard des spécificités du traitement, ce qui constitue un manquement à l'article 5-1-e du RGPD.

E. Sur le manquement à l'obligation de transparence et d'information des personnes (articles 12 et 14 du RGPD)

76. 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 ".

77. L'article 14 du RGPD prévoit que lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée par le traitement, le responsable de traitement fournit à cette dernière les éléments d'information visés à ce même article " dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées ".

78. Ainsi, au titre de cet article, le responsable de traitement doit fournir à la personne concernée des informations notamment sur l'identité et les coordonnées du responsable du traitement (et le cas échéant les coordonnées du délégué à la protection des données), les finalités du traitement, sa base juridique, les catégories de données à caractère personnel concernées, le cas échéant les destinataires ou les catégories de destinataires des données, le fait que le responsable du traitement a l'intention d'effectuer un transfert des données vers un pays tiers ainsi que, si cela est nécessaire pour garantir un traitement équitable et transparent, la durée de conservation des données, l'existence des différents droits dont bénéficient les personnes dont celui de demander au responsable du traitement l'accès aux données à caractère

personnel, la rectification ou celui de s'opposer au traitement, la source d'où proviennent les données et l'existence éventuelle d'une prise de décision automatisée.

79. Aux termes du paragraphe 5, b), de ce même article, cette obligation d'information ne s'impose toutefois pas lorsque " la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés " ou lorsque le respect de cette obligation d'information " est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement ".

80. Dans ses lignes directrices du 29 novembre 2017 révisées le 11 avril 2018 relatives à la transparence, le groupe de travail " article 29 " sur la protection des données souligne que " Les articles 13 et 14 font référence à l'obligation imposée au responsable du traitement de "[fournir] toutes les informations suivantes...". Le mot " fournir " est crucial en l'occurrence. Il signifie que le responsable du traitement doit prendre des mesures concrètes pour fournir les informations en question à la personne concernée ou pour diriger activement la personne concernée vers l'emplacement desdites informations ". Il ressort ainsi des lignes directrices que " La personne concernée ne doit pas avoir à chercher activement les informations couvertes par ces articles parmi d'autres informations telles que les conditions d'utilisation d'un site internet ou d'une application " (point 33).

81. Le rapporteur relève, s'agissant de l'obligation d'information, que ce n'est qu'à partir du 18 mai 2022 que la société a commencé à informer les personnes concernées que leurs données à caractère personnel avaient été collectées dans un courriel en langue anglaise renvoyant vers un lien permettant de s'opposer au traitement. Le rapporteur considère pourtant que la société était en capacité d'informer les personnes cibles, dès le déploiement de l'application, que leurs données étaient traitées, dès lors que parmi les données qu'elle collecte figure une adresse de messagerie électronique.

82. Le rapporteur relève ensuite, s'agissant de l'obligation de transparence, que l'information délivrée dans le courriel d'information envoyé depuis le 18 mai 2022 est exclusivement rédigée en anglais, ce qui ne permet pas d'informer valablement les personnes ne maitrisant pas cette langue.

83. En défense, la société soutient qu'entre 2018 et 2022, soit entre la création de l'extension et la mise en place de courriels d'information relatifs au traitement, l'information des personnes a été faite par l'intermédiaire des politiques de confidentialité de LinkedIn et de KASPR, et que si la communication mise en œuvre le 18 mai 2022 était uniquement disponible en langue anglaise, cela ne constitue pas un manquement à l'obligation de transparence dès lors que l'extension KASPR est utilisée par un public de professionnels pour lesquels cette langue peut être considérée comme était couramment utilisée au sein de l'Union européenne.

84. A titre, liminaire, la formation restreinte souligne que le manquement aux articles 12 et 14 ne concerne pas l'information des personnes dont les données ont étés collectées de façon illicite, comme exposé aux paragraphes 40 à 50, l'obligation d'information de ces personnes étant, de ce fait, sans objet. La formation restreinte note toutefois que si la société procédait à la collecte (qu'elle considérait à tort comme licite) de ces données, elle n'informait pas non plus les personnes concernées.

85. La formation restreinte note en premier lieu, s'agissant de l'obligation d'information, que les données des personnes cibles ont été collectées et traitées pendant près de 4 ans, sans qu'aucune information ne leur soit transmise par la société, cette dernière ne prévoyant dans son analyse d'impact que depuis juillet 2022 qu'elle " notifie toutes les personnes concernées présentes dans sa base de données en conformité avec ses obligations prévues par l'article 14 du RGPD et constitue une équipe dédiée à la gestion des demandes d'accès dans les délais impartis ".

86. La formation restreinte considère que la société ne peut se prévaloir de sa politique de confidentialité ou de celle de LinkedIn pour considérer qu'elle a rempli son obligation d'information vis-à-vis des personnes concernées par le traitement. La formation restreinte note à ce propos que dans sa politique de confidentialité, la société LinkedIn précise " Toutes les données que vous incluez dans votre profil ou dans le contenu que vous publiez, ainsi que vos actions sur les réseaux sociaux (…) réalisées sur nos Services, sont visibles par d'autres personnes selon vos préférences ". Or la pratique de la société KASPR, en rendant accessible des données qu'un utilisateur souhaitait garder " privées ", va à l'encontre de leur volonté. La politique de confidentialité de KASPR n'apporte quant à elle aucune information précise notamment sur la source des données collectées, se contentant d'indiquer " Nous collectons ces données auprès de sources publiques, d'annuaires professionnels et de nos partenaires ponctuellement ".

87. La formation restreinte considère en second lieu, s'agissant de l'obligation de transparence, que l'information des personnes dont les coordonnées sont traitées par un courriel uniquement disponible en anglais, ne répond pas à l'exigence de fourniture d'une information transparente posée à l'article 12 du Règlement (CNIL, FR, 29 décembre 2023, Sanction, n°SAN 2023-023). La formation restreinte rappelle que selon les lignes directrices du groupe de travail " de l'Article 29 " sur la transparence au sens du règlement (UE) 2016/679, adoptées le 11 avril 2018, un aspect primordial du principe de transparence réside dans le fait que " la personne concernée devrait être en mesure de déterminer à l'avance ce que la portée et les conséquences du traitement englobent afin de ne pas être prise au dépourvu à un stade ultérieur

quant à la façon dont ses données à caractère personnel ont été utilisées " et qu'" Une traduction dans une ou plusieurs langues devrait être fournie lorsque le responsable du traitement cible des personnes concernées parlant ces langues ".

88. En l'espèce, si la société soutient que les professionnels dont les données sont collectées maîtrisent la langue anglaise dès lors qu'ils travaillent au sein de l'Union européenne, la formation restreinte considère que le seul fait que ces personnes soient inscrites sur le réseau social et travaillent dans un pays de l'Union européenne ne préjuge pas de leur niveau d'anglais. Toute personne peut en effet s'inscrire sur LinkedIn, sans nécessairement exercer une profession qui requiert l'usage de l'anglais, comme l'a récemment soulevé l'autorité néerlandaise de protection des données dans le cadre d'un manquement à l'obligation de transparence à l'encontre des sociétés Uber Technologies Inc. et Uber BV. L'autorité a en effet considéré que le responsable de traitement est dans l'obligation de traduire les informations fournies aux personnes dont les données sont traitées dans une langue qu'elles comprennent, et qu'il n'est pas possible de préjuger de leur niveau d'anglais (Dutch data protection authority, 11 décembre 2023, Uber Technologies Inc. et Uber BV).

89. Or en l'espèce, l'absence d'information compréhensible pour les personnes avait pour conséquence, jusqu'à la mise en place d'informations disponibles en plusieurs langues dont la société a fait part dans le cadre de ses deuxièmes observations, de les priver de la possibilité de s'opposer au traitement et donc au versement de ces données dans la base de la société.

90. Si la société note que certains plaignants ont adressé leur demande d'exercice des droits en anglais, la formation restreinte rappelle qu'il n'est pas possible de présupposer du niveau d'anglais de chaque personne dont le contact est présent dans la base de données KASPR, et note à ce propos que même lorsque les plaignants se sont adressés en français à la société, celle-ci a répondu en anglais.

91. Enfin, la formation restreinte note que la société a indiqué pour la première fois dans ses observations produites le 19 août 2024 qu'elle permettait désormais aux personnes de sélectionner la langue de leur choix concernant le courriel d'information et la politique de confidentialité de KASPR afin de les lire en français, espagnol, néerlandais ou allemand, sans toutefois préciser la date à laquelle cette option a été mise en œuvre, ni pour quelle raison ces documents n'ont pas été mis à disposition dans toutes les langues parlées au sein de l'Union européenne.

92. Il résulte de ce qui précède qu'entre 2018 et 2022 aucune information n'était fournie aux personnes cibles qui n'avaient pas restreints la visibilité de leurs données et que depuis 2022, une information est délivrée en anglais, ce qui ne répond pas à l'exigence de transparence, de sorte qu'un manquement aux articles 12 et 14 est constitué jusqu'à la mise en place de la possibilité pour les personnes de sélectionner la langue de leur choix.

F. Sur le manquement à l'obligation de faire droit aux demandes d'exercice du droit d'accès (article 15 du RGPD)

93. Aux termes de l'article 15, paragraphe 1, point g) du Règlement : " la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi que, […] lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source ".

94. L'article 12, paragraphe 4, du RPGD prévoit que " le responsable du traitement fournit à la personne concernée des informations sur les mesures prises à la suite d'une demande formulée en application des articles 15 à 22, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande ".

95. Le rapporteur note qu'il ressort de plusieurs saisines que les plaignants ayant fait l'objet de démarchage et ayant interrogé la société KASPR sur l'origine des données n'ont reçu aucune réponse précise de la part de la société, cette dernière se contentant de leur indiquer que les données étaient disponibles sur des sources publiquement accessibles.

96. Le rapporteur considère que la société aurait dû, dès lors qu'elle est en capacité d'identifier certaines des sources utilisées pour collecter les données présentes dans sa base de données, citer les sources de collecte possibles dans le cadre des demandes d'accès, même si elle n'était pas en mesure d'indiquer aux plaignants la source précise de collecte des données à caractère personnel les concernant.

97. En défense, la société fait valoir que la prise en compte de plaintes postérieures au contrôle sur audition porte atteinte aux droits de la défense en ce que ce n'est qu'à l'occasion de la préparation de ses observations en réponse au rapport du rapporteur qu'elle a eu la possibilité de démontrer la manière dont ces plaintes avaient été traitées.

98. La société ajoute qu'elle n'avait pas la capacité technique, avant janvier 2022, de retracer de manière distincte les différentes catégories de sources de données intégrées à la base de données KASPR, et qu'elle n'était pas en mesure de le faire de manière rétroactive à partir de janvier 2022.

99. La formation restreinte considère, en premier lieu, que la société a disposé du temps et des facilités nécessaires afin d'apporter tout élément de nature à démontrer le sort réservé aux plaintes communiquées par le rapporteur à l'appui de son rapport initial. Elle considère qu'aucune atteinte aux droits de la défense n'est constituée, les manquements étant antérieurs au prononcé de la sanction.

100. La formation restreinte considère, en second lieu, que la société doit pouvoir indiquer " toute information disponible quant à la source " des données qu'elle détient sur les personnes en application de l'article 15 précité, notamment où a été récupéré le numéro de téléphone professionnel de la personne, dans le cas où elle dispose de cette information. Or en l'espèce, il ressort des saisines que les plaignants s'interrogeaient sur la manière dont la société avait obtenu leurs coordonnées, sans qu'une réponse précise ne leur ait été apportée, la société se contentant d'indiquer que les données étaient disponibles sur des sources publiquement accessibles. Si la société soutient qu'elle a, conformément aux lignes directrices du CEPD sur les droits des personnes concernées - droit d'accès n°01/2022 du 28 mars 2023, répondu aux demandes d'accès en mettant en place un mécanisme de renvoi de deuxième niveau vers des informations plus précises, la formation restreinte note qu'il ressort des mêmes lignes directrices qui présentent un exemple, que : " S'il n'est pas possible de déterminer ex ante laquelle des entreprises interviendra dans le traitement, il suffit de mentionner les noms des entreprises éligibles dans la politique de confidentialité. Dans le cadre d'une demande fondée sur l'article 15, outre les informations selon lesquelles des informations relatives à la solvabilité ont été obtenues, il serait alors nécessaire (a posteriori) d'indiquer quelles sociétés ont été impliquées exactement. Il ressort clairement de l'article 15, paragraphe 1, point g), que les informations sur le traitement des données comprennent " toute information disponible quant à leur source " lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée ".

101. La formation restreinte considère que si la société pouvait fournir les informations requises par l'article 15 précité dans le cadre d'une information de second niveau, c'est-à-dire en intégrant un lien dans le courriel d'information renvoyant vers le site internet de KASPR et en particulier vers sa politique de confidentialité des données, celle-ci n'est pas assez précise au vu des informations dont disposait la société sur les sources des données. En effet, il est indiqué dans la politique de confidentialité en vigueur au moment de la réponse qu'elle a apporté aux plaignants, s'agissant de l'origine des données à caractère personnel des personnes cibles :" Nous collectons ces données auprès de sources publiques, d'annuaires professionnels et de nos partenaires ponctuellement ". Or, il ressort des pièces du dossier que la société KASPR a pourtant identifié précisément une partie des sources qui alimentent sa base de données.

102. En effet, elle a indiqué à la délégation de contrôle trois sources principales de données (point 19) qui sont d'ailleurs aujourd'hui visées dans la dernière version de sa politique de confidentialité, : " Nous collectons ces données auprès des réseaux sociaux tels que LinkedIn, des annuaires professionnels tels que Whois et GitHub et de nos fournisseurs de données de temps à autres ".

103. La formation restreinte considère toutefois que la mention de " nos fournisseurs de données de temps à autres " ne donne aucune précision sur les différents " fournisseurs " dont il s'agit en l'espèce et considère que dès lors que KASPR a connaissance des différentes sources précises, il lui appartient de les renseigner.

104. Ainsi, la société était en capacité de fournir davantage d'informations aux plaignants s'agissant des sources des données, quand bien même elle n'était pas en capacité d'indiquer aux plaignants la source précise.

105. La formation restreinte rappelle que le droit d'accès a pour objectif de permettre à la personne concernée de prendre connaissance du traitement de ses données et d'en vérifier la licéité. L'exercice de ce droit suppose donc que les informations fournies soient les plus précises possibles (CNIL, FR, 30 novembre 2022, Sanction, n°SAN 2022-022).

106. Il résulte de ce qui précède que la société n'a pas renseigné les personnes cibles ayant exercé leur droit d'accès sur la source à partir de laquelle elle avait collecté leurs données, de sorte qu'un manquement à l'article 15 du RGPD est constitué.

II. Sur le prononcé de mesures correctrices et la publicité

107. Aux termes du 2. de l'article 58 du RGPD, " Chaque autorité de contrôle dispose du pouvoir d'adopter toutes les mesures correctrices suivantes: […]

c) ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits en application du présent règlement;

d) ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé; […]

i) imposer une amende administrative en application de l'article 83, en complément ou à la place des mesures visées au présent paragraphe, en fonction des caractéristiques propres à chaque cas ".

108. Le III de l'article 20 de la loi du 6 janvier 1978 modifiée prévoit que : " lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut […] saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […]

2° Une injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'État, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte ; […]

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. "

109. L'article 83 du RGPD dispose en outre que " chaque autorité de contrôle veille à ce que les amendes administratives imposées […] 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.

110. La formation restreinte doit ainsi tenir compte dans la détermination du montant de l'amende de critères tels que le nombre de violations, leur nature et gravité, le nombre de personnes concernées et les avantages financiers obtenus du fait du manquement.

111. La société soutient que son traitement est légitime, que le prononcé d'une amende est privé de fondements en l'absence de manquements effectivement constitués et que le prononcé d'une amende reviendrait à refuser de prendre en compte des mesures de conformité pourtant existantes. La société soutient ensuite que le montant de l'amende est disproportionné par rapport à la gravité des manquements et du comportement de KASPR qui devrait constituer un " facteur atténuant ". Enfin, la société soutient que la proposition d'injonction est dénuée d'objet et que la publicité de la sanction serait contre-productive à l'égard d'une société qui s'est investie dans une démarche de conformité au RGPD.

112. En premier lieu, la formation restreinte rappelle que, si l'imposition d'une amende administrative est conditionnée à l'établissement d'une violation fautive de la part de l'organisme poursuivi, cette faute peut découler d'un comportement délibéré mais également d'une négligence, en application de l'alinéa b) de l'article 83, paragraphe 2 du RGPD (CJUE, Grande Chambre, 5 décembre 2023, Deutsche Wohnen SE e.a., C-807/21 ; CJUE, Grande Chambre, 5 décembre 2023, Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos e.a., C-683/21).

113. La formation restreinte considère qu'en l'espèce, les manquements commis par la société révèlent une négligence certaine de sa part. En effet, la formation restreinte souligne, d'une part, que les règles rappelées dans la présente délibération font l'objet d'une interprétation constante de la part de la CNIL. A titre d'exemple, la formation restreinte s'est déjà prononcée sur le droit d'accès en indiquant que les informations fournies doivent être les plus précises possibles (CNIL, FR, 30 novembre 2022, Sanction, n°SAN 2022-022), mais aussi sur l'obligation de transparence en considérant que l'information des personnes dont les coordonnées sont traitées par un courriel uniquement disponible en anglais ne répond pas à l'exigence de fourniture d'une information transparente posée à l'article 12 du Règlement (CNIL, FR, 29 décembre 2023, Sanction, n°SAN 2023-023). D'autre part, la formation restreinte relève que la multiplicité des manquements témoigne d'une négligence dans la mise en œuvre des traitements réalisés par la société.

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

115. La formation restreinte relève tout d'abord que les manquements aux articles 5-1-e et 6 du RGPD concernent les principes fondamentaux de la protection des données et sont ainsi susceptibles de faire l'objet d'une amende pouvant s'élever jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel de l'exercice précédent de la société – soit le montant maximal prévu par les textes -, en application de l'article 83, paragraphe 5 du RGPD. A cet égard, les lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD adoptées le 24 mai 2023 par le comité européen de la protection des données rappellent qu'à " travers cette distinction, le législateur a donné une première indication de la gravité de la violation, de manière abstraite. Plus la violation est grave, plus l'amende est susceptible d'être élevée " (point 50).

116. La formation restreinte note ensuite, comme elle l'a expliqué au paragraphe 31 de la présente délibération, que les manquements aux articles 5-1-e, 12 et 14 relevés sont susceptibles de concerner un nombre important de personnes, la

base de données de KASPR comprenant près de 160 millions de contacts au jour du contrôle sur audition, dès lors qu'il convient de prendre en compte l'ensemble des contacts présents dans la base de données KASPR, ceux-ci étant des personnes concernées par le RGPD.

117. La formation restreinte souligne en outre que pour les personnes ayant décidé de ne pas afficher leurs coordonnées sur LinkedIn, le traitement présente une atteinte particulièrement forte aux droits des personnes dans la mesure où il va à l'encontre de leur souhait de garder ces données privées afin notamment de les démarcher, comme le corroborent les différentes plaintes reçues par les services de la Commission.

118. Cette incertitude face à l'ampleur de l'atteinte à la confidentialité de leurs données se superpose au dérangement occasionné par ces démarchages intempestifs, dénoncés par les plaignants dans les saisines reçues par la Commission.

119. Enfin, la formation restreinte remarque que l'examen des plaintes met également en évidence la défaillance des procédures d'exercice des droits mises en œuvre au sein de la société, qui ne répond pas précisément aux plaignants souhaitant connaitre la source à partir de laquelle leurs données de contacts ont été obtenues de manière indirecte.

120. En troisième lieu, la formation restreinte entend faire application du critère prévu à l'alinéa k) de l'article 83, paragraphe 2 du RGPD, relatif aux avantages financiers obtenus du fait du manquement.

121. Elle relève, à cet égard, que la société tire tous ses revenus de la facturation à ses clients d'un service dont le fonctionnement repose en partie sur des données collectées illicitement et, jusqu'en 2022, à l'insu des personnes concernées.

122. Ainsi, tout le modèle d'affaires de la société repose sur la violation de dispositions majeures du RGPD, en ce que la base de données à partir de laquelle fonctionne son extension a été constituée pour partie illicitement.

123. En quatrième lieu, la formation restreinte entend tenir compte des mesures prises par la société pour atténuer des manquements, en application de l'alinéa c) de l'article 83, paragraphe 2 du RGPD. Il apparait en effet que, suite à la réception du rapport de sanction, la société a mis en œuvre une nouvelle durée de conservation s'agissant des données des utilisateurs de KASPR, et a déployé, pour le courriel d'information et la politique de confidentialité de la société, la possibilité pour les personnes concernées de choisir la langue du texte en français, espagnol, néerlandais ou allemand.

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

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

126. Elle considère que l'activité de la société et sa situation financière doivent notamment être prises en compte. Elle relève à cet égard que la société KASPR a réalisé, au titre de l'année 2022, un chiffre d'affaires de […] euros pour un bénéfice de […] euros. L'année suivante, ce chiffre d'affaires s'est élevé à […] euros, pour un bénéfice de […] euros.

127. Au regard de la responsabilité de la société, de ses capacités financières et des critères pertinents de l'article 83, paragraphe 2 du RGPD évoqués ci-avant, la formation restreinte estime qu'une amende de deux cent quarante mille (240 000) euros apparaît justifiée.

128. S'agissant du prononcé d'une injonction assortie d'une astreinte, le rapporteur propose dans son rapport à la formation restreinte de prononcer à l'encontre de la société une injonction de mise en conformité, assortie d'une astreinte, au titre des manquements aux articles 5-1-e, 6, 12, 14 et 15 du RGPD.

129. La société considère que les mesures d'injonction proposées par le rapporteur sont dénuées d'objet, dès lors que la société a procédé à la mise en conformité de son traitement au mieux compte tenu de ses ressources.

130. En premier lieu, sur la base juridique, la formation restreinte relève que la société continue de traiter des données qui ont été collectées en l'absence d'une base valable.

131. Par conséquent, la formation restreinte estime nécessaire le prononcé d'une injonction afin que la société se mette en conformité avec les obligations applicables en la matière.

132. En deuxième lieu, sur l'obligation de définir et de respecter une durée de conservation des données proportionnée à la finalité du traitement, la formation restreinte note que la société n'a pas indiqué avoir mis en place une politique de durée de conservation proportionnée s'agissant des personnes cibles.

133. Par conséquent, la formation restreinte estime nécessaire de maintenir l'injonction sur ces points.

134. En troisième lieu, sur le manquement à l'obligation de faire droit aux demandes d'exercice de droit d'accès, la formation restreinte note que les plaignants n'ont toujours pas été informés de la source précise des données les concernant collectées par la société.

135. Par conséquent, la formation restreinte considère que l'injonction est justifiée sur ce point.

136. En dernier lieu, en ce qui concerne les modalités de l'injonction avec astreinte, la formation restreinte relève qu'afin de conserver à l'astreinte sa fonction comminatoire, son montant doit être à la fois proportionné à la gravité des manquements commis et adapté aux capacités financières du responsable de traitement. Elle estime, par ailleurs, que pour la détermination de ce montant il doit également être tenu compte du fait que le manquement concerné par l'injonction participe directement aux bénéfices générés par le responsable de traitement.

137. Au regard de ces éléments, la formation restreinte considère comme justifié le prononcé d'une astreinte d'un montant de 10 000 euros par jour de retard et liquidable à l'issue d'un délai de six mois.

138. S'agissant de la publicité de la sanction, la formation restreinte considère que celle-ci se justifie au regard de la gravité de certains des manquements en cause, de la position de la société sur le marché, de la portée du traitement et du nombre de personnes concernées.

139. Elle relève également que cette mesure a notamment vocation à informer les personnes concernées par les traitements mis en œuvre par la société, qu'il s'agisse des utilisateurs de l'extension ou des personnes cibles. Cette information leur permettra, le cas échéant, de faire valoir leurs droits.

140. Enfin, elle estime que cette mesure est proportionnée dès lors que la décision n'identifiera plus nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

PAR CES MOTIFS

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

• prononcer une amende administrative à l'encontre de la société KASPR d'un montant de deux cent quarante mille (240 000) euros au regard des manquements constitués aux articles 5-1-e), 6, 12, 14 et 15 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ;

• prononcer à l'encontre de la société KASPR, une injonction :

o s'agissant du manquement à l'article 6 du RGPD,

- de cesser de collecter des données des contacts des utilisateurs de KASPR ayant choisi de limiter la visibilité de leurs coordonnées ;

- de supprimer l'ensemble des données de contacts importées lors de la synchronisation des comptes LinkedIn des utilisateurs ayant choisi de limiter la visibilité de leurs coordonnées ou à défaut, en cas d'impossibilité de distinguer ces données dont la visibilité a été limitée des autres données, de les informer, dans un délai de 3 mois, du traitement de leurs données et de la possibilité de s'y s'opposer et de n'utiliser les données que dans ce but ;

o s'agissant du manquement à l'article 5-1-e du RGPD, concernant les personnes cibles, cesser de renouveler automatiquement la durée de conservation de 5 ans des données des personnes cibles dès la mise à jour de leur profil et ne conserver les données que pour une durée proportionnée au traitement ;

o s'agissant du manquement aux articles 12 et 14 du RGPD: d'informer les personnes concernées de l'ensemble des mentions prévues à cet article dans une langue qu'ils maîtrisent ;

o s'agissant du manquement à l'article 15 du RGPD,

- de faire suite aux demandes de droit d'accès des personnes en leur fournissant toute information disponible quant à la source qui a permis le versement de leurs données de contacts dans la base de données de la société ;

- et de faire droit aux demandes de droit d'accès des personnes à l'origine des saisines […] dans les mêmes conditions, avant suppression des données relatives aux saisines […].

• assortir l'injonction d'une astreinte de dix mille euros (10 000 €) par jour de retard à l'issue d'un délai de six mois suivant la notification de la présente délibération, les justificatifs de la mise en conformité devant être adressés à la formation restreinte dans ce délai ;

• rendre publique, sur le site web de la CNIL et sur le site web de Légifrance, sa délibération, qui ne permettra plus d'identifier nommément la société à l'issue d'une durée de deux ans à compter de sa publication.

Le président

Philippe-Pierre CABOURDIN

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