Délibération SAN–2026-003 du 22 janvier 2026

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Date de publication sur Légifrance : Jeudi 29 janvier 2026
Etat juridique : En vigueur

Délibération de la formation restreinte n° SAN–2026-003 du 22 janvier 2026 prononçant une sanction pécuniaire à l'encontre de l'opérateur FRANCE TRAVAIL

Les développements de la délibération comportant des données à caractère personnel ou des secrets protégés par la loi sont remplacés par le signe […]

****

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Philippe-Pierre CABOURDIN, président, Mmes Laurence FRANCESCHINI et Isabelle LATOURNARIE-WILLEMS, MM. Didier KLING et 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 personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

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

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

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

Vu la décision n° 2025-1154 QPC du 8 août 2025 du Conseil constitutionnel ;

Vu la décision n° 2024-051C du 13 mars 2024 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 ;

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 du 3 juillet 2025 ;

Vu le rapport de M. Fabien TARISSAN, commissaire rapporteur, notifié à FRANCE TRAVAIL le 24 juillet 2025 ;

Vu les observations écrites de FRANCE TRAVAIL reçues le 22 septembre 2025 ;

Vu la réponse du rapporteur notifiée à la FRANCE TRAVAIL le 22 octobre 2025 ;

Vu les observations écrites de FRANCE TRAVAIL reçues le 21 novembre 2025 ;

Vu la clôture de l'instruction notifiée à FRANCE TRAVAIL le 2 décembre 2025 ;

Vu la demande de huis-clos formulée le 11 décembre 2025 et refusée le 12 décembre 2025 ;

Vu les observations orales formulées lors de la séance de la formation restreinte du 18 décembre 2025 ;

Vu les autres pièces du dossier,

Étaient présents, lors de la séance de la formation restreinte :

- M. Fabien TARISSAN, commissaire, entendu en son rapport ;

En qualité de représentants de FRANCE TRAVAIL :

- […]

En qualité de commissaire du Gouvernement :

- Monsieur Damien MILIC.

L'opérateur FRANCE TRAVAIL ayant été informé de son droit de garder le silence sur les faits qui lui étaient reprochés et ayant eu la parole en dernier ;

Après en avoir délibéré, a adopté la décision suivante :

I. Faits et procédure

A. Présentation de l'opérateur FRANCE TRAVAIL et du traitement mis en œuvre

1. L'opérateur FRANCE TRAVAIL (ci-après, "l'opérateur" ou "l'organisme") sis Le Cinetic 1-5, 1 avenue du Docteur Gley à Paris (75020), est un établissement public administratif placé sous la tutelle du Ministère chargé de l'emploi. FRANCE TRAVAIL est doté de l'autonomie financière.

2. Les missions de FRANCE TRAVAIL sont définies à l'article L. 5312-1 du code du travail. L'opérateur assure notamment des missions d'indemnisation et d'accompagnement des demandeurs vers le retour à l'emploi, ainsi que de conseil aux entreprises dans leurs recrutements. L'opérateur a également pour mission de proposer un accompagnement adapté aux besoins des personnes ayant fait l'objet d'une décision de reconnaissance de la qualité de travailleur handicapé et bénéficiaires de l'obligation d'emploi.

3. FRANCE TRAVAIL assure cette dernière mission en lien avec les CAP EMPLOI, qui sont des organismes de placement spécialisés mentionnés à l'article L. 5214-3-1 du code du travail. Il existe 98 structures CAP EMPLOI en France, qui sont représentées auprès des pouvoirs publics, des décideurs économiques et des partenaires sociaux par le Conseil national handicap et emploi des organismes de placement spécialisés (CHEOPS). Les structures CAP EMPLOI sont autonomes et généralement créées sous forme associative, indépendantes de FRANCE TRAVAIL. Elles accompagnent environ 20 % des personnes en situation de handicap inscrites auprès de FRANCE TRAVAIL.

4. Depuis 2018, afin de pallier le morcellement de l'accompagnement, une offre de services unifiée permet aux demandeurs d'emploi ayant fait l'objet d'une décision de reconnaissance de la qualité de travailleur handicapé et bénéficiaires de l'obligation d'emploi d'être accompagnés au sein des agences de FRANCE TRAVAIL, que leur conseiller référent soit un conseiller FRANCE TRAVAIL ou un conseiller CAP EMPLOI.

5. Afin de permettre cette offre de service intégrée, un " traitement de données de santé nécessaires à l'accompagnement adapté des demandeurs d'emploi en situation de handicap " a été créé par le décret n° 2022-1161 du 16 août 2022 (articles D. 5312-50 à D. 5312-54 du code du travail). Ce décret autorise l'intégration de l'accompagnement par CAP EMPLOI au système d'information de FRANCE TRAVAIL. La Commission nationale de l'informatique et des libertés (ci-après " la CNIL " ou " la Commission ") a rendu un avis sur ce traitement dans sa délibération n° 2022-050 du 21 avril 2022 (non publique).

6. Le traitement autorise à ce titre l'intégration au système d'information préexistant de FRANCE TRAVAIL (article R. 5312-38 du code du travail) de données permettant à l'opérateur FRANCE TRAVAIL et aux organismes CAP EMPLOI d'assurer les missions listées à l'article D. 5312-50 du même code. L'article D. 5312-51 du code du travail prévoit une co-responsabilité de traitement entre l'opérateur FRANCE TRAVAIL et les organismes de placement spécialisés (représentés par le CHEOPS).

7. Les données traitées dans ce cadre et enregistrées dans le système d'information de FRANCE TRAVAIL concernent : le type de handicap, l'origine du handicap, le besoin lié à la compensation du handicap, le besoin lié au rétablissement de la personne, les limitations de capacités et le titre justifiant du bénéfice de l'obligation d'emploi (article D. 5312-51 du code du travail).

8. Elles sont ensuite intégrées à l'application métier de FRANCE TRAVAIL nommée […]. Les utilisateurs habilités des CAP EMPLOI peuvent se connecter à cet outil, […] depuis un navigateur web. Environ 2 300 salariés des structures CAP EMPLOI disposent d'un tel accès.

9. L'outil […] dispose d'une fonctionnalité […] qui permet de réaliser une recherche, selon différents critères, parmi l'ensemble des personnes présentes dans la base de données de FRANCE TRAVAIL […]. La recherche peut être effectuée au

sein de la région de l'agent connecté, mais également d'autres régions sans limitation géographique.

B. La notification de violation de données à caractère personnel

10. Le jeudi 29 février 2024, une activité anormale a été détectée sur le système de mesure de performances du système d'information de FRANCE TRAVAIL, entraînant une indisponibilité partielle du service et une forte consommation en ressources. L'alerte a été constatée et prise en compte le lundi 4 mars 2024 en fin de journée, puis a donné lieu à des investigations le mardi 5 mars 2024.

11. Les investigations menées par FRANCE TRAVAIL ont permis d'établir une intrusion sur son système d'information. L'attaque, qui s'est étendue du mardi 6 février au mardi 5 mars 2024, a ciblé spécifiquement des comptes de salariés CAP EMPLOI.

12. L'attaque a été menée par des techniques dites " d'ingénierie sociale ", c'est-à-dire selon des techniques consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes (définition de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)). En effet, après avoir réussi à récupérer les données nécessaires à la réinitialisation du mot de passe d'un compte de conseiller CAP EMPLOI, les attaquants ont fait une demande de réinitialisation auprès du prestataire du support informatique en se faisant passer pour des employés CAP EMPLOI et ont ainsi pu usurper les comptes. Les attaquants ont ensuite contacté les conseillers CAP EMPLOI dont ils avaient usurpé le compte en se faisant passer pour le support informatique afin de leur communiquer leur nouveau mot de passe. […].

13. Les investigations menées ont révélé que les attaquants ont accédé aux données de […] (nom d'usage, nom de naissance, prénom, sexe, date de naissance, NIR, adresse, code postal, numéro de téléphone, adresse électronique, adresse géographique (région d'appartenance), référence individuelle, statut de demandeur d'emploi (inscrit, radié ou identifié), date de début et de fin d'inscription) […].

14. FRANCE TRAVAIL a précisé que les attaquants ont exfiltré de cette manière 25 giga octets (Go) de données concernant 36 820 828 personnes vers des plateformes d'hébergement externes. Cela correspond aux données non seulement des personnes inscrites auprès de FRANCE TRAVAIL au cours des 20 dernières années, mais également de celles non inscrites sur la liste des demandeurs d'emploi mais possédant un espace candidat sur le site web " francetravail.fr ", qui permet par exemple de consulter les offres d'emploi.

15. Le 8 mars 2024, FRANCE TRAVAIL a procédé à une notification de violation de données auprès de la CNIL, complétée le 15 mai 2024.

16. En application de la décision n° 2024-051C du 13 mars 2024 de la présidente de la Commission, une délégation de la CNIL a effectué une mission de contrôle sur place de l'opérateur FRANCE TRAVAIL afin de vérifier le respect des 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 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 sur la protection des données (ci-après " le RGPD " ou " le Règlement ").

17. Ce contrôle sur place a donné lieu à un procès-verbal n° 2024-051/1 du 21 mars 2024.

18. Les 2 avril et 15 mai 2024, FRANCE TRAVAIL a fourni des éléments complémentaires sollicités par la délégation lors du contrôle sur place et durant les investigations.

19. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 3 juillet 2025, désigné M. Fabien TARISSAN en qualité de rapporteur sur le fondement de l'article 22 de la loi du 6 janvier 1978 modifiée.

20. Le 24 juillet 2025, à l'issue de son instruction, le rapporteur a fait notifier à l'organisme un rapport aux termes duquel il estimait que FRANCE TRAVAIL avait commis un manquement à l'article 32 du RGPD et proposait à la formation restreinte de prononcer à son encontre une amende administrative, ainsi qu'une injonction de mettre ses traitements en conformité avec les dispositions susvisées, assortie d'une astreinte. 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.

21. Le 22 septembre 2025, FRANCE TRAVAIL a produit des observations en réponse au rapport.

22. Le 22 octobre 2025, la réponse du rapporteur a été notifiée à FRANCE TRAVAIL.

23. Le 21 novembre 2025, FRANCE TRAVAIL a adressé de nouvelles observations en réponse.

24. Par courrier du 2 décembre 2025, le rapporteur a, en application de l'article 40, III, du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi Informatique et Libertés, informé l'organisme que l'instruction était close.

25. Par courrier du 2 décembre 2025, l'opérateur FRANCE TRAVAIL a été informé que le dossier était inscrit à l'ordre du jour de la séance de la formation restreinte du 18 décembre 2025.

26. Le 12 décembre 2025, le président de la formation restreinte a refusé la demande de huis-clos formée par FRANCE TRAVAIL dans son courrier du 11 décembre 2025. Il a rappelé que la procédure devant la formation restreinte étant écrite et que si l'organisme ne souhaitait pas dévoiler devant des tiers des éléments susceptibles de lui porter préjudice, elle pouvait, lors de la séance, renvoyer à ses observations écrites. Il a également ajouté que les risques d'atteintes à l'intégrité du système d'information et aux agents de FRANCE TRAVAIL n'étaient pas étayées en l'état.

27. Le 18 décembre 2025, le rapporteur et l'organisme ont présenté des observations orales lors de la séance de la formation restreinte.

II. Motifs de la décision

A. Sur la responsabilité de FRANCE TRAVAIL vis-à-vis du traitement en cause

28. Aux termes de l'article 4, alinéa 7 du RGPD, le responsable de traitement est " la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ".

29. L'article 26 du RGPD dispose que " lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement […] ".

30. Les lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, adoptées par le CEPD le 7 juillet 2021 indiquent que " l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente des différents opérateurs concernés par un traitement de données à caractère personnel. Au contraire, la CJUE a précisé que ces opérateurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce ".

31. Le rapporteur considère que FRANCE TRAVAIL est responsable de la mise en œuvre des mesures techniques et organisationnelles appropriées pour son système d'information, y compris lorsque celui-ci est mis à disposition de ses co-responsables de traitement les CAP EMPLOI (représentés par le CHEOPS). Il estime que les CAP EMPLOI ont pour leur part la responsabilité de respecter les règles imposées par FRANCE TRAVAIL pour l'accès à ce système d'information.

32. FRANCE TRAVAIL conteste avoir la responsabilité exclusive de la mise en œuvre de ces mesures techniques et organisationnelles et soutient que les CAP EMPLOI jouent nécessairement un rôle en leur qualité de co-responsables du traitement. L'opérateur ajoute que le périmètre de la responsabilité conjointe a clairement été défini dans les différents documents contractuels, dont il ressort que les CAP EMPLOI ont été chargés des mesures qui se trouvent dans leur environnement et qui leur permettent d'accéder au système d'information de FRANCE TRAVAIL.

33. À titre liminaire, la formation restreinte relève que la co-responsabilité de traitement entre l'opérateur FRANCE TRAVAIL et les organismes de placement spécialisés (CAP EMPLOI) est prévue par l'article D. 5312-51 du code du travail.

34. Elle relève également que tant les lignes directrices 07/2020 précitées, que la Cour de justice de l'Union européenne (ci-après la " CJUE "), ont estimé qu'une co-responsabilité ne se traduit pas nécessairement par une responsabilité équivalente. Le niveau de responsabilité de chacune des parties doit être évalué en tenant compte des circonstances pertinentes du cas d'espèce (CJUE, 7 mars 2024, " IAB Europe c. Gegevensbeschermingsautoriteit ", C-604/22, point 58).

35. En l'espèce, la formation restreinte rappelle que le traitement en cause est un traitement préexistant de FRANCE TRAVAIL, auquel le décret n° 2022-1161 du 16 août 2022 a autorisé l'intégration de données pour l'accompagnement des demandeurs d'emploi bénéficiaires de l'obligation d'emploi. Pour pouvoir assurer cet accompagnement, les conseillers CAP EMPLOI se connectent à distance, […], à l'applicatif métier […] du système d'information de FRANCE TRAVAIL.

36. La formation restreinte relève que les CAP EMPLOI signent une demande d'adhésion permettant de formaliser, en complément de la convention de responsabilité conjointe de traitement, les conditions de cet accès. Par cette adhésion, les CAP EMPLOI manifestent " leur accord sur les caractéristiques du système d'information commun " et s'engagent à respecter, diffuser et appliquer les consignes communiquées par FRANCE TRAVAIL relatives à la protection des données à caractère personnel et à la sécurité de son système d'information.

37. En plus de ces engagements, les CAP EMPLOI offrent à FRANCE TRAVAIL un appui dans le contrôle du respect de ces règles, notamment en " facilitant la réalisation des audits de sécurité des postes de travail des Cap emploi et en informant Pôle emploi [FRANCE TRAVAIL] des difficultés rencontrées par les Cap emploi ".

38. Ensuite, la formation restreinte observe que FRANCE TRAVAIL s'engage à " mettre en œuvre les mesures de sécurité technique pour les outils mis à disposition des salariés Cap emploi " et s'assure du bon respect des règles liées aux habilitations, à la minimisation, et à la conformité au droit de la protection des données à caractère personnel. De manière plus générale, FRANCE TRAVAIL s'assure que le niveau de sécurité de l'environnement de travail des CAP EMPLOI est suffisamment élevé, ce que l'opérateur se réserve le droit de vérifier par des audits. La formation restreinte relève qu'en cas de non-conformités des environnements de travail des CAP EMPLOI, l'opérateur FRANCE TRAVAIL peut formuler des préconisations, voire ordonner la déconnexion des environnements jugés insuffisamment sécurisés en cas de persistance de ces non-conformités.

39. Par ailleurs les analyses d'impact relatives à la protection des données (AIPD) – réalisées préalablement à la mise en œuvre du traitement en 2022 – précisent que ce sont les règles du corpus documentaire de la politique de sécurité des systèmes d'information de FRANCE TRAVAIL qui s'appliquent au traitement en cause. Si FRANCE TRAVAIL soutient qu'il s'agit là " simplement d'une mesure normale de bonne gestion par France Travail de ses propres solutions auxquelles il donne accès à des tiers ", la formation restreinte estime qu'il ressort clairement de ce passage ainsi que de l'ensemble des documents contractuels transmis que le déploiement effectif des mesures techniques permettant d'assurer la sécurité, de son propre système d'information, incombe à FRANCE TRAVAIL.

40. La formation restreinte souscrit à l'argument de FRANCE TRAVAIL selon lequel " cela ne décharge [pas] ces tiers de leurs obligations de mettre leur propre environnement en condition de respecter ces conditions " et reconnaît à ce titre le rôle important que jouent les CAP EMPLOI dans la diffusion et l'application des règles de sécurité. Néanmoins et indépendamment de ces obligations des CAP EMPLOI qui résultent de leur co-responsabilité de traitement (voir paragraphe 33), la formation restreinte observe que c'est à FRANCE TRAVAIL que revient en premier lieu l'initiative du déploiement et du pilotage des mesures destinées à assurer la sécurité de son système d'information, dont il a ouvert l'accès aux CAP EMPLOI pour l'accompagnement des demandeurs d'emploi ayant fait l'objet d'une décision de reconnaissance de la qualité de travailleur handicapé et bénéficiaires de l'obligation d'emploi.

41. La formation restreinte estime que FRANCE TRAVAIL reste responsable de traitement et principal responsable de la détermination des règles de sécurité applicables.

B. Sur le manquement à l'obligation d'assurer la sécurité des données à caractère personnel traitées

1. Sur la portée de l'obligation de FRANCE TRAVAIL s'agissant de la sécurité du traitement

42. Aux termes de l'article 24-1 du RGPD, " compte tenu 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 met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire ".

43. L'article 32-1 du RGPD dispose : " 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 […] ".

44. L'article 32-2 du RGPD prévoit : " Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite ".

45. Le rapporteur estime que le niveau de sécurité assuré par un responsable de traitement doit s'apprécier au regard du risque lié à la divulgation et à l'accès non autorisé aux données traitées. En l'espèce, il souligne que le traitement comporte de nombreuses données à caractère personnel, dont des catégories particulières au sens de l'article 9, paragraphe 1 du RGPD, ainsi que des données faisant l'objet d'une protection particulière comme le NIR. Il considère que FRANCE TRAVAIL a commis un manquement à l'article 32 du RGPD en n'assurant pas un niveau de sécurité des données traitées suffisamment élevé pour le traitement mis en œuvre.

46. En défense, FRANCE TRAVAIL fait valoir que contrairement à ce qui est avancé par le rapporteur, les vulnérabilités reprochées ne sont pas la conséquence de l'absence de mise en œuvre par FRANCE TRAVAIL de mesures qualifiées de " basiques ". FRANCE TRAVAIL soutient avoir au contraire déployé des mesures de sécurité fortes sur la composante du traitement conjoint sous son contrôle, et ce dès la mise en œuvre du traitement.

47. À titre liminaire, la formation restreinte relève que la CJUE a estimé dans son arrêt " Natsionalna agentsia za prihodite " (14 décembre 2023, C/2024/1065, point 47), que l'absence de violation de données à caractère personnel ne suffit pas à démontrer l'absence de manquement, pas plus que la survenance d'une violation de données ne suffit à caractériser en elle-même l'existence d'un manquement à l'article 32 du RGPD. Des défauts de sécurité peuvent être sanctionnés en tant que tels en raison du risque qu'ils ont fait peser sur l'intégrité des données traitées. La formation restreinte sanctionne régulièrement des manquements à l'obligation de sécurité sans que ceux-ci soient nécessairement à l'origine d'une violation de données, tels qu'une politique de mot de passe insuffisamment robuste (délibération de la formation restreinte n° SAN-2018-009 du 6 septembre 2018, publiée), le stockage de mots de passe en clair (délibération de la formation restreinte n° SAN-2022-018 du 8 septembre 2022), l'absence de politique d'habilitation (délibération de la formation restreinte n°SAN-2021-019 du 29 octobre 2021, publiée) ou encore l'utilisation d'une version obsolète du protocole TLS (décision du président de la formation restreinte n°SANPS-2024-011 du 31 janvier 2024, non publiée).

48. Le respect de l'obligation de moyens par un responsable de traitement ou un sous-traitant s'apprécie au regard du caractère approprié des mesures techniques et organisationnelles mises en œuvre, en tenant compte des risques et en appréciant si la nature, la teneur et la mise en œuvre de ces mesures sont adaptées à ces risques. Elle rappelle que s'il n'apparait pas possible pour un responsable de traitement de se prémunir contre l'ensemble des attaques dites " d'ingénierie sociale ", c'est-à-dire qui exploitent la psychologie humaine, cela ne saurait exonérer le responsable de traitement de ses obligations en vertu des articles 24-1 et 32 du RGPD.

49. Par ailleurs la formation restreinte observe que l'ANSSI applique le principe de " défense en profondeur " aux systèmes d'information, qui consiste à ne pas faire reposer la sécurité " sur un élément mais sur un ensemble cohérent. Cela signifie donc qu'il ne doit en théorie pas exister de point sur lequel tout l'édifice repose ", c'est-à-dire que toute faille de sécurité potentielle d'un composant logiciel doit être compensée par au moins un second niveau de sécurité (voir le Memento sur le concept de défense en profondeur appliquée aux systèmes d'information, version 1.1 du 19 juillet 2004). La formation restreinte note que l'ANSSI fait reposer ce concept sur le postulat que " tout composant d'un système peut être défaillant ou compromis. Ce postulat, qui s'applique également aux fonctions de sécurité d'un SI [système d'information], est confirmé régulièrement par l'actualité sur les vulnérabilités de nombreux produits et logiciels " (voir la note blanche Système d'information hybride et sécurité : un retour à la réalité, 10 août 2021).

50. En l'espèce, la formation restreinte note que […], qui a fait l'objet de la violation, comporte de nombreuses données à caractère personnel (voir paragraphe 13 de la présente délibération). De nombreuses autres données sont également traitées par FRANCE TRAVAIL – même si elles n'ont pas fait l'objet de la violation – telles que les dossiers complets des demandeurs d'emploi. Ainsi FRANCE TRAVAIL traite de nombreuses données intimes et sensibles, portant par exemple sur l'origine du handicap, les contraintes d'un poste de travail, l'évolution de la situation de handicap, les besoins liés à la compensation du handicap et au rétablissement de la personne, les limitations des capacités en milieu professionnel, ainsi que des champs de rédaction libre dans lesquels sont renseignées, pour les besoins du service, les habitudes de vie et les situations particulières des personnes. Ces données peuvent constituer des données de santé en soi ou par croisement. La formation restreinte souligne également que la combinaison potentielle de toutes ces données accroît les risques engendrés par la divulgation de chaque type de données pris séparément.

51. Compte tenu des caractéristiques du traitement et de la portée de l'obligation de sécurité précisées ci-dessus, il appartient à FRANCE TRAVAIL de mettre en place les mesures techniques et organisationnelles adéquates et proportionnées au regard des exigences de l'article 32 du RGPD. Le niveau de sécurité prévu pour le traitement doit permettre de se prémunir contre ces risques.

2. Sur les mesures mises en place par FRANCE TRAVAIL

(i) Sur des modalités d'authentification aux comptes utilisateurs des conseillers CAP EMPLOI

a. S'agissant des mécanismes de restriction d'accès au compte

52. Lorsque les traitements mis en œuvre entraînent la mise en place d'un mécanisme d'authentification par mots de passe, un mot de passe fort est recommandé tant par l'ANSSI que par la Commission dans sa délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés.

53. Cette recommandation, qui n'a certes pas de caractère impératif fournit un éclairage pertinent sur les mesures qu'il convient de prendre en matière de sécurité. Elle prévoit que pour assurer un niveau de sécurité et de confidentialité suffisant, dans l'hypothèse où l'authentification repose uniquement sur un identifiant et un mot de passe, ce dernier doit soit être composé d'au minimum 12 caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux à choisir dans une liste d'au moins 37 caractères spéciaux possibles ; soit être d'au minimum 14 caractères comprenant des majuscules, des minuscules et des chiffres, sans caractère spécial obligatoire ; ou encore, lorsqu'il correspond à une phrase fondée sur des mots de la langue française, être composé d'au minimum 7 mots.

54. À défaut, la Commission considère que permet également d'assurer un niveau de sécurité et de confidentialité suffisant une authentification reposant sur un mot de passe d'une longueur minimum de 8 caractères, composé de 3 catégories de caractères différentes, dès lors qu'elle est accompagnée d'une mesure complémentaire telle que la temporisation d'accès au compte après plusieurs échecs (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (ex : " captcha ") et/ ou le blocage du compte après plusieurs tentatives d'authentification infructueuses (au maximum 10).

55. La formation restreinte a, à plusieurs reprises, adopté des mesures répressives à l'encontre de responsables de traitement qui prévoyaient des mots de passe de connexion d'une robustesse insuffisante (voir notamment les délibérations n° SAN-2022-020 du 10 novembre 2022, n° SAN-2023-021 du 27 décembre 2023 et n° SAN-2023-023 du 29 décembre 2023).

56. Le rapporteur estime que la politique d'authentification par mot de passe prévue par FRANCE TRAVAIL au moment de la violation, plus spécifiquement le seuil de 50 tentatives d'authentification infructueuses avant de verrouiller l'accès aux machines virtuelles des conseillers CAP EMPLOI, était insuffisamment robuste au regard des recommandations et de l'état de l'art. Le rapporteur considère ce seuil insuffisamment proportionné compte tenu de la volumétrie du traitement ainsi que de la sensibilité des données à caractère personnel traitées, ne permettant ainsi pas d'assurer leur sécurité.

57. FRANCE TRAVAIL considère au contraire que sa politique de mot de passe était conforme aux recommandations de la CNIL en ce qu'elle prévoyait, en plus des critères de longueur et de complexité, un seuil de blocage du compte après 50 tentatives infructueuses de connexion – seuil que FRANCE TRAVAIL estime conforme en l'absence d'une position commune des autorités compétentes de sécurité informatique sur ce point. De plus, FRANCE TRAVAIL indique avoir prévu des mesures complémentaires pour assurer la sécurité des données, telles que des techniques de prévention du " password spraying " (qui consiste à utiliser une sélection de mots de passe faibles ou courants pour tenter d'usurper un compte) ainsi qu'un mécanisme de blocage pérenne du compte, nécessitant l'intervention d'un opérateur pour le débloquer. En tout état de cause, FRANCE TRAVAIL souligne qu'aucun critère de complexité ni seuil de blocage n'aurait pu empêcher les intrusions, puisque les attaquants étaient en possession des mots de passe.

58. En l'espèce, la formation restreinte relève que les constatations réalisées par la délégation de contrôle ont permis d'établir qu'à date de la violation de données, la politique de FRANCE TRAVAIL imposait des mots de passe d'une longueur minimum de 8 caractères, avec au minimum 3 types de caractères différents (majuscule, minuscule, chiffre ou caractère spécial), et renouvellement obligatoire du mot de passe tous les 90 jours.

59. Cette modalité correspond au cas n° 2 prévu par la recommandation de la CNIL, c'est-à-dire un mot de passe permettant d'assurer l'équivalent d'une entropie d'au moins 50 bits (avec un minimum de 8 caractères, dont un minimum de 3 caractères spéciaux). Ainsi cette modalité aurait dû, comme l'indique la même recommandation, s'accompagner d'un mécanisme de restriction d'accès au compte. En l'espèce il était prévu un verrouillage du compte après 50 tentatives infructueuses depuis internet – seuil bien supérieur aux 10 tentatives maximales dans un délai donné recommandées par la CNIL dans sa délibération n° 2022-100 précitée. Aucun autre des mécanismes de restriction listés dans cette recommandation (par exemple un " captcha ") n'avait été mis en place pour compenser ce seuil excessivement élevé.

60. La formation restreinte estime par ailleurs que les mesures complémentaires mises en place, bien que relevant de bonnes pratiques, ne compensent pas la faiblesse liée à l'absence de mécanismes de restriction. D'une part, la prévention du " password spraying " vise à renforcer la garantie d'un mot de passe complexe, alors qu'une telle absence de complexité n'est pas reprochée à FRANCE TRAVAIL. D'autre part, le déblocage manuel d'un compte par un opérateur n'enlève rien au fait que le seuil de 50 tentatives fixé avant le blocage du compte est bien trop élevé pour pouvoir constituer une mesure de protection efficace du compte auquel il est lié.

61. En effet, le fait de permettre aux attaquants de tester 50 mots de passe différents avant de bloquer le compte accroit d'autant le risque qu'une de ses tentatives lui donne accès au compte. Le fait que l'ANSSI ne propose pas, comme le fait la CNIL, de seuil précis pour le nombre de tentatives infructueuses à partir duquel le compte utilisateur devrait être bloqué,

ne saurait pour autant conforter FRANCE TRAVAIL dans son choix d'un seuil fixé à 50 tentatives. L'efficience d'un tel mécanisme dépend du nombre de tentatives infructueuses de connexion retenu déclenchant le blocage, un seuil trop élevé pouvant le priver de tout effet utile. Ce seuil doit aussi s'apprécier au regard des risques présentés par le traitement.

62. L'ANSSI a également contribué à la délibération n° 2022-100 du 21 juillet 2022 précitée lors de la consultation publique réalisée par la Commission à cette occasion, y associant ses homologues européens et des experts du domaine. L'ANSSI souligne elle aussi l'importance d'un mécanisme de blocage temporaire " des tentatives d'authentification pendant plusieurs secondes voire minutes (de façon linéaire ou exponentielle) après un certain nombre d'essais infructueux " dans ses " recommandations relatives à l'authentification multi facteurs et aux mots de passe ".

63. Enfin, si la formation restreinte relève que cette vulnérabilité n'a pas été exploitée par les attaquants dans le cadre de la violation de données, il n'en demeure pas moins qu'elle est constitutive d'un manquement à l'obligation de sécurité, qu'il lui appartient de sanctionner.

64. Au regard de la sensibilité, de la volumétrie du traitement, et du risque que fait peser sur celui-ci l'absence de prise en compte des préconisations en matière de robustesse des mots de passe des agents, la formation restreinte considère que les mesures prévues par FRANCE TRAVAIL en lien avec les modalités d'authentification des conseillers CAP EMPLOI ne permettaient pas d'assurer la sécurité des données traitées.

65. FRANCE TRAVAIL indique depuis avoir prévu une évolution de sa politique de mot de passe au premier trimestre 2026, pour imposer l'utilisation d'un mot de passe de 12 caractères, avec au minimum 3 types de caractères différents (majuscule, minuscule, chiffre ou caractère spécial), ainsi qu'un abaissement à 10 du seuil de tentatives de connexion infructueuses en 5 minutes avant blocage du compte.

b. S'agissant de l'absence d'authentification multifacteur pour l'accès aux comptes

66. La Commission souligne dans sa délibération n° 2022-100 précitée que " les acteurs peuvent mettre en œuvre d'autres mesures de sécurité que celles décrites dans cette recommandation s'ils sont en capacité de montrer qu'elles garantissent un niveau de sécurité au moins équivalent " et qu'elle a " notamment toujours considéré que d'autres moyens d'authentification, comme par exemple l'authentification à double facteur ou les certificats électroniques, offrent davantage de sécurité que le seul mot de passe ". Par ailleurs dans son guide pratique sur la sécurité des données personnelles, la CNIL recommande de privilégier l'authentification multifacteur lorsque cela est possible, en particulier lorsque la connexion est accessible depuis l'extérieur du réseau de l'organisme.

67. Le rapporteur considère que FRANCE TRAVAIL n'a pas mis en œuvre de mesures complémentaires à la politique de mots de passe suffisamment robustes permettant d'assurer la sécurité des données traitées. Il estime que cette sécurisation des données aurait dû être assurée – entre autres – par la mise en œuvre d'une authentification multifacteur, mesure dont les AIPD réalisées par FRANCE TRAVAIL prévoyaient la mise en œuvre dès 2023, mais que celui-ci avait finalement repoussée à avril 2024 au regard des difficultés rencontrées.

68. En défense, FRANCE TRAVAIL soutient que le déploiement d'une authentification multifacteur a été retardé par les CAP EMPLOI, sur lesquels repose contractuellement la charge d'assurer " les frais d'investissement et d'exploitation des systèmes d'information, rendus nécessaires pour accéder au système d'information […] ". FRANCE TRAVAIL soutient qu'en vertu du partage des responsabilités, la partie logicielle lui incombe tandis que la partie matérielle (notamment la fourniture de téléphones portables en tant que second terminal pour l'authentification multifacteur) reposait sur les CAP EMPLOI. Ces derniers n'ayant pas été en mesure de disposer d'un second terminal ni de l'enrôler auprès du système d'authentification, puis ayant refusé la solution alternative d'une authentification multifacteur logicielle, FRANCE TRAVAIL soutient qu'il ne peut lui être reproché de ne pas avoir pallié le non-respect des obligations qui n'entraient pas dans le champ de sa responsabilité propre.

69. FRANCE TRAVAIL ajoute que suspendre le traitement ou retarder l'adhésion des CAP EMPLOI tant que ces derniers ne justifiaient pas de conditions d'accès conformes à leurs engagements n'était pas envisageable au regard de la nécessité de permettre l'accompagnement des demandeurs d'emploi bénéficiaires de l'obligation d'emploi. Le risque lié à l'absence d'authentification multifacteur avait été jugé comme seulement théorique en raison des autres mesures fortes de sécurité mises en place. En tout état de cause, FRANCE TRAVAIL souligne qu'une authentification multifacteur n'aurait pas permis de déjouer l'attaque conduite par " ingénierie sociale ".

70. La formation restreinte relève également que dans sa délibération n° 2025-019 du 20 mars 2025 portant adoption d'une recommandation relative à l'authentification multifacteur, la CNIL préconise de recourir à l'authentification multifacteur pour " les traitements de données sensibles, au sens de l'article 9 du RGPD (par exemple le traitement de données de santé), et les traitements ou les opérations à risque pour les personnes concernées " car une telle authentification réduit " significativement la vraisemblance du risque d'accès non autorisés à des systèmes d'information, et a fortiori à des données à caractère personnel ".Bien que récente, cette délibération s'inscrit dans une doctrine antérieurement établie. La nécessité d'une authentification multifacteur avait en effet déjà été soulignée par l'ANSSI en 2021 (recommandations

relatives à l'authentification multifacteur et aux mots de passe), par la CNIL en 2022 (délibération n° 2022-100 précitée) et en 2024 (guide sur la sécurité des données personnelles précité). La formation restreinte a également déjà estimé que la mise en place d'une mesure d'authentification multifactorielle aurait été de nature à empêcher une violation de données (CNIL, FR, 19 décembre 2018, Sanction, n° SAN-2018-011, publié). Ainsi cette doctrine est connue des acteurs et s'impose en particulier pour les traitements de données sensibles et les traitements ou les opérations à risque pour les personnes concernées.

71. En l'espèce, la formation restreinte relève que la délégation de contrôle a été informée de l'absence d'une authentification multifacteur pour l'accès aux comptes des utilisateurs CAP EMPLOI, alors même que les risques associés à l'absence d'une telle mesure avaient été identifiés dès les AIPD (" la connexion sur la machine virtuelle pour les conseillers Cap emploi se fait par authentification simple (identifiant et mot de passe unique) : si un attaquant externe pirate le poste d'un conseiller Cap emploi il lui sera facile d'accéder aux données contenues dans la machine virtuelle (et donc sur le SI de Pôle emploi) [FRANCE TRAVAIL] "). Ces mêmes AIPD prévoyaient la mise en œuvre d'une solution d'authentification à deux facteurs pour 2023, ce que la Commission accueillait favorablement dans son avis n° 2022-050 du 21 avril 2022.

72. La formation restreinte note que c'est précisément l'exploitation de cette vulnérabilité qui a pu conduire – ou du moins n'a pas empêché – la violation de données par usurpation des comptes des conseillers CAP EMPLOI. La formation restreinte ne saurait souscrire à l'argument de FRANCE TRAVAIL selon lequel la mise en place d'une authentification multifacteur aurait été inefficace en cas d'attaque par " ingénierie sociale ". En effet, bien qu'il ne soit pas possible, comme déjà convenu, de se prémunir de toutes les attaques de ce type, en l'espèce une authentification multifacteur aurait rendu extrêmement difficile l'authentification des attaquants au système d'information de FRANCE TRAVAIL. À titre d'exemple, pour une authentification multifacteur reposant sur une application mobile dédiée (avec un second facteur de type " possession " permettant aux employés CAP EMPLOI de recevoir un code sur un téléphone), cela aurait impliqué que les attaquants volent le téléphone, parviennent à le déverrouiller, puis à connaître et saisir le code au sein de l'application permettant de générer un code à usage unique pour finalement accéder à l'outil MAP.

73. De plus, s'il ressort des documents contractuels que les CAP EMPLOI avaient à leur charge d'assurer les frais d'investissement et d'exploitation nécessaires pour accéder au système d'information, ainsi qu'une responsabilité pour la partie matérielle, la formation restreinte a rappelé ci-avant qu'elle considère FRANCE TRAVAIL comme responsable du pilotage de la mise en œuvre des règles de sécurité applicables à son système d'information (voir point II.A. de la présente délibération). Il incombait ainsi à FRANCE TRAVAIL, en sa qualité de développeur et hébergeur de l'outil qu'il ouvre aux CAP EMPLOI, d'apprécier la faisabilité de mise en œuvre de la solution choisie, et de l'adapter en fonction des contraintes respectives. La difficulté du recours à un téléphone comme second facteur, du fait de l'indépendance des CAP EMPLOI, aurait pu être surmontée par d'autres mesures, par exemple par la distribution de calculettes OTP (" One-Time Password ") aux employés des CAP EMPLOI.

74. Enfin, force est de constater que le risque lié à l'absence d'authentification multifacteur n'était pas seulement théorique comme indiqué par FRANCE TRAVAIL. La formation restreinte considère que France TRAVAIL aurait donc dû prendre davantage en considération ce risque réel lors de sa mise en balance avec la nécessité de continuité du service public et de l'accompagnement des demandeurs d'emploi bénéficiaires de l'obligation d'emploi, et ce alors même qu'il existait des solutions alternatives ou intermédiaires. Le choix opéré par France TRAVAIL a conduit à la compromission des données à caractère personnel de plus 36,8 millions de personnes, y compris de données faisant l'objet d'une protection particulière comme le NIR (compte tenu des risques d'usurpation ou d'interconnexion qu'il présente en raison de sa nature signifiante, unique et pérenne).

75. FRANCE TRAVAIL fait état de la mise en place d'une authentification multifacteur après la violation de données, reposant sur […].

(ii) Sur le suivi des journaux d'activité de l'outil […]

76. Dans sa recommandation du 14 octobre 2021 n° 2021-122 relative à la journalisation, la CNIL recommande que " les opérations de création, consultation, modification et suppression des données à caractère personnel et des informations contenues dans les traitements auxquels la journalisation est appliquée fassent l'objet d'un enregistrement comprenant l'auteur individuellement identifié, l'horodatage, la nature de l'opération réalisée ainsi que la référence des données concernées par l'opération " et de " mettre en œuvre un système de traitement et d'analyse des données collectées et de formaliser un processus permettant de générer des alertes et de les traiter en cas de suspicion de comportement anormal ".

77. L'ANSSI rappelle également dans ses " Recommandations de sécurité pour l'architecture d'un système de journalisation " du 28 janvier 2022, que " l'analyse continue des journaux d'évènements permet de repérer des activités inhabituelles, tandis que l'archivage des journaux rend possible les levées de doutes a posteriori. En ce sens, la journalisation constitue également le prérequis indispensable à la mise en œuvre d'une capacité de détection, d'analyse et de réponse aux incidents de sécurité ".

78. Autrement dit, la simple collecte des données de journalisation ne suffit pas à sécuriser un système d'information. Le dispositif de journalisation est efficace uniquement si une entité est en mesure de traiter les informations enregistrées dans les journaux afin d'être capable, le cas échéant, de détecter rapidement un comportement suspect.

79. La Commission préconise donc, dans sa recommandation susvisée, de " mettre en œuvre un système de traitement et d'analyse des données collectées et de formaliser un processus permettant de générer des alertes et de les traiter en cas de suspicion de comportement anormal. Ces données peuvent également servir ex post lorsqu'une violation de données (notamment par consultation, transmission ou usage illégaux des données) est constatée et que le responsable de traitement cherche à en établir la responsabilité. "

80. Le Comité européen de la protection des données considère également dans ses lignes directrices 9/2022 sur la notification de violations de données à caractère personnel en vertu du RGPD, que " la capacité de détecter une violation, d'y remédier et de la communiquer dans les meilleurs délais devrait être considérée comme un élément essentiel ".

81. Le rapporteur reproche à FRANCE TRAVAIL l'absence de contrôle régulier automatique des journaux permettant de détecter et d'analyser les incidents de sécurité et de leur apporter une réponse rapide et efficace. Il estime que la mise en place de telles mesures de journalisation aurait permis de détecter plus rapidement l'attaque dont a été victime FRANCE TRAVAIL.

82. En défense, FRANCE TRAVAIL soutient que le rapporteur sous-estime la difficulté d'analyser les journaux d'un système d'information aussi complexe que le sien et qu'il est toujours plus aisé, comme le fait le rapporteur, d'analyser une situation a posteriori. En l'espèce au moment de la violation, FRANCE TRAVAIL indique qu'il aurait été très difficile de détecter un trafic illégitime alors même que l'attaque s'est déroulée via des comptes légitimes. France TRAVAIL expose qu'il convient de se placer au moment de l'attaque et de son propre point de vue, afin d'estimer si des mesures adaptées au risque avaient été mises en place – obligation que l'organisme estime avoir remplie en l'espèce.

83. La formation restreinte rappelle tout d'abord que la conservation des données de traçabilité est une mesure élémentaire de sécurité d'un traitement, en faveur de laquelle des recommandations ont été publiées par la CNIL en 2021 (recommandation n° 2021-122 précitée) et par l'ANSSI dès 2013 (recommandations de sécurité pour l'architecture d'un système de journalisation du 2 décembre 2013, mises à jour en 2022). Ces recommandations avancent que la journalisation est avant tout justifiée par l'objectif de sécurisation du traitement et qu'elle doit être " active ", c'est-à-dire permettre une détection en continu et en temps réel des opérations anormales afin d'y remédier rapidement. La formation restreinte de la CNIL a déjà sanctionné différents acteurs pour défaut de journalisation efficace.

84. En l'espèce, la formation restreinte relève que FRANCE TRAVAIL disposait, au moment de la violation de données, d'un système de journalisation avec identifiant interne technique et horodatage des actions effectuées par les agents qui conservait ces données pendant un an, ainsi que d'un centre des opérations de sécurité ("security operations center" ou "SOC") surveillant le trafic sur son système d'information.

85. Il ressort de l'instruction que les attaquants, bien qu'apparaissant comme un utilisateur légitime une fois connecté au système d'information de FRANCE TRAVAIL, ont eu un comportement anormal, ne correspondant pas aux habitudes de travail des salariés.

86. En effet, la formation restreinte souligne que si l'attaque s'est effectivement déroulée par le biais de comptes légitimes d'employés de CAP EMPLOI, l'activité de ces comptes présentait de nombreuses caractéristiques suspectes qui auraient dû déclencher des alertes. Les opérations réalisées présentaient un caractère hautement anormal au regard des horaires et de la fréquence des requêtes, du volume considérable de données extraites (25 Go de données de type "texte"), du taux d'erreur de certaines requêtes (69 % sur un des comptes usurpés, correspondant probablement à une phase de test et de tentative de modification du code javascript par les attaquants), et du fait même que les données ont été extraites alors que l'activité des conseillers CAP EMPLOI ne nécessite ni une consommation importante de ressources, ni une extraction importante de données (par exemple, rien que le mardi 6 février 2024, 9 Go de données ont été extraites, ce qui correspondrait à plus de 13 millions de fiches pour un seul conseiller en une seule journée).

87. Or, en dépit de l'ensemble de ces anomalies, le dispositif mis en place par FRANCE TRAVAIL n'a pas permis de détecter les mesures de suivi des journaux d'activité de l'outil, en particulier en générant une alerte afin d'y remédier.

88. Compte tenu de ces éléments, la formation restreinte ne saurait souscrire à l'argument de FRANCE TRAVAIL selon lequel l'attaque n'était pas facilement détectable. Par ailleurs le fait que son système d'information soit extrêmement complexe et fasse régulièrement l'objet d'attaques aurait justement dû conduire FRANCE TRAVAIL à mettre en place un système de journalisation à la hauteur de ce risque et surtout de s'assurer de son exploitation efficace.

89. Cette circonstance est aggravée par le fait que la Commission avait déjà alerté FRANCE TRAVAIL sur la nécessité de mettre en place un système d'analyse des traces dans sa délibération n° 2022-050 du 21 avril 2022.

90. La formation restreinte prend acte des nouvelles mesures mises en place par FRANCE TRAVAIL, comprenant le déclenchement d'alertes selon des seuils d'erreur et de sollicitations prédéfinis et constamment réévalués, ainsi que la réalisation de tests d'intrusion évaluant les capacités de détection et de réponse à des incidents de sécurité.

(iii) Sur la gestion des habilitations d'accès aux données à caractère personnel

91. Le rapporteur estime qu'en autorisant les employés des CAP EMPLOI à accéder, pour l'ensemble des personnes présentes dans la base de données de FRANCE TRAVAIL, à toutes les données de […], FRANCE TRAVAIL n'a pas limité l'accès aux données aux seules personnes ayant besoin d'en connaître.

92. En défense, FRANCE TRAVAIL soutient que cet accès est nécessaire à l'accompagnement des demandeurs d'emploi bénéficiaires de l'obligation d'emploi. L'opérateur souligne que si les conseillers CAP EMPLOI ont accès à toutes les données de toutes les personnes présentes dans […], ils n'ont en revanche accès qu'aux dossiers complets des personnes accompagnées. Enfin, FRANCE TRAVAIL souligne que les comptes des agents CAP EMPLOI sont paramétrés selon trois profils d'habilitation et sur le principe du moindre privilège.

93. La formation restreinte rappelle qu'en vertu de l'article 32 du RGPD, le responsable de traitement doit mettre en place des mesures appropriées pour assurer la confidentialité des données et éviter qu'elles ne soient traitées de façon illicite par des personnes qui n'ont pas besoin d'en connaître. La gestion des habilitations à consulter ou à utiliser un système d'information doit tendre à limiter les accès aux seules données à caractère personnel dont un utilisateur a besoin pour l'accomplissement de ses missions (CNIL, FR, 29 octobre 2021, Sanction, n° SAN-2021-019). Pour déterminer le niveau de finesse de gestion des habilitations, il y a lieu de tenir compte de la quantité et de la nature des données traitées, du caractère plus ou moins imbriqué des différentes finalités de traitement, ainsi que des moyens techniques et humains du responsable de traitement.

94. En l'espèce, la formation restreinte note que les employés des CAP EMPLOI ont accès en consultation à toutes les données présentes dans […] (voir liste de ces données au paragraphe 13). Ils ont accès à ces données pour l'ensemble des demandeurs d'emplois, y compris ceux qui ne sont pas bénéficiaires de l'obligation d'emploi. Ils n'ont en revanche accès aux dossiers complets (c'est-à-dire à toutes les informations de suivi, y compris les données de santé) que pour les personnes accompagnées. La formation restreinte relève également que si les conseillers CAP EMPLOI ont accès par défaut aux données des personnes présentes dans leur région de référence, ils peuvent, à leur seule initiative, modifier le périmètre de la recherche sans limitation géographique.

95. La formation restreinte ne remet pas en cause la nécessité de ces accès, dont elle admet le caractère utile à l'accompagnement des personnes. Elle estime néanmoins que le périmètre des données consultables – tant sur la nature des données que sur les zones géographiques – s'étend bien au-delà de ce qui est strictement nécessaire pour l'exercice des missions des employés CAP EMPLOI. En effet il n'apparaît pas indispensable que ces conseillers aient ainsi accès à autant de données, pour tous les demandeurs d'emploi et pour un périmètre géographique aussi large, ce qui est confirmé par le fait que FRANCE TRAVAIL a indiqué dans ses écritures prévoir de revoir les règles d'habilitations d'accès – sans que cela ne semble lui entraver le suivi des bénéficiaires.

96. La formation restreinte considère que l'accès par les conseillers CAP EMPLOI à un nombre important de données de tous les demandeurs d'emploi présents dans […] a pu élargir le périmètre de la violation de données, puisque les attaques ont été réalisées via des comptes de conseillers CAP EMPLOI, qui avaient accès à l'ensemble de […] de toutes les personnes présentes dans la base de données de FRANCE TRAVAIL, et non seulement aux données des demandeurs d'emploi ayant fait l'objet d'une décision de reconnaissance de la qualité de travailleur handicapé et bénéficiaires de l'obligation d'emploi.

97. La formation restreinte relève néanmoins que des mesures de minimisation et de restriction des accès sont prévues par FRANCE TRAVAIL, qui permettront de limiter les requêtes réalisées sur […] par les employés CAP EMPLOI (limitations géographiques, limitation sur les types de profils affichés, exclusion du NIR dans certains cas).

98. En conclusion, la formation restreinte considère que l'opérateur n'a pas mis en place les mesures techniques et organisationnelles adéquates et proportionnées au regard des exigences prévues par l'article 32 du RGPD, alors même que FRANCE TRAVAIL avait identifié la plupart de ces risques préalablement à la mise en œuvre du traitement. La formation restreinte souligne notamment l'importance d'une authentification robuste, d'une journalisation efficace et d'une politique d'habilitation adaptée, dans un contexte de multiplication des violations de données massives dont avait conscience FRANCE TRAVAIL ainsi qu'à un moment où, comme indiqué par FRANCE TRAVAIL, son système d'information a vocation à être ouvert à davantage d'acteurs du réseau pour l'emploi.

99. Par conséquent, la formation restreinte considère que FRANCE TRAVAIL a manqué à ses obligations issues de l'article 32 du RGPD.

III. Sur les mesures correctrices

100. L’article 20-IV de la loi n° 78-17 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 : […]

101. 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 ".

102. L’article 22, alinéa 2 de la loi Informatique et Libertés dispose ensuite que " la formation restreinte peut rendre publiques les mesures qu’elle prend ".

103. La formation restreinte rappelle que, pour évaluer l’opportunité de prononcer une amende, elle doit tenir compte des critères précisés à l’article 83 du RGPD tels que la nature, la gravité et la durée de la violation, la portée ou la finalité du traitement concerné, le nombre de personnes concernées, 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, les catégories de données concernées et le niveau de dommage subi par les personnes.

104. La CJUE a rappelé à cet égard que " seule une amende administrative dont le montant est déterminé en fonction de la capacité économique réelle ou matérielle de son destinataire […] est susceptible de réunir les trois conditions énoncées à l’article 83, paragraphe 1, du RGPD, à savoir d’être à la fois effective, proportionnée et dissuasive " (CJUE, grande chambre, 5 décembre 2023, C-807/21, " Deutsche Wohnen " ; CJUE, cinquième chambre, 13 février 2025, C-383/23, " Ilva A/S ").

105. En outre, la formation restreinte souligne 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).

106. Enfin, elle rappelle qu’en vertu de l’article 83 du RGPD, les amendes administratives doivent être dissuasives et proportionnées.

A. Sur le prononcé d’une amende administrative et son montant

107. La formation restreinte rappelle qu’il convient d’examiner les critères pertinents de l’article 83 du RGPD pour décider s’il y a lieu d’imposer une amende administrative à l’organisme et, le cas échéant, pour déterminer son montant.

108. Le rapporteur propose à la formation restreinte de prononcer à l’encontre de FRANCE TRAVAIL une amende administrative au regard du manquement constitué à l’article 32 du RGPD.

1. Sur la possibilité du prononcé d’une amende

109. Le rapporteur considère qu’il est possible pour la formation restreinte de prononcer une sanction pécuniaire à l’encontre de FRANCE TRAVAIL, en sa qualité d’opérateur indépendant de l'État.

110. FRANCE TRAVAIL conteste tout d’abord le principe même du prononcé d’une amende à son encontre, estimant que les dispositions de l’article 20 de la loi Informatique et Libertés n’autorisent pas la formation restreinte à sanctionner pécuniairement des traitements mis en œuvre par l’État. Cela reviendrait à ce que l’État s’impose une amende à lui-même, particulièrement pour FRANCE TRAVAIL dont le budget est directement et indirectement abondé par l’État. En outre, FRANCE TRAVAIL demande à la formation restreinte de privilégier le recours à une mesure préventive, telle qu’un rappel à la loi ou une mise en demeure, puisque les manquements étaient susceptibles de faire l’objet d’une mise en conformité. FRANCE TRAVAIL avance à ce titre que l’intention du législateur était de prévoir une gradation des peines listées à l’article 20 de la loi Informatique et Libertés, l’amende administrative figurant en dernière position.

111. En premier lieu, la formation restreinte relève que le Conseil d’État a jugé qu’" il résulte clairement de ces dispositions [article 45 de la loi du 6 janvier 1978, devenu l'article 20 de la même loi] que le prononcé d'une sanction par la formation restreinte de la CNIL n'est pas subordonné à l'intervention préalable d'une mise en demeure du responsable du traitement ou de son sous-traitant par le président de la CNIL " (Conseil d'État, 10ème - 9ème chambres réunies, 04/11/2020, 433311).

112. En second lieu, la formation restreinte ne saurait souscrire à l'argument de FRANCE TRAVAIL selon lequel le législateur a souhaité exonérer d'amende ou d'astreinte les établissements publics administratifs tels que FRANCE TRAVAIL.

113. En effet, s'il ressort des dispositions de l'article 20 de la loi Informatique et Libertés que le prononcé d'une amende administrative par la formation restreinte est exclu s'agissant des traitements " mis en œuvre par l'État ", cette exception, qui doit s'interpréter strictement, n'est pas prévue s'agissant des traitements " mis en œuvre pour le compte de l'État " – notion par ailleurs utilisée par le législateur (notamment au même article 20 de la loi Informatique et Libertés).

114. En l'espèce, FRANCE TRAVAIL est, en vertu de l'article L. 5312-1 du code du travail, une institution nationale publique dotée de la personnalité morale et donc une entité bien distincte de l'État.

115. La formation restreinte relève également que si FRANCE TRAVAIL voit ses orientations générales définies par l'État (notamment dans une convention pluriannuelle d'objectifs et de gestion conclue entre l'État, l'Unédic et FRANCE TRAVAIL), c'est un opérateur qui dispose d'une marge d'initiative importante pour décliner ces objectifs dans des actions concrètes. Par ailleurs FRANCE TRAVAIL est doté de l'autonomie financière, avec un budget qui n'est financé qu'à hauteur d'un tiers par l'État. Le reste est financé par des cotisations et contributions obligatoires des employeurs ; quand bien même celles-ci sont encadrées par l'État, il ne peut être soutenu qu'il s'agit là de ressources directes de l'État.

116. Au total, le traitement concerné n'est ainsi pas mis en œuvre par l'État mais par FRANCE TRAVAIL " pour le compte de l'État ". Il n'est donc pas soumis à l'exclusion prévue au 7° du IV de l'article 20 de la loi Informatique et Libertés.

117. Ainsi les dispositions de l'article 20 de la loi Informatique et Libertés ne font pas obstacle à ce que soit imposée une amende administrative à un établissement public administratif, ce que la formation restreinte souligne avoir déjà fait par le passé (délibération de la formation restreinte n° SAN-2019-004 du 31 janvier 2019, non publiée ; décision du président de la formation restreinte n° SANPS-2024-023 du 23 mai 2024, non publiée).

118. Au regard de l'ensemble de ces éléments, la formation restreinte considère que les conditions du prononcé d'une amende sont remplies.

2. Sur la prise en compte des critères pertinents pour le prononcé d'une amende

119. FRANCE TRAVAIL fait valoir que l'amende administrative proposée par le rapporteur est manifestement disproportionnée au regard des critères de l'article 83 du RGPD. Tout d'abord, l'organisme conteste la gravité du manquement, estimant que le rapporteur l'apprécie comme si FRANCE TRAVAIL était auteur de la violation et non victime, amplifiant par conséquent la gravité attribuée à ce manquement. Ensuite, FRANCE TRAVAIL soutient avoir déployé des mesures de sécurité fortes, particulièrement sur la partie du traitement comportant des données sensibles, et en tout état de cause sur celle du traitement conjoint sous sa responsabilité. Enfin, FRANCE TRAVAIL soutient que la négligence qui lui est imputée – par opposition au caractère délibéré – devrait alléger sa responsabilité plutôt que de l'alourdir.

120. En premier lieu, la formation restreinte considère qu'il y a lieu de faire application du critère prévu à l'article 83, paragraphe 2, a) du RGPD relatif à la nature, à la gravité et à la durée de la violation, compte tenu de la nature, de la portée ou de la finalité des traitements concernés ainsi que du nombre de personnes concernées.

121. La formation restreinte rappelle que la circonstance que des attaquants aient porté atteinte au système d'information de France TRAVAIL est sans incidence sur son obligation de sécurité de moyens résultant de l'article 32 du RGPD. Elle considère que le manquement constaté est grave et que la méconnaissance des principes de sécurité par FRANCE TRAVAIL a fait courir un risque pour la sécurité des données à caractère personnel des millions de personnes concernées.

122. S'ajoute, s'agissant de l'appréciation de la gravité du manquement, le fait que le traitement concerne en partie des personnes vulnérables au sens des Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est " susceptible d'engendrer un risque élevé " aux fins du règlement (UE) 2016/679.

123. La formation restreinte rappelle en outre que la violation de données a concerné les personnes inscrites au cours des 20 dernières années (durées prévues par l'article R. 3212-44 du code du travail, dans sa version en vigueur au moment du contrôle ; qui a depuis été modifié pour réduire et affiner les durées de conservation selon les finalités), ainsi que les données de personnes non inscrites sur la liste des demandeurs d'emploi mais possédant un espace candidat sur le site web " francetravail.fr " (qui permet notamment de consulter les offres d'emploi) – soit au total plus de 36,8 millions de personnes. Elle souligne également de nouveau la richesse des données traitées dans […] auxquelles les attaquants ont eu accès, ainsi que des nombreuses autres données traitées par FRANCE TRAVAIL (dont des données de santé, et des données relatives au handicap), ce qui accentue à la fois l'atteinte à la vie privée des personnes concernées et les risques qui résultent pour elles de la violation.

124. En deuxième lieu, la formation restreinte estime qu'il convient de tenir compte du critère prévu à l'article 83, paragraphe 2, b) du RGPD, relatif au fait que la violation ait été commise délibérément ou par négligence.

125. La formation restreinte relève que si la doctrine requiert la caractérisation d'une " violation fautive " pour imposer une amende administrative, cette notion recouvre une violation commise délibérément mais aussi celles commises par négligence et implique que " le responsable du traitement ne pouvait ignorer le caractère infractionnel de son comportement, qu'il ait eu ou non conscience d'enfreindre les dispositions du RGPD " (CJUE, " Nacionalinis visuomenės " précité, point 81).

126. La formation restreinte considère que le manquement résulte d'une négligence grave de la part de FRANCE TRAVAIL, qui a omis de prendre en compte l'état de l'art, la doctrine constante de la CNIL et de l'ANSSI, ainsi que les recommandations qui lui avaient été faites. Elle ajoute que les vulnérabilités étaient connues et identifiées par FRANCE TRAVAIL dès la mise en œuvre du traitement, les AIPD ayant listé les risques exacts qui se sont matérialisés plus de deux ans après le début de la mise en œuvre du traitement et lors de la violation de données. La Commission avait en outre attiré son attention sur ces enjeux dans sa délibération n° 2022-050 du 21 avril 2022.

127. En troisième lieu, la formation restreinte considère qu'il y a lieu de tenir compte, en application de l'article 83, paragraphe 2, d) du RGPD, du degré de responsabilité du responsable de traitement, compte tenu des mesures techniques et organisationnelles qu'il a mises en œuvre en vertu des articles 25 et 32 du RGPD.

128. Or, comme démontré s'agissant de la responsabilité de FRANCE TRAVAIL vis-à-vis du traitement en cause (II.A.) et sur l'absence d'authentification multifacteur pour l'accès aux comptes des CAP EMPLOI (II.B.2-(i)-b)), la formation restreinte estime que FRANCE TRAVAIL ne saurait se défaire de ses responsabilités de mise en œuvre de mesures techniques et organisationnelles adaptées pour son système d'information.

129. En quatrième lieu, la formation restreinte entend tenir compte des catégories de données à caractère personnel concernées par le manquement, en application de l'article 83, paragraphe 2, g) du RGPD.

130. La formation restreinte rappelle que le traitement en cause comporte des données relatives à la santé, et notamment au handicap, qui sont des catégories particulières de données au sens de l'article 9 du RGPD, dites données sensibles (voir paragraphes 4 à 9). La formation restreinte souligne que bien que les dossiers complets des personnes, comportant les données de santé et les données relatives au handicap, n'aient pas été compromis, il n'en demeure pas moins que les lacunes en termes de sécurité ont mis en évidence un risque certain sur la confidentialité de ces données " sensibles ".

131. Enfin, c'est également le cumul de toutes les données traitées qui permet de fournir des indications précises et complètes sur la vie privée des personnes concernées. En l'espèce la formation restreinte rappelle que la violation a concerné des données permettant d'identifier avec précision la personne à laquelle elles se rapportent (nom d'usage, nom de naissance, prénom, sexe, date de naissance, NIR, adresse, code postal, numéro de téléphone, adresse électronique, adresse géographique (région d'appartenance), référence individuelle, statut de demandeur d'emploi (inscrit, radié ou identifié), date de début et de fin d'inscription). Certaines données comme le NIR font l'objet d'une protection particulière et sont susceptibles de permettre des actions frauduleuses, au préjudice notamment des personnes concernées.

132. Au regard de l'ensemble de ces éléments, la formation restreinte considère que le prononcé d'une amende est justifié.

3. Sur le montant de l'amende

133. En défense, FRANCE TRAVAIL soutient que l'amende proposée est démesurée pour un établissement public administratif qui œuvre à l'intérêt général, qu'elle pèserait lourdement sur son budget et donc également sur les moyens affectés à la conformité des traitements, et qu'elle serait beaucoup plus stricte que des amendes prononcées par la formation restreinte à l'encontre de sociétés qui réalisent des bénéfices.

134. Par ailleurs FRANCE TRAVAIL soutient que le principe de légalité des délits et des peines impose une transparence des modalités de calcul de l'amende proposée à son encontre, afin de pouvoir préparer utilement sa défense. En l'espèce, le rapporteur n'a pas détaillé la méthode de calcul utilisée, que FRANCE TRAVAIL estime erronée en ce qu'elle ne prend pas en compte la spécificité du fonctionnement économique d'un établissement public administratif. FRANCE TRAVAIL souligne à ce titre que son budget n'est pas comparable à un chiffre d'affaires et que son budget repose uniquement sur des dotations publiques.

135. La formation restreinte rappelle tout d'abord que l'article 83 du RGPD prévoit, pour un responsable de traitement qui n'est pas une entreprise, une amende administrative pouvant s'élever jusqu'à dix millions (10 000 000) d'euros en cas de manquement à l'article 32 du RGPD. Elle rappelle que les amendes administratives doivent être dissuasives et proportionnées.

136. La formation restreinte rappelle également que l'exigence de motivation d'une sanction administrative n'impose ni à la formation restreinte, ni au rapporteur de se prononcer sur l'ensemble des critères prévus à l'article 83 du RGPD, et qu'elle n'implique pas non plus que soient indiqués les éléments chiffrés relatifs au mode de détermination du montant de la sanction proposée ou prononcée (CE, 10e/9e, 19 juin 2020, n° 430810 ; CE, 10e/9e, 14 mai 2024, n° 472221).

137. S'agissant de la comparaison avec des amendes prononcées dans d'autres procédures, FRANCE TRAVAIL ne peut utilement comparer sa situation à celles d'autres organismes ayant été sanctionnés pour des manquements prétendument similaires, dans la mesure où le montant d'une amende doit être déterminé au cas par cas. Le Conseil d'État a en ce sens considéré que " la circonstance que des amendes d'un montant plus faible, en proportion de leur chiffre d'affaires mondial, auraient été prononcées par la formation restreinte de la CNIL à l'encontre d'autres sociétés est sans incidence sur la proportionnalité de la sanction infligée à la société requérante " (CE, 10ème et 9ème chambre réunie, 14 mai 2024, société VOODOO, n° 472221).

138. Dès lors, tout en tenant compte des spécificités de FRANCE TRAVAIL en sa qualité d'établissement public administratif, la formation restreinte estime, au regard de la responsabilité de cet opérateur, de ses capacités financières et des critères pertinents de l'article 83, paragraphe 2 du RGPD évoqués ci-avant, qu'une amende administrative d'un montant de cinq millions d'euros (5 000 000 €) euros, au regard du manquement constitué à l'article 32 du RGPD apparaît justifiée.

B. Sur le prononcé d'une injonction

139. Le rapporteur avait initialement sollicité le prononcé d'une injonction de prévoir une politique d'habilitations stricte et reflétant les besoins métiers des conseillers des structures CAP EMPLOI. L'opérateur FRANCE TRAVAIL ayant fait part d'une modification de sa politique d'habilitation, le rapporteur a abandonné la demande d'injonction dans ses écritures du 22 octobre 2025.

140. FRANCE TRAVAIL demande à la formation restreinte, plutôt que de prononcer une amende administrative, de lui enjoindre d'allouer une certaine somme à la sécurisation de son système d'information.

141. La formation restreinte rappelle que l'injonction et l'amende ont des objets différents. Si l'amende administrative est prononcée pour sanctionner des manquements, qui peuvent être passés, l'injonction a vocation à ce que le responsable de traitement cesse la pratique constatée. Par ailleurs la formation restreinte souligne qu'il ne lui appartient pas de flécher les attributions budgétaires de l'organisme.

142. La formation restreinte note également que FRANCE TRAVAIL indique avoir apporté des correctifs sur l'ensemble des vulnérabilités identifiées à la suite de la violation de données et que le rapporteur a abandonné sa demande d'injonction. Cependant elle note qu'aucun document justificatif n'a été transmis à l'appui des déclarations de FRANCE TRAVAIL. Par conséquent, la formation restreinte estime nécessaire le prononcé d'une injonction afin de s'assurer de la mise en œuvre effective des mesures correctrices par FRANCE TRAVAIL.

143. 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.

144. Au regard de ces éléments, la formation restreinte considère comme justifié le prononcé d'une astreinte d'un montant de cinq mille euros (5 000 €) par jour de retard et liquidable à l'issue d'un délai d'un (1) mois suivant la notification de la présente délibération, pour les mesures que FRANCE TRAVAIL indique avoir déjà mises en œuvre, et […].

C. Sur la publicité de la sanction

145. L'opérateur FRANCE TRAVAIL conteste la proposition du rapporteur de rendre publique la présente délibération, soulignant que des mesures de remédiation ont été mises en place immédiatement après la violation et avant même l'intervention de la CNIL, qu'aucune malveillance ni acte volontaire n'a entaché son action, et que les manquements relèvent d'un environnement qui n'était pas sous son seul contrôle. FRANCE TRAVAIL ajoute que les personnes concernées ont déjà été informées de la violation de données, et qu'une telle publicité pourrait aggraver les relations que subissent déjà ses conseillers de la part des usagers.

146. La formation restreinte estime qu'il n'est pas fait grief à FRANCE TRAVAIL de ne pas avoir informé les personnes concernées de la violation de données, et qu'indépendamment de cette information, la publicité est justifiée par la gravité du manquement en cause, la nature du responsable de traitement, les missions d'intérêt public qui lui sont confiées, la sensibilité des données traitées, le nombre très important de personnes concernées et l'absence de choix pour ces dernières de soumettre leurs données à caractère personnel à FRANCE TRAVAIL.

147. S'agissant de l'impact de cette publicité sur les comportements des usagers vis-à-vis des conseillers FRANCE TRAVAIL, la formation restreinte considère que bien d'autres paramètres étrangers à celle-ci interviennent dans la caractérisation de

ces relations.

148. La formation restreinte estime que cette mesure apparait proportionnée dès lors que la décision n'identifiera plus nommément l'organisme à l'issue d'un délai de deux ans à compter de sa publication.

PAR CES MOTIFS

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

- prononce à l'encontre de FRANCE TRAVAIL, une amende administrative d'un montant de cinq millions d'euros (5 000 000 €) au regard du manquement constitué à l'article 32 du RGPD ;

- prononce à l'encontre de FRANCE TRAVAIL une injonction de justifier de la mise en œuvre des mesures de mise en conformité à l'article 32 du RGPD :

1. s'agissant de la robustesse des mots de passe, justifier de la mise en conformité par la mise en œuvre d'une politique de mots de passe prévoyant des mécanismes de restriction d'accès au compte ;

2. s'agissant des modalités d'authentification aux comptes utilisateurs des conseillers CAP EMPLOI, justifier de la mise en conformité par la mise en œuvre d'une authentification multifacteur ;

3. s'agissant du suivi des journaux d'activité de l'outil MAP, justifier de la mise en conformité par les nouvelles mesures mises en places ;

4. s'agissant de la gestion des habilitations d'accès aux données à caractère personnel, justifier de la mise en conformité par les restrictions d'accès aux données.

- assortit l'injonction d'une astreinte de cinq mille euros (5 000 €) par jour de retard à l'issue d'un délai

o d'un mois suivant la notification de la présente délibération, pour les mesures indiquées comme déjà mises en œuvre par FRANCE TRAVAIL […]

o […]

les justificatifs de la mise en conformité devant être adressés à la formation restreinte dans ce délai ;

- décide de rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération, qui n'identifiera plus nommément FRANCE TRAVAIL à l'expiration d'un délai de deux ans à compter de sa publication.

Le Président

Philippe-Pierre CABOURDIN

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