Délibération SAN-2022-018 du 8 septembre 2022

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Etat juridique : En vigueur

Date de publication sur Légifrance : Mardi 13 septembre 2022

Délibération de la formation restreinte n° SAN-2022-018 du 8 septembre 2022 concernant XX

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

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

Vu la 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 n° 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° 2021-032C du 6 janvier 2021 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 de tout traitement accessible à partir du site […] ou portant sur des données à caractère personnel collectées à partir de ce dernier ;

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 21 octobre 2021 ;

Vu le rapport de Monsieur François PELLEGRINI, commissaire rapporteur, notifié […] le 16 février 2022 ;

Vu les observations écrites versées par […] le 15 avril 2022 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 12 mai 2022 :

- Monsieur François PELLEGRINI, commissaire, entendu en son rapport ;

En qualité de représentants […] :

- […] ;

- […] ;

- […].

[…] ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. […] (ci-après l'organisme ou le groupement), dont le siège social est situé […], est un groupement d'intérêt économique (GIE) […] qui édite depuis 1986 le service de diffusion de l'information légale et officielle sur les entreprises à travers plusieurs canaux, notamment le site web […] depuis 1996.

2. Le site web […] permet de consulter des informations légales sur les entreprises et de commander des documents […]. Les utilisateurs souhaitant visualiser ou commander un acte payant sur le site web doivent obligatoirement disposer d'un compte et sont désignés par […] comme étant des membres . Il est également possible pour les utilisateurs de souscrire un abonnement annuel, permettant notamment aux abonnés d'accéder à certains services dans la rubrique de consultations d'affaires. Lors de la création d'un compte, membre ou abonné, l'utilisateur doit renseigner les champs obligatoires suivants : nom, prénom, adresses postale et électronique, téléphone fixe ou portable et choix d'une question secrète et de sa réponse. Les données bancaires des abonnés (IBAN et BIC) sont également traitées par […].

3. Pour l'année 2019, l'organisme a réalisé un chiffre d'affaires de […] euros, pour un résultat net de […] euros. En 2020, il a réalisé un chiffre d'affaires de […] euros, pour un résultat net de […] euros.

4. Le 12 décembre 2020, la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission) a été saisie d'une plainte à l'encontre de l'organisme, d'une personne indiquant que le site web […] conserve les mots de passe des utilisateurs en clair et qu'elle a été capable d'obtenir son mot de passe par téléphone en donnant simplement son nom à l'interlocutrice du service d'assistance téléphonique.

5. En application de la décision n° 2021-032C du 6 janvier 2021 de la présidente de la CNIL, une mission de contrôle a été réalisée afin de vérifier la conformité de tout traitement accessible à partir du domaine […], ou portant sur des données à caractère personnel collectées à partir de ce dernier, aux dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après la loi du 6 janvier 1978 modifiée ou la loi Informatique et Libertés) et au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le Règlement ou le RGPD).

6. Ainsi, un contrôle en ligne a été effectué le 4 mars 2021 sur le site […] mis en œuvre par le groupement. Le procès-verbal n° 2021-032/1 dressé à l'issue du contrôle a été notifié à l'organisme par courrier recommandé, réceptionné le 10 mars 2021.

7. La délégation de la CNIL s'est notamment attachée à vérifier la procédure de transmission des mots de passe des utilisateurs lors de la création d'un compte ou en cas d'oubli ou de perte du mot de passe.

8. Par courriers des 19 mars, 25 mai et 24 juin 2021, l'organisme a transmis à la CNIL les éléments sollicités par le procès-verbal n° 2021-032/1 et a répondu à ses demandes de complément d'informations adressées par courriels les 17 mai et 18 juin 2021. L'organisme y confirme notamment qu'il détermine les finalités et les modalités de mise en œuvre des traitements de données à caractère personnel du site […] . Il précise également les durées de conservation des données qu'il collecte et les mesures prises afin d'assurer leur sécurité. […] a également indiqué à la délégation qu'au cours de l'année 2020, le site a été consulté par plus de 24 millions de personnes dans le monde et que, sur les 3,7 millions de personnes disposant d'un compte, plus de 8 000 comptes européens n'étaient pas français.

9. 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 cheffe de file concernant les traitements transfrontaliers mis en œuvre par […], résultant de ce que l'établissement unique du groupement se trouve en France. Après échange entre la CNIL et les autorités de protection des données européennes dans le cadre du mécanisme de guichet unique, celles-ci sont toutes concernées par le traitement puisque des comptes utilisateurs ont été créés par les résidents de tous les États membres de l'Union européenne.

10. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 21 octobre 2021, désigné Monsieur François PELLEGRINI en qualité de rapporteur sur le fondement de l'article 22 de la loi du 6 janvier 1978 modifiée, et en a informé l'organisme par courrier daté du 26 octobre 2021.

11. Le 2 décembre 2021, le rapporteur demandait à l'organisme de fournir ses trois derniers bilans comptables, ce que l'organisme a fait par courrier daté du 15 décembre 2021.

12. À l'issue de son instruction, le rapporteur a, le 16 février 2022, fait notifier à l'organisme un rapport détaillant les manquements au RGPD qu'il estimait constitués en l'espèce, accompagné d'une convocation à la séance de la formation restreinte du 21 avril 2022. Le courrier de notification du rapport indiquait à l'organisme qu'il disposait d'un délai d'un mois pour communiquer ses observations écrites en réponse, conformément à l'article 40 du décret n° 2019-536 du 29 mai 2019 modifié.

13. Ce rapport proposait à la formation restreinte de la Commission de prononcer une amende administrative au regard des manquements aux articles 5, paragraphe 1, e) et 32 du RGPD. Il proposait également que cette décision soit rendue

publique, mais qu'il ne soit plus possible d'identifier nommément l'organisme à l'expiration d'un délai de deux ans à compter de sa publication.

14. Le 22 février 2022, l'organisme a sollicité une extension du délai d'un mois pour produire des observations en réponse au rapport de sanction. Le 25 février 2022, le président de la formation restreinte a fait droit à cette demande et reporté la séance de la formation restreinte.

15. Le 15 avril 2022, l'organisme a produit ses observations en réponse au rapport de sanction et sollicité le huis clos de la séance de la formation restreinte. Cette demande a été rejetée par le président de la formation restreinte, l'organisme en étant avisé par courrier daté du 21 avril 2022.

16. L'organisme et le rapporteur ont présenté des observations orales lors de la séance de la formation restreinte.

II. Motifs de la décision

17. En application de l'article 60, paragraphe 3, du RGPD, le projet de décision adopté par la formation restreinte a été transmis à l'ensemble des autorités de protection des données européennes le 19 juillet 2022.

18. Au 16 août 2022, aucune autorité de contrôle 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 à l'obligation de conserver les données pour une durée proportionnée à la finalité du traitement en application de l'article 5, paragraphe 1, e) du RGPD

19. 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.

20. Dans le cadre du contrôle, la délégation a constaté que la Charte de confidentialité du site web […] prévoit que les données à caractère personnel des membres et des abonnés sont conservées 36 mois à compter de la dernière commande de prestation et/ou documents.

21. Toutefois, l'organisme a fourni à la délégation de la CNIL un fichier de tableur dont il ressort qu'au 1er mai 2021, il conservait les données à caractère personnel de 946 023 membres et de 17 558 abonnées dont la dernière commande, la dernière formalité ou encore la dernière facture pour les abonnés, date de plus de 36 mois, sans que l'organisme soit en mesure de justifier d'un contact récent avec lesdits membres ou abonnés.

22. Le rapporteur relève qu'aucune procédure de suppression automatique des données à caractère personnel n'a été mise en place par l'organisme et que les données étaient conservées pour des durées excessives par rapport à leur finalité et la propre politique fixée par l'organisme.

23. En défense, l'organisme admet que des données à caractère personnel ont été conservées plus longtemps que la durée indiquée au sein de sa Charte mais conteste le fait que la durée indiquée dans cette Charte soit prise comme seule référence alors qu'au regard d'autres finalités, comme par exemple celle relative aux opérations de recouvrement, il serait justifié que certaines données soient conservées pour une durée supérieure à 36 mois. S'agissant de l'anonymisation des données à caractère personnel, l'organisme admet que 25% des comptes ont été conservés au-delà de 36 mois après la dernière commande, formalité ou facture, sans être anonymisés. Il admet également le retard pris dans l'automatisation de l'anonymisation mais conteste le fait qu'il n'y ait eu aucune anonymisation des comptes.

24. En premier lieu, la formation restreinte relève que la finalité relative aux opérations de recouvrement, citée par l'organisme, et la durée de conservation afférente ne pourraient a priori concerner que les données des abonnés et non des membres, ces derniers payant immédiatement en échange de la réception d'un acte. En outre, la formation restreinte relève que, pour cette finalité comme pour les finalités comptables et fiscales, l'organisme n'avait pas identifié ces finalités et les durées correspondantes dans sa Charte de confidentialité à la date du contrôle. En tout état de cause, la formation restreinte relève que si la conservation de certaines données pour ces finalités peut apparaître justifiée, elle requiert que différentes actions soient réalisées. Ainsi, la formation restreinte rappelle qu'une fois la finalité du traitement atteinte, la conservation de certaines données pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses est possible, mais les données doivent être alors placées en archivage intermédiaire, pour une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont conservées, conformément aux dispositions en vigueur. Seules les données pertinentes doivent être placées en archivage intermédiaire, soit dans une base de données d'archive dédiée, soit en effectuant une séparation logique au sein de la base active, permettant que seules les personnes habilitées puissent y accéder. La formation restreinte relève qu'au jour du contrôle, aucune de ces actions n'était mise en œuvre par l'organisme.

25. En second lieu, la formation restreinte relève que l'anonymisation manuelle mise en œuvre par l'organisme sur demande des utilisateurs ne concernait qu'une très faible quantité de compte puisqu'au jour du contrôle en ligne, 25% des comptes n'étaient pas anonymisés alors qu'ils auraient dû l'être. La formation restreinte relève qu'aucune procédure d'anonymisation automatique n'était mise en œuvre au jour du contrôle en ligne, l'organisme conservant ainsi des données identifiantes sans limitation de durée en l'absence de demande d'anonymisation de la part des utilisateurs.

26. Dès lors, la formation restreinte considère que les faits précités constituent un manquement structurel à l'article 5, paragraphe 1, e) du RGPD.

27. La formation restreinte relève que l'organisme a indiqué, au cours de la procédure, qu'une purge des comptes inactifs depuis plus de 36 mois était mise en œuvre depuis le contrôle, mais retient que le manquement reste caractérisé pour le passé.

B. Sur les manquements à l'obligation d'assurer la sécurité des données à caractère personnel (article 32 RGPD).

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

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

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

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

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

29. Le rapporteur relève, en premier lieu, que la délégation a constaté que les mots de passe de connexion des utilisateurs à leurs comptes, accessibles depuis le site web de l'organisme, sont d'une robustesse insuffisante en ce qu'ils sont limités à huit caractères, sans aucun critère de complexité, et ne sont associés à aucune mesure de sécurité complémentaire. En outre, le rapporteur relève qu'au jour des constats, il était impossible pour l'ensemble des utilisateurs ou des abonnés du site web […] , soit pour plus de 3,7 millions de comptes, de saisir un mot de passe sécurisé en raison de la limitation de leur taille à 8 caractères maximum.

30. Le rapporteur relève, en deuxième lieu, que l'organisme transmet en clair par courriel des mots de passe non temporaires permettant l'accès aux comptes.

31. Le rapporteur souligne, en troisième lieu, que l'organisme conserve également en clair dans sa base de données, les mots de passe ainsi que les questions et réponses secrètes utilisés lors de la procédure de réinitialisation des mots de passe par les utilisateurs.

32. En dernier lieu, le rapporteur relève que l'organisme ne confirme pas non plus à l'utilisateur la modification de son mot de passe. Le rapporteur considère que l'utilisateur qui n'est pas alerté en cas de modification non autorisée, n'est donc à ce titre pas protégé contre les tentatives d'usurpation de son compte.

33. Au regard de ces éléments, le rapporteur considère que les différentes mesures de sécurité mises en place par l'organisme sont insuffisantes au regard de l'article 32 du RGPD.

34. En défense, l'organisme fait valoir que l'obligation de sécurité est une obligation de moyens qui doit être appréciée in concreto et que son inexécution doit être constatée par un constat de l'inefficacité des mesures mises en œuvre, ayant conduit à un accès non autorisé, ce qui n'est pas le cas en l'espèce. Il souligne que la recommandation relative aux mots de passe évoquée par le rapporteur constitue du droit souple, qu'il ne s'agit pas de règles impératives, applicables in abstracto, indépendamment de tout contexte et dont le non-respect serait, en lui-même, de nature à justifier une sanction administrative. En outre, l'organisme précise que l'analyse d'impact relative à la protection des données a révélé un risque faible pour les données à caractère personnel en cas d'accès non autorisé puisque pour les comptes membres, représentant la majorité des comptes, les données bancaires ne sont pas enregistrées, contrairement aux comptes abonnés et qu'un tiers non autorisé ne pourra effectuer d'autres démarches que l'achat de documents et l'envoi de formalités à la place du titulaire du compte. Enfin, l'organisme souligne que les informations accessibles en se connectant sur le compte d'un utilisateur sont pour l'essentiel des données à caractère personnel présentes dans les extraits K ou KBIS

et les autres actes pouvant être commandés, sauf pour les comptes créés par des non-professionnels dont les données d'identification et de localisation ne sont pas publiques.

35. Tout d'abord, la formation restreinte rappelle que, 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 . La formation restreinte considère que l'utilisation d'un mot de passe court ou simple sans imposer de catégories spécifiques de caractères et sans mesure de sécurité complémentaire, peut 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. 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. En l'espèce, la formation restreinte relève que les mots de passe en cause sont limités à huit caractères sans aucun critère de complexité, et ne sont associés à aucune mesure de sécurité complémentaire. La formation restreinte considère que le risque encouru par les personnes concernées est réel : un tiers ayant eu accès au mot de passe pourrait non seulement accéder à toutes les données à caractère personnel présentes dans le compte de la personne concernée, mais également consulter l'historique de ses commandes, télécharger ses factures et/ou changer le mot de passe du compte et les informations de contact à l'insu de l'utilisateur.

36. En outre, la formation restreinte considère que les modalités de transmission et de conservation des mots de passe mises en œuvre par l'organisme ne sont pas adaptées au regard du risque que ferait peser sur la personne concernée la captation de leur identifiant et de leur mot de passe par un tiers. En effet, la transmission, en clair, d'un mot de passe qui n'est ni temporaire, ni à usage unique et dont le renouvellement n'est pas imposé, le rend aisément et immédiatement utilisable par un tiers qui aurait un accès indu au message qui le contient. La formation restreinte rappelle qu'une simple erreur de manipulation peut conduire à divulguer à des destinataires non habilités des données personnelles et à porter ainsi atteinte au droit à la vie privée des personnes. Enfin, la formation restreinte considère que l'utilisateur qui n'est pas alerté en cas de modification non autorisée n'est donc pas protégé contre les tentatives d'usurpation de son compte.

37. 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.

38. Ensuite, la formation restreinte précise que si la délibération n° 2017-012 du 19 janvier 2017, le guide de la CNIL relatif à la sécurité des données à caractère personnel et la note technique de l'ANSSI relative aux mots de passe cités dans les écrits du rapporteur n'ont certes pas de caractère impératif, ils exposent toutefois les précautions élémentaires de sécurité correspondant à l'état de l'art. Dès lors, la formation restreinte rappelle qu'elle retient un manquement aux obligations découlant de l'article 32 du RGPD et non du non-respect des recommandations, qui constituent au demeurant un éclairage pertinent pour évaluer les risques et l'état de l'art en matière de sécurité des données à caractère personnel.

39. Outre ces recommandations, 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 traités, et non pas seulement le résultat de l'existence d'une violation de données à caractère personnel. Les délibérations n° SAN-2019-006 du 13 juin 2019 et n° SAN-2019-007 du 18 juillet 2019 visent notamment l'insuffisante robustesse des mots de passe ainsi que leur transmission aux clients de l'organisme par courriel, en clair, après la création du compte.

40. Dans ces conditions, eu égard aux risques encourus par les personnes, rappelés ci-dessus, ainsi qu'au volume et à la nature des données à caractère personnel qui peuvent être contenues dans plus de 3,7 millions de comptes (données bancaires des comptes abonnés, nom, prénom, adresse postale et électronique, numéros de téléphone fixe ou portable, question secrète et sa réponse de l'ensemble des comptes), la formation restreinte considère que l'organisme a manqué aux obligations qui lui incombent en vertu de l'article 32 du RGPD.

41. La formation restreinte relève que dans le cadre de la présente procédure l'organisme a pris certaines mesures pour assurer la sécurité des données traitées. Néanmoins, elle considère que, depuis la mise en œuvre de sa politique de mots de passe en 2002 et jusqu'au mois de juin 2021, les mesures de sécurité mises en place par l'organisme ne lui permettaient pas d'assurer un niveau de sécurité suffisant des données à caractère personnel traitées et que, partant, un manquement aux obligations de l'article 32 du Règlement est constitué.

III. Sur les mesures correctrices et leur publicité

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

Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés

peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […] 7° À l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83.

43. 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.

44. En premier lieu, sur le principe du prononcé d'une amende, l'organisme insiste en défense sur la responsabilité contractuelle de son sous-traitant au regard des instructions qui lui avaient été données concernant la sécurité et l'anonymisation des données à caractère personnel, sur la priorisation d'autres chantiers légaux et règlementaires par rapport à sa mise en conformité au RGPD, sur son importante coopération avec la CNIL et les importants efforts engagés depuis le début du contrôle.

45. La formation restreinte rappelle 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, le nombre de personnes affectées, les mesures prises par le responsable du traitement pour atténuer le dommage subi par les personnes concernées, le fait que la violation a été commise par négligence, le degré de coopération avec l'autorité de contrôle et les catégories de données à caractère personnel concernées par la violation.

46. La formation restreinte considère d'abord que bien que l'organisme ait donné des instructions spécifiques en matière d'anonymisation et de sécurité à son sous-traitant, il apparaît qu'il n'a pas suivi l'exécution de ces instructions et n'a pas exercé un contrôle satisfaisant et régulier sur les mesures techniques et organisationnelles mise en œuvre par son sous-traitant pour assurer la conformité au RGPD et, notamment pour assurer l'anonymisation et la sécurité des données à caractère personnel traitées.

47. La formation restreinte considère par ailleurs qu'il convient de prendre en compte la nature de l'acteur concerné […]. À ce titre, la formation restreinte considère que l'organisme aurait dû, dès lors, faire preuve d'une particulière rigueur dans le respect de l'ensemble de ses obligations légales et réglementaires. Or, il résulte des débats que l'organisme a reporté la mise en œuvre des chantiers relatifs à l'anonymisation et à la sécurité des données à caractère personnel afin de répondre, sans accroître ses moyens disponibles, à d'autres obligations de mise en conformité qui n'étaient pas liées à la protection des données.

48. La formation restreinte relève ensuite que les manquements reprochés sont des manquements à des principes clés du RGPD qui n'ont pas été introduits par ce texte mais préexistaient dans la loi Informatique et Libertés . La formation restreinte souligne en outre que ces manquements ne sauraient être regardés comme un incident isolé. S'agissant du manquement relatif à la durée de conservation, la formation restreinte rappelle que l'organisme avait lui-même fixé une durée de conservation des données à caractère personnel qu'il n'a pas respectée et que ce manquement concerne plus d'un million de comptes utilisateurs, membres et abonnés. S'agissant du manquement relatif à la sécurité des données, la formation restreinte considère que la faiblesse extrême des règles de complexité des mots de passe, ainsi que les mesures de sécurité en matière de communication, conservation et renouvellement des mots de passe, en vigueur depuis 2002, rendaient l'ensemble des comptes vulnérables.

49. Enfin, la formation restreinte relève que les mesures de conformité mises en place à la suite de la notification du rapport de sanction n'exonèrent par l'organisme de sa responsabilité pour les manquements constatés.

50. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative au regard des manquements constitués aux article 5, paragraphe 1, e) et 32 du RGPD.

51. En deuxième lieu, s'agissant du montant de l'amende, l'organisme insiste en défense sur le caractère isolé de la plainte à l'origine du contrôle et l'absence de gain financier tiré des manquements.

52. La formation restreinte rappelle que les amendes administratives doivent être à la fois dissuasives et proportionnées. Elle considère que l'origine du contrôle, intervenu à la suite d'une seule plainte, ne saurait minimiser la gravité des manquements qui au demeurant se sont révélés structurels. En l'espèce, la formation restreinte constate, s'agissant du manquement relatif à la durée de conservation des données à caractère personnel, que l'organisme a fait preuve de négligence grave portant sur un principe fondamental du RGPD et que ce manquement concerne plus de 25% des comptes. S'agissant du manquement relatif à la sécurité, la formation restreinte relève que compte tenu de l'accumulation

des défauts de sécurité, les faits constatés sont d'une particulière gravité, d'autant plus qu'ils ont rendu l'ensemble des comptes vulnérables. La formation restreinte rappelle ensuite que l'organisme a repoussé sa mise en conformité au RGPD au profit d'autres priorités légales et règlementaires. Enfin, la formation restreinte tient compte de l'activité de l'organisme et de sa situation financière. Elle acte par ailleurs des efforts réalisés par l'organisme pour se mettre en conformité tout au long de la présente procédure.

53. Au vu de ces éléments, la formation restreinte considère que le prononcé d'une amende administrative de deux-cent-cinquante-mille euros apparaît justifié.

54. En dernier lieu, s'agissant de la publicité de la sanction, l'organisme soutient qu'une telle mesure serait disproportionnée au regard de l'atteinte que cela lui causerait.

55. La formation restreinte considère que la publicité de la sanction se justifie au regard de la gravité des manquements relevés, de la nature de l'acteur concerné qui, compte tenu de sa taille et de son activité, dispose des ressources humaines, financières et techniques devant lui permettre d'assurer un niveau satisfaisant de protection des données à caractère personnel et la forte réputation dont bénéficie le site web en matière de données commerciales.

PAR CES MOTIFS

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

• prononcer à l'encontre […] une amende administrative d'un montant de 250 000 (deux-cent-cinquante-mille) euros pour les manquements aux articles 5, paragraphe 1, e) et 32 du RGPD ;

• rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération, qui n'identifiera plus nommément l'organisme 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.