Délibération SAN-2024-021 du 19 décembre 2024

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Date de publication sur Légifrance : Mardi 04 février 2025
Etat juridique : En vigueur

Délibération de la formation restreinte n°SAN-2024-021 du 19 décembre 2024 concernant la société […]

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Philippe-Pierre CABOURDIN, président, M. Bertrand du MARAIS, Mmes Laurence FRANCESCINI et Isabelle LATOURNARIE-WILLEMS, 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 (ci-après le " Règlement " ou " RGPD ") ;

Vu la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après " la loi Informatique et Libertés " ou " loi du 6 janvier 1978 modifiée "), notamment ses articles 20 et suivants ;

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

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

Vu la décision n° 2022-160C du 29 septembre 2022, de la présidente de la Commission nationale de l'informatique et des libertés (ci-après " la Commission " ou " la CNIL ") de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par la société […] ou pour son compte ;

Vu les procès-verbaux n° 2022-160/1 et 2022-160/2 des 17 et 20 octobre 2022, notifiés à la société […] les 19 et 24 octobre 2022 ;

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 5 mars 2024 ;

Vu le rapport de Madame Sophie LAMBREMON, commissaire rapporteur, notifié à la société […] le 31 mai 2024 ;

Vu les observations écrites de la société […] reçues le 16 juillet 2024 ;

Vu la réponse de la rapporteure notifiée à la société […] le 7 août 2024 ;

Vu les observations écrites de la société […] reçues le 23 septembre 2024 ;

Vu la clôture de l'instruction notifiée à la société […] le 11 octobre 2024 ;

Vu les observations orales formulées lors de la séance de la formation restreinte du 14 novembre 2024 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 14 novembre 2024 :

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

En qualité de représentants de la société […] :

- […]

Le président ayant vérifié l'identité des représentants du mis en cause, présenté le déroulé de la séance et rappelé que les mis en cause peuvent, s'ils le souhaitent, présenter des observations orales introductives ou en réponse aux questions des membres de la formation restreinte.

La société […] ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La société […] (ci-après " la société "), société par actions simplifiée dont le siège social est situé […], a un établissement secondaire situé […]. La société, qui exerce une activité d'agence immobilière, propose notamment à sa clientèle, majoritairement des acheteurs professionnels, d'identifier les biens immobiliers présentant la plus forte rentabilité.

2. En 2022, la société employait environ […] personnes, majoritairement des alternants. Pour la période du 1er avril 2020 au 31 décembre 2021, la société a réalisé un chiffre d'affaires de […] euros pour un résultat net de […] euros, puis, en 2022, un chiffre d'affaires de […] euros pour un résultat net de […] euros. En 2023, la société a réalisé un chiffre d'affaires de […] euros, pour un résultat net de […] euros.

3. La société a mis en place le logiciel TIME DOCTOR (ci-après " le logiciel ") dans le cadre du télétravail de ses employés à compter du mois de septembre 2021, pour le suivi de leur activité, puis l'a désactivé le 17 octobre 2022. Installé sur les ordinateurs utilisés par les salariés non cadres de ses départements " marketing/communication ", " chasse ", " gestion locative " et " tech ", les données qu'il collectait étaient consultables par les encadrants à travers une application web.

4. Le logiciel était installé sous deux versions, la première, dite " interactive ", sur les ordinateurs personnels des employés, nécessitant une activation et une désactivation manuelle par ces derniers pendant leur temps de travail et de pause, et la seconde, dite " silencieuse ", installée sur les ordinateurs fournis par la société, pour laquelle l'activation et la désactivation étaient automatiques lors du démarrage et de l'arrêt des ordinateurs.

5. La société a en outre mis en place au sein de son établissement secondaire, en juillet 2022, un dispositif vidéo composé de deux caméras, afin de prévenir les atteintes aux biens (vols).

6. Les 17 et 20 octobre 2022, une délégation de la CNIL a procédé à un contrôle dans les locaux de l'établissement secondaire de la société. Celui-ci avait pour but de vérifier le respect des dispositions de la loi Informatique et Libertés et des autres dispositions relatives à la protection des données personnelles prévues par les textes législatifs et réglementaires, le droit de l'Union européenne et les engagements internationaux de la France. Les procès-verbaux dressés à l'issue ont été notifiés à la société […] les 19 et 24 octobre 2022.

7. Entre octobre et décembre 2022, la société a fourni les éléments d'information complémentaires sollicités par la délégation lors des missions de contrôle.

II. Motifs de la décision

A. Sur les griefs de la société en lien avec la procédure

1) Sur l'absence de communication des plaintes

8. L'article 40. I. paragraphe 7 du décret n° 2019-536 du 29 mai 2019 énonce que " lorsque la procédure a pour origine une réclamation ou une plainte, l'identité de son auteur n'est pas communiquée au mis en cause, à moins que cela soit indispensable à la cessation du ou des manquements constatés ou lorsque les éléments de preuve opposés au mis en cause pour l'établissement du ou des manquements allégués ont été fournis par l'auteur de la plainte ou de la réclamation ".

9. La société fait valoir que les plaintes ayant donné lieu au contrôle d'octobre 2022 ne lui ont pas été communiquées, en méconnaissance du principe du contradictoire et de l'article 6 de la convention européenne des droits de l'homme. Elle estime que la communication de ces plaintes lui aurait permis de prendre connaissance des griefs énoncés, de leur contexte et d'exercer ses droits.

10. La formation restreinte relève qu'il résulte des dispositions de l'article 40. I, paragraphe 7 du décret susvisé que lorsqu'une plainte est à l'origine d'une procédure de sanction, l'identité de son auteur n'est pas communiquée au mis en cause, sauf dans les cas explicitement prévus à cet article.

11. La formation restreinte relève qu'en l'espèce, si des plaintes ont été à l'origine des opérations de contrôle de la CNIL, elles n'ont pas pour autant constitué des éléments de preuve sur lesquels repose l'établissement des manquements que la rapporteure a proposé à la formation restreinte de retenir, ceux-ci étant caractérisés au regard des éléments constatés dans les procès-verbaux de contrôle et des éléments communiqués par la société en réponse aux demandes faites par la délégation, comme cela ressort du rapport de sanction et des observations de la rapporteure. Les éléments de preuve opposés à la société pour l'établissement des manquements n'ont ainsi pas été fournis par les auteurs des plaintes. La formation restreinte relève que la communication de l'identité des plaignants n'était pas non plus indispensable à la cessation des manquements relevés.

12. Par conséquent, la formation restreinte considère que le principe du contradictoire et le respect des droits de la défense n'ont pas été méconnus.

2) Sur l'absence de mesure d'avertissement ou de mise en demeure prise à l'encontre de la société

13. La société fait valoir qu'elle a pleinement coopéré avec la CNIL qui aurait dû prononcer à son égard une mesure d'avertissement ou de mise en demeure, afin qu'elle puisse déterminer si les mesures ainsi mises en œuvre lui permettaient de garantir la conformité des traitements.

14. La formation restreinte rappelle que les dispositions de l'article 20, paragraphe IV de la loi Informatique et Libertés prévoient que la décision de saisir la formation restreinte relève des pouvoirs de la présidente de la CNIL, sans qu'une telle décision soit conditionnée au prononcé d'une mise en demeure préalable (CE, 10ème, 26 avril 2022, Optical Center, n° 449284, inédit). En outre, conformément à ce même article, une mesure d'avertissement ne peut être mise en œuvre que pour avertir un organisme que le traitement qu'il envisage est susceptible de méconnaître les textes applicables, à un stade où ce traitement n'est pas encore déployé, ce qui n'était pas le cas en l'espèce.

15. Compte tenu de ce qui précède, la formation restreinte considère qu'il ressort des dispositions de l'article 20 de la loi Informatique et Libertés que l'autorité de contrôle dispose d'un ensemble de mesures correctrices, adaptées selon les caractéristiques propres à chaque cas, qui peuvent être combinées entre elles et être précédées ou non d'une mise en demeure, les mesures correctrices pouvant être prises directement dans tous les cas (en ce sens, CNIL, FR, sanction n°SAN-2021-021 du 28 décembre 2021).

16. Par conséquent, la formation restreinte considère que la CNIL n'a pas méconnu l'étendue de sa compétence en engageant la présente procédure de sanction à l'encontre de la société, sans avertissement ou mise en demeure préalable.

3) Sur le cadre applicable aux manquements

17. Aux termes de l'article 8, 2° de la loi informatique et libertés, la CNIL " veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi et aux autres dispositions relatives à la protection des données personnelles prévues par les textes législatifs et réglementaires, le droit de l'Union européenne et les engagements internationaux de la France. "

18. La société soutient que, la CNIL étant chargée de sanctionner un éventuel non-respect de ses obligations vis-à-vis du RGPD ou de la loi Informatique et Libertés, il n'entre pas dans ses compétences d'évaluer d'éventuels manquements au regard d'autres dispositions légales ou réglementaires applicables telles que le code du travail, ainsi qu'à la jurisprudence de la Cour de cassation et du Conseil d'Etat.

19. La formation restreinte rappelle que, en vertu de l'article 8, I, 2° de la loi informatique et libertés, la CNIL est compétente pour sanctionner tous manquements au regard notamment des dispositions du RGPD et de la loi Informatique et Libertés. A cet égard, l'article 16 de ladite loi confie à la formation restreinte la compétence pour sanctionner les responsables de traitement ou les sous-traitants qui ne respectent pas les obligations découlant du RGPD et de cette loi.

20. La formation restreinte relève avoir sanctionné, dans un précédent dossier, des manquements aux dispositions de l'article 6 du RGPD, dès lors que le traitement en cause porte une atteinte disproportionnée aux droits des salariés à la vie privée, à la protection de leurs données personnelles, à des conditions de travail qui respectent leur sécurité, leur santé et leur dignité, et en particulier au droit de ne pas faire l'objet d'une surveillance excessive en application de l'article L. 1121-1 du code du travail (CNIL, Sanction SAN-2023-021 du 27 décembre 2023).

21. En effet, pour se prévaloir de la base légale de l'intérêt légitime, le responsable de traitement doit opérer un contrôle de proportionnalité entre les intérêts poursuivis et l'atteinte portée aux droits et intérêts des personnes dont les données sont traitées ; ce contrôle s'effectue en tenant compte du cadre juridique spécifique applicable au traitement, en l'espèce le droit du travail. Un tel raisonnement, à la lumière des dispositions du code du travail, avait été antérieurement confirmé par le Conseil d'Etat (CE, 15 décembre 2017, 10ème et 9ème Ch. réunies, Société Odeolis, n°403776).

22. La formation restreinte relève qu'en l'espèce, les manquements proposés par la rapporteure sont fondés sur les seules dispositions de l'article 6 du RGPD, à la lumière des dispositions de l'article L. 1121-1 du code du travail qui s'appliquent à la surveillance excessive dont ont fait l'objet les salariés de la société […].

23. La formation restreinte est donc compétente pour examiner le manquement à l'article 6 du RGPD à la lumière de l'article L. 1121-1 du code du travail.

B. Sur les manquements relatifs au dispositif de vidéosurveillance et au logiciel de mesure de l'activité des salariés

1. Sur le cadre applicable

24. En premier lieu, l'article 5, paragraphe 1, c) du RGPD prévoit que " [l]es données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ". Le considérant 39 du RGPD précise que " les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens ".

25. En second lieu, aux termes de l'article 6, paragraphe 1, f) du RGPD, " le traitement n'est licite que si, et dans la mesure où, au moins l'une des conditions suivantes est remplie : […] le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel […] ".

26. Le considérant 47 du RGPD précise que " [l]es intérêts légitimes d'un responsable du traitement […] peuvent constituer une base juridique pour le traitement, à moins que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent, compte tenu des attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable du traitement. […] En tout état de cause, l'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive, notamment afin de déterminer si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée […] ".

27. Ainsi, la base légale de l'intérêt légitime repose sur trois conditions : que l'intérêt poursuivi soit légitime, qu'il soit nécessaire de traiter les données à caractère personnel pour la réalisation de cet intérêt légitime et que le traitement ne heurte pas les droits et libertés fondamentaux des personnes dont les données sont traitées, compte tenu de leurs attentes raisonnables. L'atteinte portée aux droits et libertés des salariés constitue l'élément essentiel à prendre en compte dans la mise en balance des intérêts, quand bien même il est également tenu compte d'autres éléments tels que la nature des données à caractère personnel en cause, la nature et les modalités du traitement, ainsi que les attentes raisonnables de la personne concernée (CJUE, 11 décembre 2019, Asociatja de Proprietari bloc M5A-ScaraA, aff. C-708/18 du 11 décembre 2019, § 40, § 56 et 58).

28. Enfin, le considérant 75 du RGPD apporte des précisions sur les risques pour les droits et libertés des personnes physiques pouvant être induits par certains traitements, dont le degré de gravité et de probabilité varie, et qui peuvent entraîner des dommages physiques, matériels ou un préjudice moral. Parmi ces risques, le considérant évoque en particulier ceux résultant de traitements qui visent des personnes physiques vulnérables et/ou portent sur un volume important de données.

29. La formation restreinte relève que, compte tenu de la nature des traitements en cause et leurs conditions de mise en œuvre, les fondements juridiques prévus par les dispositions de l'article 6.1 sous a), b), c), d) et e) du RGPD - liés à l'exécution du contrat, au consentement des personnes, au respect d'une obligation légale, à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique et à l'exécution d'une mission d'intérêt public - ne trouvent pas à s'appliquer en l'espèce, de sorte que seule la base légale liée aux intérêts légitimes poursuivis par le responsable de traitement, prévue par les dispositions de l'article 6.1 sous f), peut trouver à s'appliquer.

30. Elle relève que l'intérêt de la société, en tant qu'employeur, à prévenir les atteintes aux biens dans ses locaux, ainsi qu'à mesurer le temps de travail et à évaluer le travail de ses salariés, constitue un intérêt légitime au sens de l'article 6, paragraphe 1, f) du RGPD. Elle considère que cet intérêt est licite, qu'il est déterminé de façon suffisamment claire et précise et qu'il est, enfin, réel et présent pour la société. Néanmoins, la formation restreinte rappelle que, pour être admis comme base légale du traitement, celui-ci ne doit pas porter une atteinte disproportionnée aux droits et libertés des personnes, eu égard aux finalités poursuivies (CNIL, Sanction SAN-2023-021 du 27 décembre 2023).

31. Par ailleurs, aux termes de l'article L. 1121-1 du code du travail : " Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ". Les droits et libertés protégés sont, en particulier, le droit à la vie privée et personnelle, la protection des données à caractère personnel, le droit à la protection de son intégrité physique et mentale. Il résulte d'une jurisprudence constante de la Cour de cassation que si l'employeur a le droit de surveiller ses salariés, il doit le faire par des moyens proportionnés aux objectifs poursuivis (Cass. Soc., 23 juin 2021, n° 19-13.856), l'utilisation d'un tel

dispositif de surveillance n'étant licite que lorsque ce contrôle ne peut pas être fait par un autre moyen, fût-il moins efficace (Cass. Soc., 19 décembre 2018, n°17-14.631). Cette position est également confirmée par le Conseil d'Etat (CE, 15 décembre 2017, n°403776).

32. Ainsi, c'est à l'aune de ces principes qu'il convient d'apprécier la proportionnalité des dispositifs de vidéosurveillance et du logiciel TIME DOCTOR mis en œuvre pour les finalités recherchées, qui peuvent aboutir à une surveillance permanente disproportionnée des salariés et de leur activité.

2. Sur le manquement en lien avec le dispositif de vidéosurveillance

33. La rapporteure relève que la société a mis en œuvre un dispositif de vidéosurveillance à des fins de prévention des atteintes aux biens (vols) filmant des salariés et captant le son en continu, le dispositif étant visualisable en temps réel à travers une application mobile. La rapporteure considère qu'en l'absence de circonstances particulières le justifiant, un tel dispositif apparaît excessif au regard de sa finalité.

34. En défense, la société affirme, d'une part, que ce dispositif ne permettait pas de capter les conversations de manière intelligible et que la résolution des images ne permettait pas la lecture des informations affichées sur les postes des salariés présents dans le champ des caméras. Elle ajoute que l'accès aux images était restreint à trois associés et un encadrant et que ces captations n'étaient pas conservées. Elle fait valoir, d'autre part, que ce dispositif a été mis en place aux fins de sécuriser les locaux lorsqu'ils étaient vides et non de placer délibérément ses salariés sous surveillance permanente. Elle indique que ce dispositif avait été paramétré en " mode vie privée " lors de son installation, déclenchant un cache sur les objectifs des caméras pendant les horaires d'ouverture de l'établissement, mais que ce mode aurait été désactivé par erreur, ce qu'elle aurait constaté lors des opérations de contrôle. Elle affirme avoir immédiatement réactivé ce mode, impliquant une courte période de désactivation de celui-ci. La société indique avoir depuis procédé au retrait des caméras.

35. La formation restreinte rappelle que si l'employeur a un pouvoir de direction à l'égard des salariés qui l'autorise à les contrôler pendant leur temps et sur leur lieu de travail, les dispositifs de contrôle des salariés doivent respecter le RGPD. A cet égard, comme la formation restreinte a déjà eu l'occasion de le souligner, la surveillance des salariés à travers la mise en place d'un système de vidéosurveillance doit être adéquate, pertinente et limitée à ce qui est nécessaire et ne doit pas porter une atteinte excessive au respect de la vie privée des personnes filmées, eu égard aux conditions de mise en œuvre du dispositif concerné au regard de la finalité poursuivie, du nombre de caméras installées, de leur emplacement, de leur orientation, de leurs fonctionnalités, de leur période de fonctionnement et des caractéristiques propres à l'établissement concerné (CNIL, FR, sanction n° SAN-2019-006 du 13 juin 2019, point 33, publiée). Ainsi, une surveillance permanente des salariés ne peut intervenir que dans des circonstances exceptionnelles, lorsque le dispositif est justifié par une situation ou un risque particulier auquel sont exposées les personnes filmées tenant, par exemple, à la nature de la tâche à accomplir (CNIL, FR, 17 juillet 2014, Sanction, n° 2014-307, publiée ; et CNIL, FR, 14 octobre 2014, Sanction, n° 2014-051, publiée).

36. La formation restreinte rappelle qu'il ressort également de la jurisprudence de la Cour de cassation comme de celle du Conseil d'Etat qu'est " attentatoire à la vie personnelle du salarié, et disproportionné[e] au but allégué par l'employeur de sécurité des personnes et des biens ", la surveillance constante d'un salarié (Cass, soc., 23 juin 2021, n°19-13.856), telle que résultant d'un dispositif de vidéosurveillance les filmant de manière permanente (CE, 18 novembre 2015, Société PS Consulting, n° 371196, Rec.). La Cour de cassation considère également de manière constante que " le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée " (Cass. soc., 2 oct. 2001, Société Nikon France, no 99-42.942 ; Cass. soc., 9 sept. 2020, no 18-20.489) ".

37. La formation restreinte relève en outre que, pour être proportionné, un dispositif de vidéosurveillance ne doit pas, en principe, capter le son. La captation du son n'est admissible que dans des circonstances exceptionnelles dont l'employeur doit pouvoir justifier, et doit alors généralement ne pas être mise en œuvre en continu mais seulement lorsqu'un événement particulier se produit, telle une agression.

38. En l'espèce, la formation restreinte relève qu'il ressort des constatations de la délégation de contrôle que le dispositif de vidéosurveillance captait en continu les images en haute définition ainsi que le son d'espaces de travail des salariés, certains de ces espaces constituant également des espaces de repos. Deux caméras filmaient ainsi un ou plusieurs salariés en continu, pendant leur temps de travail comme pendant leur temps de pause. A cet égard, la formation restreinte note que la résolution des images issues de l'application, tel que cela ressort des constatations, était suffisante pour permettre, à tout le moins, d'observer les salariés en train de travailler.

39. En outre, la formation restreinte relève que, quand bien même le dispositif aurait été initialement paramétré par la société pour déclencher des caches sur les objectifs des caméras durant les heures de travail des employés, et qu'il aurait été désactivé par erreur, cette circonstance ne remet pas en cause l'existence du manquement, caractérisé sur la base des faits constatés lors des contrôles. Par ailleurs, si la société justifie avoir retiré son dispositif de vidéosurveillance en juillet 2024, il n'en reste pas moins que la présence de caméras filmant les salariés dans les conditions précitées, sans cache, a

été constatée lors des contrôles réalisés en octobre 2022, ainsi que la possibilité de consulter en continu les images et le son à travers une application, ce qui n'est pas contesté par la société. Elle note que l'existence d'un " mode vie privée " n'a pas été constatée par la délégation de la CNIL et que la société n'en a pas fait mention lors des opérations de contrôle, mais uniquement en cours d'instruction, en réponse au rapport de sanction, sans préciser d'ailleurs la date à laquelle le " mode vie privée " aurait été désactivé par erreur.

40. La formation restreinte relève enfin que la société ne justifie pas d'une situation particulière ou d'un événement justifiant le recours à la captation permanente des images et du son dans le cadre d'un dispositif de vidéosurveillance à des fins de prévention des atteintes aux biens (vols).

41. Par conséquent, la formation restreinte considère que la captation d'images en continu des employés sur leur poste de travail, et pendant leurs temps de pause, ainsi que la captation en permanence du son, en l'absence de circonstances particulières justifiant la mise en œuvre d'un tel dispositif, ne sont ni adéquates, ni pertinentes, ni limitées à ce qui est nécessaire au regard des finalités poursuivies, et apparaissent dès lors excessives au regard de la finalité précitée. Elle considère en outre que si la société a justifié avoir retiré le dispositif de vidéosurveillance, le manquement à l'article 5, paragraphe 1, c) du RGPD est néanmoins constitué pour le passé.

3. Sur le manquement en lien avec le dispositif TIME DOCTOR

42. La rapporteure relève qu'il ressort des indications données par la société lors des opérations de contrôle que le logiciel TIME DOCTOR a été mis en œuvre par cette dernière non seulement à des fins de mesure du temps de travail des salariés, mais également à des fins d'évaluation de leur productivité. Ainsi, d'une part, ce logiciel comptabilisait les temps d'inactivité des salariés à travers leurs mouvements de souris et leur activité sur leurs claviers (" idle minutes "). D'autre part, il visait également à mesurer la productivité des salariés en procédant à des captures régulières de leurs écrans d'ordinateur (" screencast ") et en comptabilisant leur temps passé sur certains sites web préalablement paramétrés comme productifs ou non par la société. La rapporteure considère que ces traitements sont mis en œuvre de manière disproportionnée eu égard aux finalités poursuivies, de sorte qu'ils ne pouvaient reposer sur la base légale de l'intérêt légitime, en méconnaissance des dispositions de l'article 6 du RGPD.

43. En défense, la société fait valoir que le dispositif TIME DOCTOR n'outrepassait pas les attentes raisonnables des salariés, dès lors qu'ils étaient oralement informés du fonctionnement du logiciel et qu'ils disposaient de la faculté d'en refuser l'utilisation sans conséquence négative. La société indique que peu d'ordinateurs auraient été configurés avec la version " silencieuse " du logiciel, et que les salariés pouvaient aisément justifier, sur simple déclaration, leur temps de travail effectivement réalisé. La société soutient en outre que les données collectées par ce dispositif constituaient un simple indice pour la mesure du temps de travail des salariés, et n'étaient pas utilisées à des fins de surveillance permanente de ces derniers. Par ailleurs, s'il n'est pas contesté que le logiciel permettait le recours à la fonction " screencast " permettant d'effectuer des captures d'écran des ordinateurs des salariés, la société soutient que ces captures d'écran n'étaient pas consultées par les encadrants et que la liste de sites web consultés n'était pas utilisée pour évaluer la productivité des salariés. Elle indique enfin avoir entrepris la suppression des captures d'écran enregistrées dès les opérations de contrôle, n'avoir utilisé le logiciel que sur une période d'un an et deux mois, et l'avoir désinstallé ensuite. Elle ajoute procéder désormais à la " mesure de la performance " de ses salariés avec d'autres outils.

3.1. Sur la finalité de mesure du temps de travail

44. La formation restreinte rappelle, d'une part, que la CNIL considère les dispositifs de surveillance automatisée permanente des salariés, tels que la prise de captures d'écran du salarié à intervalles réguliers ou l'utilisation de " keyloggers " (enregistreurs de frappe / de surveillance de la fréquence des frappes de clavier et des clics de souris permettant d'enregistrer à distance toutes les actions accomplies sur un ordinateur) comme disproportionnés au regard des intérêts légitimes de l'employeur, sauf circonstances exceptionnelles (CNIL, mise en demeure n° MED 2023-102 du 17 novembre 2023, cf. Tables Informatique et Libertés (TIL) sur le site web de la CNIL). La formation restreinte a de même considéré, dans une décision de sanction récente portant sur un système de surveillance automatisée des salariés mesurant très précisément les interruptions d'activité de ces derniers, qu'un tel système " conduit à recenser informatiquement l'intégralité des temps d'interruption d'un salarié […] et à les cumuler sur la semaine, ce qui porte ainsi une atteinte excessive, notamment, au droit à la vie privée et personnelle du salarié ainsi qu'à son droit à des conditions de travail qui respectent sa santé et sa sécurité ". Il ne peut dès lors être mis en œuvre sur le fondement de l'intérêt légitime de l'employeur (CNIL, Sanction SAN-2023-021 du 27 décembre 2023).

45. D'autre part, en application de L.3121-1 du code du travail, la formation restreinte précise en outre que le temps de travail est défini comme " le temps pendant lequel le salarié est à la disposition de l'employeur et se conforme à ses directives sans pouvoir vaquer librement à des occupations personnelles ". Il résulte de ce qui précède que le temps de travail effectif ne se limite pas à la réalisation d'une action continue, circonscrite à une activité de frappe sur un clavier ou un mouvement de souris. Il s'analyse plus largement, comme un temps durant lequel le salarié est à la disposition de son

employeur, pour agir selon ses directives, et sans que ce temps se limite nécessairement à la réalisation d'une tâche continue matérialisée par des actions faites sur ordinateur.

46. En l'espèce, la formation restreinte relève qu'il ressort tant des constatations de la délégation de contrôle que des éléments de réponse de la société, que le logiciel utilisé pour effectuer un décompte du temps de travail incluait une fonctionnalité " time out ", laquelle " permettait de soustraire les temps de pause des périodes de travail actives des salariés ". Cette fonctionnalité était ainsi utilisée pour mesurer nominativement les temps considérés par la société comme étant des temps " d'inactivité " des salariés, identifiés en fonction d'une durée préalablement paramétrée, entre trois et quinze minutes, au cours de laquelle le salarié n'avait effectué aucune frappe sur son clavier d'ordinateur ou aucun mouvement de souris (ce temps correspondant ainsi à des " idle minutes " - minutes d'inactivité). Sur cette base, le logiciel calculait le pourcentage de temps d'inactivité eu égard au temps de travail considéré comme effectif, en tenant compte des horaires d'activation et de désactivation du logiciel. Ce temps de travail effectif était ainsi considéré comme un temps pendant lequel le salarié était constamment en activité, qui se matérialisait à travers les mouvements effectués sur son ordinateur. Les temps " d'inactivité " comptabilisés, que la société considérait comme non travaillés, à défaut d'être justifiés par le salarié ou rattrapés, pouvaient faire l'objet d'une retenue sur salaire. La société demandait en effet à ses salariés de justifier de ces heures comptabilisées comme non travaillées, a posteriori, lors du décompte précédant la paie. Pour les salariés ne pouvant en justifier, la société procédait à une retenue sur salaire.

47. Au vu de ces éléments, la formation restreinte relève que les traitements mis en œuvre via le dispositif TIME DOCTOR – dont la finalité poursuivie était, selon la société, le seul " décompte du temps de travail ", conduisaient à analyser et comptabiliser de manière automatisée, tout au long de la journée, chaque temps " d'inactivité " des salariés supérieur à une durée préalablement et individuellement déterminée pour chacun d'entre eux. La société précise que ce dispositif était utilisé en vue de réaliser un décompte journalier des heures de travail considérées comme effectives et celles jugées comme ne l'étant pas, ces dernières étant identifiées au travers de ces périodes d'absences de frappe sur un clavier ou de mouvement de la souris. Le logiciel permettait ainsi d'analyser toutes les actions – ou absences d'actions – effectuées par les salariés sur leur ordinateur et d'en conclure que certaines périodes correspondaient à du temps travaillé, et d'autres non.

48. Or, la formation restreinte relève tout d'abord que des périodes pendant lesquelles le salarié n'utilise pas son matériel informatique peuvent également correspondre à du temps de travail effectif au cours duquel il peut effectuer diverses tâches, dans le cadre de ses missions, comme par exemple des réunions, du travail manuel à la demande d'un responsable, ou encore des appels téléphoniques. Il ressort des éléments communiqués par la société que de telles tâches sont bien confiées à ses salariés. La formation restreinte rappelle en outre que, en application de l'article L. 3121-1 du code du travail précité.

49. En défense, la société met en avant le fait que ces temps d'inactivité pouvaient être justifiés par les salariés et que, en cas de justification satisfaisante, aucune retenue sur salaire n'était effectuée. La formation restreinte considère que cet argument, loin de constituer une garantie, illustre au contraire le fait que le décompte du temps de travail via ce dispositif, particulièrement intrusif, n'est pas révélateur et que son utilisation n'est pas adaptée à l'atteinte de la finalité poursuivie. Elle observe en outre que de telles justifications peuvent en pratique être difficiles à apporter par les salariés, compte tenu non seulement du temps écoulé depuis le décompte des périodes d'inactivité relevées par le logiciel, mais aussi du volume des temps comptabilisés dont il leur est demandé de justifier. La formation restreinte relève ainsi, à titre d'exemple, une demande de justification faite à un salarié portant sur quarante-trois heures à justifier au cours du moins précédent. Un tel dispositif, reposant en partie sur la possibilité pour les salariés de justifier de leurs actes a posteriori, lors du décompte précédant la paie, ne saurait constituer un système fiable de décompte des heures de travail.

50. Par conséquent, un tel dispositif de mesure du temps de travail, déduisant de ce décompte des temps " d'inactivité " identifiés en fonction des modalités décrites ci-dessus, ne constitue pas un élément de mesure fiable au sens des dispositions de l'article L.3171-4 du code du travail, qui requiert que " le décompte des heures de travail accomplies par chaque salarié, [dès lors qu'il] est assuré par un système d'enregistrement automatique, [soit] fiable et infalsifiable ".

51. En outre, la formation restreinte estime que l'atteinte portée par le dispositif aux droits des salariés était, en tout état de cause disproportionnée. Elle relève que les traitements mis en œuvre via ce logiciel, excédant largement dans ses modalités de mise en œuvre le seul décompte du temps de travail, ne pouvaient entrer dans les attentes légitimes des salariés. En effet, si ces derniers pouvaient s'attendre à un décompte de leur temps de travail - notamment du fait de l'information orale fournie dont fait état en défense la société - ils ne pouvaient raisonnablement s'attendre, pour cette finalité, à une telle surveillance permanente par l'enregistrement, tout au long de la journée, à partir de leurs mouvements de frappe sur leur clavier ou de souris. La formation restreinte estime ainsi que les traitements mis en œuvre via le logiciel TIME DOCTOR constituent un dispositif de surveillance automatisée permanente des salariés, disproportionné au regard de la finalité de mesure du temps de travail, ne pouvant entrer dans leurs attentes raisonnables. La formation restreinte relève de surcroît que plus de la moitié des salariés concernés par l'installation du logiciel disposait d'un ordinateur professionnel, et était soumise à sa version " silencieuse ", ne leur permettant pas d'activer ou de désactiver le logiciel pendant les temps de pause, ajoutant au caractère disproportionné du dispositif TIME DOCTOR.

52. La formation restreinte relève que la société ne fait état d'aucune circonstance exceptionnelle pouvant justifier une telle mise sous surveillance permanente de ses salariés. Le télétravail ne saurait constituer une telle justification dans la mesure où des moyens alternatifs, moins intrusifs, peuvent être mis en place pour encadrer et contrôler le temps de travail et l'activité des salariés (tels qu'une badgeuse électronique, des plannings prévisionnels ou des échanges réguliers avec l'encadrant).

53. Compte tenu de tout ce qui précède, la formation restreinte considère que l'utilisation de ce dispositif pour la mise en œuvre des traitements opérés par le logiciel TIME DOCTOR, n'est pas nécessaire pour l'atteinte de la finalité poursuivie et porte une atteinte disproportionnée à leurs droits au regard de l'intérêt légitime de mesure du temps de travail poursuivi par la société.

54. Par conséquent, la formation restreinte considère que les traitements des données à caractère personnel des salariés de la société par le logiciel TIME DOCTOR ne reposent sur aucune base juridique en méconnaissance de l'article 6 du RGPD.

3.2. Sur la finalité de mesure de la productivité des salariés

55. La formation restreinte relève que le logiciel permettait de mesurer la productivité des salariés, sur la base d'une liste de sites web et de programmes préalablement identifiés et paramétrés comme productifs ou non, eu égard à l'historique de sites et de programmes effectivement consultés par les salariés concernés et recensés par le logiciel. Le logiciel collectait ainsi, pour chaque salarié, des données relatives aux pages web visitées et aux applications utilisées avec la durée afférente, au temps passé sur des sites web jugés productifs et non productifs par la société, et au pourcentage du temps passé sur chacune de ces catégorises de sites web par rapport au temps de travail effectué. Le logiciel permettait en outre d'effectuer des captures régulières de l'écran (" screencast ") de l'ordinateur de chaque employé concerné, dont la récurrence était paramétrée au cas par cas par la direction, par intervalles d'une durée entre trois et quinze minutes. Par ailleurs, dans la version " silencieuse " du logiciel, le salarié ne pouvait pas désactiver cette fonction " screencast " durant ses temps de pause, puisqu'il n'était pas en mesure d'avoir connaissance du caractère actif ou non du logiciel lors de l'utilisation de son ordinateur.

56. La formation restreinte souligne, d'une part, qu'un tel dispositif présente un caractère, si ce n'est permanent, quasi-permanent, compte tenu de la récurrence des captures d'écran, qui constitue ainsi une surveillance particulièrement intrusive des salariés. Elle relève, d'autre part, que la mise en œuvre de ce logiciel peut conduire à la captation d'éléments d'ordre privé (courriels personnels, conversations de messageries instantanées ou de mots de passe confidentiels), ce qui renforce encore le caractère intrusif du dispositif utilisé pour évaluer la productivité des salariés. Ce dispositif porte dès lors une atteinte disproportionnée à la vie privée des salariés.

57. La formation restreinte relève en outre que des moyens alternatifs moins intrusifs sont par ailleurs utilisés par la société afin d'évaluer la productivité des employés. Il ressort en effet des constatations effectuées lors des opérations de contrôle que, interrogée sur les modalités de mesure de la performance de ses salariés, la société a indiqué utiliser, pour le département " chasse ", un outil statistique développé en interne, permettant de déterminer sur la base de différents critères le nombre de biens gérés par le salarié et de faire des comparaisons au sein de l'équipe, pour le département commercial, un outil de gestion de la relation clients pour déterminer le chiffre d'affaires réalisé par chaque salarié et, pour les départements pour lesquels la productivité du travail est plus difficilement quantifiable, une évaluation par les encadrants, lors d'entretiens, de la réalisation du travail effectué.

58. S'agissant de l'argument mis en avant par la société en défense, selon lequel elle n'aurait, in fine, pas utilisé les données collectées par le logiciel à des fins de mesure de la productivité de ses employés, il n'en demeure pas moins qu'elle a paramétré en amont le logiciel afin qu'il collecte ces mesures pour cette finalité, peu importe son choix ultérieur de ne pas les utiliser. En outre, la collecte et la conservation de données qui n'ont pas d'utilité avérée est contraire au principe de finalité prévu par l'article 5 du RGPD et dès lors illicite.

59. Par conséquent, la formation restreinte considère que les traitements de ces données étaient disproportionnés au regard des intérêts et droits fondamentaux des salariés, en particulier de leur droit à la protection de leur vie privée et personnelle, de sorte que les traitements de leurs données à caractère personnel effectués par ce logiciel ne reposaient sur aucune base juridique. Elle considère en outre que si la société a justifié avoir retiré le dispositif TIME DOCTOR, le manquement à l'article 6 du RGPD est néanmoins constitué pour le passé.

C. Sur le manquement à l'obligation d'information des personnes

60. L'article 12 du RGPD prévoit que " le responsable de traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 […] en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible ". Il ajoute que l'information des personnes s'effectue par écrit et que celle-ci peut être délivrée oralement dans l'hypothèse où une telle demande est effectuée par la personne concernée.

61. A titre d'éclairage, les lignes directrices du groupe de travail " article 29 " concernant la transparence au sens du règlement (UE) 2016/679, adoptées le 11 avril 2018, WP260 rev. 01, énoncent que " le responsable du traitement devrait […] veiller à conserver une trace écrite, et s'assurer qu'il est en mesure de [le] prouver (aux fins de la conformité à l'exigence de responsabilité), de : i) la demande d'informations par voie orale, ii) la méthode par laquelle l'identité de la personne concernée a été vérifiée […] et iii) du fait que les informations ont été transmises à la personne concernée ".

62. L'article 13 du RGPD dresse la liste des informations devant être fournies à la personne concernée lorsque les données à caractère personnel sont collectées directement auprès d'elle. Ces informations portent notamment sur l'identité du responsable de traitement et ses coordonnées, les finalités du traitement mis en œuvre, sa base juridique, les destinataires ou les catégories de destinataires des données, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données vers un pays tiers. L'article impose également au responsable de traitement, lorsque cela apparaît nécessaire pour garantir "un traitement équitable et transparent " des données personnelles en l'espèce, d'informer les personnes sur la durée de conservation des données, l'existence des différents droits dont bénéficient les personnes, l'existence du droit de retirer son consentement à tout moment et le droit d'introduire une réclamation auprès d'une autorité de contrôle.

1. Sur le logiciel TIME DOCTOR

63. La rapporteure relève que, si l'usage d'un dispositif de décompte des heures de travail peut être admis, à l'instar d'un contrôle par pointeuse à badge, dès lors qu'il respecte le principe de minimisation des données, il doit cependant faire l'objet d'une information des personnes concernées respectant les dispositions des articles 12 et 13 du RGPD. Elle ajoute que l'information écrite délivrée par la société à ses employés sur le traitement opéré par le logiciel pour contrôler leur temps de travail n'était pas complète, au sens de l'article 13 du RGPD, et que l'information orale dont la société fait état, fût-elle complète, ne remplit pas les conditions prévues par les dispositions de l'article 12 du RGPD.

64. En défense, la société fait valoir que, pour la version " silencieuse " (dont l'activation/désactivation étaient automatiques lors du démarrage/arrêt des ordinateurs), les salariés étaient informés oralement, lors de la remise du matériel informatique, de l'installation du logiciel et de leur possibilité de la refuser, ainsi que de son fonctionnement et de ses finalités. Pour la version " interactive " (nécessitant une activation/désactivation manuelle pendant leurs temps de travail et de pause), outre une information orale lors de leur entrée dans l'entreprise, les salariés alternants étaient invités, par email de la société, à procéder à son installation et à le lui confirmer. En outre, elle fait valoir que tous les salariés, quelle que soit la version du logiciel, disposaient d'une information supplémentaire par le règlement intérieur, la charte informatique, ainsi qu'une clause dans leurs contrats de travail et qu'elle a communiqué, suite aux opérations de contrôle, à l'ensemble des salariés, une notice d'information détaillée afin de se conformer à ses obligations en matière d'information.

65. La formation restreinte relève, s'agissant de l'information écrite fournie aux salariés, que font défaut dans le règlement intérieur, accompagné de la charte informatique, la durée de conservation des données collectées via le logiciel, le droit d'accès à ces données, ainsi que le droit à leur rectification ou à leur effacement, le droit à la limitation des traitements ou de s'y opposer, le droit à la portabilité des données, ou encore le droit d'introduire une réclamation auprès d'une autorité de contrôle.

66. Font défaut dans les contrats de travail communiqués par la société les mentions relatives au droit à la limitation des traitements ou de s'y opposer, au droit à la portabilité des données, ou encore au droit d'introduire une réclamation auprès d'une autorité de contrôle, mentions qui apparaissent en l'espèce nécessaires au caractère équitable des traitements. La formation restreinte relève en outre qu'aucune des mentions précitées ne figure dans les contrats d'alternance.

67. Compte tenu de ce qui précède, la formation restreinte relève que l'information écrite fournie aux salariés, relative aux traitements effectués aux fins de mesure du temps de travail, n'était pas complète au sens de l'article 13 du Règlement puisque les informations relatives aux droits des personnes concernées ne sont pas fournies.

68. S'agissant de l'information orale fournie aux salariés, la formation restreinte relève que, si l'article 12 du RGPD prévoit que les informations requises peuvent être délivrées à l'oral, c'est à la condition que leur fourniture selon ces modalités ait été demandée par la personne concernée, ce dont la société ne justifie pas.

69. En outre, à la lumière des lignes directrices précitées, la formation restreinte considère qu'en l'absence de conservation par la société d'une trace écrite de l'information orale fournie, le caractère complet de l'information n'est pas établi. La formation restreinte considère en outre que, dans de telles circonstances, une simple information orale, même complète, ne permet pas, par nature, de garantir son accessibilité dans le temps pour les salariés qui souhaiteraient s'y référer ultérieurement, de sorte qu'elle ne remplit pas les conditions d'accessibilité prévues par les dispositions de l'article 12 du RGPD.

70. Par conséquent, la formation restreinte considère que la société n'a pas satisfait à son obligation de fournir une information complète, transparente et aisément accessible aux personnes concernées en méconnaissance des articles 12 et 13 du RGPD. En outre, si la société justifie avoir communiqué une notice d'information détaillée – en juillet 2024, soit au cours de la procédure de sanction, postérieurement au retrait du dispositif TIME DOCTOR - et avoir déployé une adresse de contact à destination de ses salariés, le manquement aux articles 12 et 13 du RGPD est néanmoins constitué pour le passé.

2. Sur le dispositif de vidéosurveillance

71. La rapporteure relève que l'information fournie aux salariés relative au dispositif de vidéosurveillance n'était pas conforme aux dispositions des articles 12 et 13 du RGPD.

72. En défense, la société soutient que ce dispositif, désormais désinstallé, avait initialement été paramétré pour déclencher des caches sur les objectifs des caméras durant les horaires de travail, à des fins de détection des intrusions. Elle soutient que, dans ces circonstances, seuls des panneaux sur les portes d'entrée des locaux, informant uniquement de la présence du dispositif, étaient nécessaires.

73. La formation restreinte relève qu'aucune information écrite ni orale n'avait été réalisée auprès des salariés relativement au dispositif de vidéosurveillance. L'unique signalétique affichée consistait en un panonceau présent sur la porte de service, sur lequel figurait un pictogramme de caméra, ainsi que la mention " espace sous vidéo surveillance ", sans autre précision. La formation restreinte relève que l'affichage constaté au jour des contrôles ne comporte pas les mentions obligatoires exigées par le RGPD, ni ne renvoie à un document d'information de second niveau qui contiendrait les informations manquantes. Or, la délégation de CNIL a constaté la présence de deux caméras actives lors des opérations de contrôle, captant les images et le son en continu, et filmant les salariés sur des zones de travail et de repos, sans qu'aucun cache ne se déclenche durant les horaires de travail des salariés.

74. Par conséquent, la formation restreinte considère que la société a commis un manquement aux articles 12 et 13 du RGPD. En outre, si la société justifie avoir désinstallé les caméras en juillet 2024, le manquement aux articles 12 et 13 du RGPD est néanmoins constitué pour le passé.

D. Sur le manquement à l'obligation d'assurer la sécurité des données

75. Aux termes de l'article 32, paragraphe 1 du RGPD, " 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 […] " et notamment " des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement " et 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 ".

76. Au titre des mesures élémentaires de sécurité, il est en principe nécessaire que l'accès à un système d'information contenant des données à caractère personnel qui n'ont pas vocation à être publiées se fasse à travers un compte individuel, auquel l'utilisateur se connecte par un identifiant et un facteur d'authentification propres. En effet, seuls les comptes individuels permettent une bonne traçabilité des accès et des actions effectués sur le système. Les comptes partagés rendent beaucoup plus difficile l'imputabilité d'une action et compliquent le travail d'investigation en cas d'incident de sécurité ou de violation de données.

77. Par ailleurs, s'agissant des mots de passe, conformément aux règles élémentaires relatives à la sécurité des systèmes d'information, un mot de passe doit, pour être efficace, demeurer secret et individuel. Or, lorsqu'un compte est partagé entre plusieurs personnes, cette règle n'est plus respectée.

78. La rapporteure relève que le compte administrateur du logiciel, permettant d'accéder aux données collectées dans le cadre de la mesure du temps de travail et de la productivité des salariés, était partagé par plusieurs utilisateurs, impliquant l'usage d'un même mot de passe, en méconnaissance des dispositions de l'article 32 du RGPD.

79. En défense, la société fait valoir la cessation de l'utilisation du logiciel depuis les opérations de contrôle et la suppression du compte partagé associé. Elle soutient avoir depuis mis en place des mesures afin de respecter les recommandations de l'ANSSI en matière de sécurité des systèmes d'information, de sorte que le manquement relevé par la rapporteure et sa portée seraient partiels.

80. En l'espèce, la formation restreinte relève qu'un encadrant et trois associés de la société étaient habilités à accéder aux données nominatives relatives à l'activité des salariés issues du logiciel TIME DOCTOR en utilisant le compte administrateur de l'un d'eux.

81. La formation restreinte considère que cette pratique ne permet pas, sans mesure complémentaire, de réidentifier les auteurs des opérations effectuées dans le système, tracées au sein des fichiers journaux, dès lors qu'il pourrait s'agir de l'un ou l'autre des utilisateurs. Cette entrave à l'imputabilité d'une action est d'autant plus dommageable quand il s'agit d'un compte administrateur, de tels comptes disposant de droits plus étendus sur les données à caractère personnel traitées par le système, ce qui en fait des cibles privilégiées d'attaque informatique et rend nécessaire de pouvoir détecter rapidement et efficacement une violation de données réalisées par l'un d'entre eux. L'exigence d'individualisation des comptes administrateurs présente ainsi une acuité particulière. À défaut, et en particulier lorsque des systèmes ou des équipements ne permettent pas de disposer de plusieurs comptes d'administration, des mesures complémentaires doivent être mises en œuvre pour assurer l'imputabilité des actions (ex. : bastion, main courante…) et assurer la protection du secret.

82. Par conséquent, ces mesures ayant fait défaut en l'espèce, la formation restreinte considère que la société a méconnu les dispositions de l'article 32 du RGPD. Si la société a justifié, au cours de la procédure de sanction, avoir supprimé ce compte et avoir pris des mesures pour se conformer aux recommandations de l'ANSSI, le manquement à l'article 32 du RGPD est néanmoins caractérisé pour le passé.

E. Sur le manquement à l'obligation d'effectuer une analyse d'impact relative à la protection des données

83. Aux termes de l'article 35, paragraphe 1 du RGPD, " lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel ".

84. Le considérant 84 du RGPD précise qu'" afin de mieux garantir le respect du présent règlement lorsque les opérations de traitement sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque. Il convient de tenir compte du résultat de cette analyse pour déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données à caractère personnel respecte le présent règlement. Lorsqu'il ressort de l'analyse d'impact relative à la protection des données que les opérations de traitement des données comportent un risque élevé que le responsable du traitement ne peut atténuer en prenant des mesures appropriées compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre, il convient que l'autorité de contrôle soit consultée avant que le traitement n'ait lieu. "

85. En outre, la CNIL a établi, en application de l'article 35 du RGPD, une liste, dans sa délibération n° 2018-327 du 11 octobre 2018, qui détermine les types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise, dont les traitements ayant pour finalité de surveiller de manière constante l'activité des employés.

86. La rapporteure relève que la société a mis en œuvre un logiciel, procédant à des traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, sans avoir préalablement réalisé une analyse d'impact relative à la protection des données (ci-après " AIPD "), en méconnaissance des dispositions de l'article 35 du RGPD.

87. En défense, la société soutient que, les salariés pouvant justifier les heures comptabilisées comme temps d'inactivité, et l'utilisation du logiciel n'ayant pas abouti à des sanctions à leur encontre hormis un cas isolé, les traitements des données à caractère personnel effectués à travers le logiciel ne poursuivaient pas une finalité de surveillance systématique des salariés mais constituaient un simple indice de mesure de leur temps de travail. Elle considère par conséquent que, parmi les deux critères précités requis dans les lignes directrices du groupe de travail " article 29 ", fait défaut celui de la collecte de données dans le cadre d'une surveillance systématique, de sorte que ces traitements n'impliquaient pas un risque élevé pour leurs droits et libertés, excluant la nécessité d'une AIPD préalable. La société fait en outre référence à la délibération de la CNIL n° 2019-118 du 12 septembre 2019, qui établit une liste des types d'opérations de traitement pour lesquelles une AIPD n'est pas requise, et considère entrer dans le champ des " traitements mis en œuvre aux seules fins de gestion de contrôle d'accès physiques et des horaires pour le calcul du temps de travail pour les organismes employant moins de 250 personnes " figurant dans cette liste.

88. En l'espèce, la formation restreinte note que la société a indiqué lors des opérations de contrôle qu'elle n'avait réalisé aucune AIPD pour les " traitements RH " mis en œuvre, parmi lesquels figurent ceux mis en œuvre par le biais du logiciel TIME DOCTOR. Or, la formation restreinte relève que, comme exposé plus haut, la société opérait une surveillance, minute par minute, de l'activité de ses salariés, en situation de subordination, pouvant aboutir à une " régularisation de salaire ", quand bien même une seule aurait été effectuée. De plus, à supposer que les données issues du logiciel n'auraient in fine pas été exploitées par la société à des fins de mesure de la productivité des salariés, il n'en reste pas moins qu'elle a sciemment activé en amont, pour chaque salarié, l'option " screencast ", et paramétré les durées entre chaque capture

d'écran, de sorte qu'elle ne s'est pas limitée à activer les seules options relatives au contrôle des horaires proposées par ce logiciel, mais a opéré volontairement un paramétrage différent, en activant des options complémentaires permettant de contrôler l'activité des salariés. Outre cette option, elle a également fait le choix d'activer l'option " time out ", pour décompter les " idle minutes ", matérialisées par l'absence de frappe sur un clavier ou de mouvement de souris pendant une durée, au cas par cas, entre trois et quinze minutes.

89. Ainsi, la formation restreinte considère que les traitements mis en œuvre via ce logiciel – et les options activées - excèdent la seule " gestion du personnel " et procèdent à une surveillance systématique des salariés. Elle rappelle qu'à la lumière des lignes directrices du groupe de travail " article 29 " concernant l'AIPD et la manière de déterminer si le traitement est " susceptible d'engendrer un risque élevé ", adoptées le 4 octobre 2017, la notion de personne vulnérable fait référence à un déséquilibre des pouvoirs qui existe entre les personnes concernées et le responsable du traitement, ce qui signifie que les premières peuvent se trouver dans l'incapacité de s'opposer aisément au traitement de leurs données ou d'exercer leurs droits. Les employés peuvent être dans ce cas. Or, la formation restreinte relève que les traitements effectués à travers le logiciel TIME DOCTOR portaient sur des salariés de la société qui entrent dans ce cas de figure visé par les lignes directrices du groupe de travail sus cité. Elle souligne que 60 % de ceux-ci étaient des alternants, dépendants de surcroît de leur employeur pour la validation de leur diplôme.

90. La formation restreinte estime que, dès lors qu'ils ne mettent pas en œuvre un simple contrôle des horaires ou des accès à l'instar d'une badgeuse (pouvant être électronique), les traitements opérés par le logiciel n'entrent pas dans le champ des types d'opération de traitement pour lesquels une AIPD n'est pas requise, listés dans la délibération n°2019-118 de la CNIL. Au contraire, la formation restreinte considère que les traitements opérés à travers le logiciel TIME DOCTOR, étaient susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Ils conduisaient à opérer une collecte de données à caractère personnel permettant une surveillance systématique des salariés, personnes vulnérables. La formation restreinte estime que ces traitements entrent dans le champ des types d'opération pour lesquels une AIPD doit être préalablement établie, listés par la CNIL dans sa délibération n° 2018-327.

91. Au regard de l'ensemble de ce qui précède, la formation restreinte considère que les traitements mis en œuvre via le logiciel TIME DOCTOR aux fins de contrôle du temps de travail et de la productivité des salariés, conduisaient la société à réaliser des traitements susceptibles d'engendrer un risque élevé pour les droits et libertés de ses salariés, au sens de l'article 35 du RGPD.

92. Par conséquent, en ne réalisant pas une AIPD préalablement à la mise en œuvre de ce traitement, la société a commis un manquement à l'article 35 du RGPD.

III. Sur les mesures correctrices

93. L'article 20 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 : […]

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 ".

94. L'article 83 du RGPD, tel que visé par l'article 20, paragraphe III, de la loi Informatique et Libertés, prévoit quant à lui 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.

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

1. Sur le prononcé d'une amende administrative

95. En défense, la société fait valoir que l'utilisation du logiciel, faite dans l'urgence et dans une période de désorganisation de la société, aurait été partielle, limitée dans le temps et sans conséquence négative pour les salariés. Elle indique que "les traitements [et les manquements associés], limités dans le temps et partiels, n'ont pas fait échec au droit à la protection des données personnelles des salariés, ni à la possibilité d'exercer leurs droits ", compte tenu des informations dont ils disposaient dans le règlement intérieur et leurs contrats de travail. La société soutient que tant le dispositif de vidéosurveillance que le dispositif TIME DOCTOR avaient été mis en place uniquement pour la gestion et l'encadrement

des salariés en période de crise, eu égard aux contraintes du télétravail, et que les traitements effectués à travers ces dispositifs étaient " secondaires à son activité ". Elle soutient en outre que doit être prise en considération sa réactivité, dès les opérations de contrôle, pour se mettre en conformité avec les dispositions du RGPD, ainsi que sa coopération avec les services de la CNIL. Enfin, elle considère que " l'absence de mise en demeure préalable doit conduire à reconsidérer le montant de l'amende administrative prévu […] ".

96. 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.

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

98. La formation restreinte considère qu'en l'espèce, les manquements commis par la société révèlent, pour certains, une intentionnalité, et pour d'autres une négligence de sa part.

99. En premier lieu, la formation restreinte considère qu'il y a lieu de faire application du critère prévu à l'alinéa a) relatif à la gravité du manquement compte tenu de la nature, de la portée ou de la finalité du traitement, ainsi que du nombre de personnes concernées affectées et du niveau de dommage qu'elles ont subi.

100. La formation restreinte relève que la société a manqué à plusieurs principes fondamentaux du RGPD, visant à garantir la licéité des traitements mis en œuvre, leur transparence à l'égard des personnes concernées, ainsi qu'à sécuriser les données à caractère personnel traitées. Elle considère que les manquements constatés sont particulièrement graves au vu de l'atteinte portée aux droits et libertés fondamentaux des salariés.

101. S'agissant du caractère disproportionné des dispositifs mis en œuvre par la société eu égard aux finalités poursuivies, la formation restreinte considère, d'une part, que la captation permanente des images et du son sur les lieux de travail et de pause des salariés, ne répondait pas aux exigences de minimisation des données et, d'autre part, que les traitements effectués à travers le logiciel TIME DOCTOR relatifs au contrôle de l'activité des salariés, comptabilisant constamment les " idle minutes " et prenant des captures d'écran à intervalles réguliers et rapprochés, s'apparentaient à une surveillance permanente des employés. La formation restreinte considère qu'eu égard aux finalités de mesure du temps de travail et de la productivité des salariés, ces traitements disproportionnés ne pouvaient être fondés sur la base de l'intérêt légitime, de sorte que la société ne disposait pas d'une base légale valable en méconnaissance de l'article 6 du RGPD. Cette surveillance est aggravée lorsque le logiciel est installé sous sa version " silencieuse ", sans possibilité de le désactiver. Ces traitements concernaient de surcroît des employés, personnes vulnérables, dont 60 % étaient des alternants particulièrement dépendants de leur employeur pour la validation de leur diplôme.

102. S'agissant du manquement à l'information et à la transparence, les salariés qui ne disposaient pas d'une information complète relative aux traitements de leurs données à caractère personnel par le logiciel TIME DOCTOR, en méconnaissance des exigences des articles 12 et 13 du RGPD. De même, l'affichage relatif au système de vidéosurveillance mis en place ne comportait pas les informations requises, ni ne renvoyait à un autre document les contenant.

103. S'agissant du manquement relatif à la sécurité des données, la formation restreinte souligne qu'il met en lumière des défaillances dans la gestion des droits d'accès et des habilitations, qui constituent pourtant des sujets élémentaires de la sécurité des systèmes d'information.

104. S'agissant enfin du manquement à l'obligation de réaliser une AIPD, la formation restreinte considère qu'au regard de la vulnérabilité des personnes concernées du fait du lien de subordination avec le responsable de traitement, ainsi que de la surveillance systématique mise en place, la réalisation d'une AIPD aurait permis à la société de constater que les traitements effectués à travers le logiciel TIME DOCTOR étaient susceptibles de présenter un risque élevé pour les droits et libertés des salariés, et lui aurait permis de renoncer à leur mise en œuvre, a minima selon les modalités contrôlées par la CNIL.

105. En deuxième lieu, la formation restreinte considère qu'il convient de faire application du critère prévu à l'alinéa b) relatif à l'intentionnalité ou non des manquements commis.

106. La formation restreinte considère que, s'agissant du logiciel TIME DOCTOR, en activant sciemment et en amont l'option " time out ", ayant permis la collecte des données à caractère personnels de ses salariés à travers le décompte de

leurs " idle minutes " aux fins de mesure du temps de travail, ainsi que l'option " screencast " aux fins de mesure de la productivité des salariés, ayant permis la collecte des données correspondantes selon des modalités de durée et de récurrence qu'elle a volontairement et préalablement paramétrées, la société révèle une intentionnalité dans le manquement qu'elle a commis.

107. En outre, la mise sous surveillance permanente des salariés, effectuée à travers le dispositif de vidéosurveillance, particulièrement intrusive et attentatoire à leur vie privée, révèle, à tout le moins, une négligence de la part de la société.

108. Par ailleurs, la formation restreinte reconnait que la société n'a pas délibérément commis le manquement à l'information des personnes concernées, à la sécurité des données, ainsi qu'à son obligation de réaliser une AIPD. La formation restreinte considère néanmoins que ces manquements résultent de sa propre négligence, aggravée d'une part par le fait que des mesures de sécurité élémentaires auraient permis de sécuriser le compte administrateur du logiciel, qui donnait accès à des données dont les traitements portaient atteinte à la vie privée des salariés, et d'autre part par l'intentionnalité de la société dans le placement sous surveillance permanente des salariés à travers le logiciel TIME DOCTOR, lequel était susceptible de présenter un risque élevé pour les droits et libertés de ces derniers.

109. En troisième lieu, la formation restreinte souligne la réactivité de la société qui a désinstallé le logiciel TIME DOCTOR dès la suite des opérations de contrôle. La formation restreinte relève néanmoins que la société, qui met en avant la suppression des caméras de vidéosurveillance, ne justifie leur désinstallation qu'à compter de juillet 2024, soit un an et neuf mois après les contrôles. De même, la société justifie avoir communiqué une notice d'information complète au titre des articles 12 et 13 du RGPD à ses salariés également en juillet 2024. En tout état de cause, les manquements sont constitués pour les faits passés et constatés.

110. En quatrième lieu, la formation restreinte considère qu'il convient de faire application du critère prévu à l'alinéa f) relatif au degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs, la société ayant promptement communiqué les éléments sollicités par la délégation de contrôle de la CNIL.

111. En conséquence, au vu de l'ensemble de ce qui précède, la formation restreinte estime, au vu de l'ensemble de ces éléments et au regard des critères fixés à l'article 83 du RGPD, qu'il y a lieu de prononcer une amende administrative au titre des manquements en cause.

2. Sur le montant de l'amende administrative

112. En défense, la société soutient que le montant de l'amende serait disproportionné compte tenu de sa taille limitée, du fait que les traitements en cause n'ont entraîné selon elle aucun avantage économique et du fait que les résultats financiers pris en considération ne reflèteraient pas sa situation financière réelle.

113. La formation restreinte relève d'abord que les manquements relatifs aux articles 5, paragraphe 1, c), 6, 12, 13 et 32 du RGPD sont des manquements à des principes clés du RGPD, susceptibles de faire l'objet, en vertu de l'article 83 du RGPD, d'une amende administrative pouvant s'élever jusqu'à 20 000 000 euros et jusqu'à 4 % du chiffre d'affaires annuel, le montant le plus élevé étant retenu. Elle rappelle que les amendes administratives doivent être dissuasives et proportionnées.

114. La formation restreinte rappelle que l'article 83 du RGPD pour déterminer le montant de l'amende, fait référence à un montant (jusqu'à 20 000 000 d'euros) ou, dans le cas d'une entreprise, à un pourcentage du chiffre d'affaires annuel (jusqu'à 4%). Si l'avantage économique qu'a pu retirer un responsable de traitement de la mise en œuvre des traitements ayant entraîné le manquement peut être pris en considération dans la détermination du montant de l'amende, il n'en constitue pas pour autant une condition.

115. En outre, la formation restreinte relève que dans le cadre de la prise en compte de l'activité de la société et de sa situation financière pour la détermination de l'amende, la société ne communique aucun élément qui démontrerait une baisse de son chiffre d'affaires ou de son résultat net, mais qu'au contraire, ceux-ci sont en augmentation entre l'exercice de 2020-2021 et l'exercice de 2022. A cet égard, la société […] a réalisé, pour la période du 1er avril 2020 au 31 décembre 2021, un chiffre d'affaires net de […] euros, pour un résultat net de […] euros et, pour l'année 2022, un chiffre d'affaires de […] euros pour un résultat net de […] euros. En 2023, la société a réalisé un chiffre d'affaires de […] euros, pour un résultat net de […] euros. Selon les informations fournies par la société, celle-ci a indiqué un chiffre d'affaires prévisionnel pour 2024 de l'ordre de […] euros avec un résultat net déficitaire de plus de […] euros.

116. Dès lors, au regard de la responsabilité de la société […], de ses capacités financières et des critères pertinents de l'article 83 du RGPD évoqués ci-avant, la formation restreinte estime qu'une amende administrative d'un montant de […] euros, au regard des manquements constitués aux articles 5, paragraphe 1 c), 6, 12, 13, 32 et 35 du RGPD, apparaît justifiée.

B. Sur la publicité de la sanction

117. En défense, la société soutient que la publicité de la sanction n'est pas justifiée. Elle considère notamment que cette publicité ne serait pas opportune dès lors que les dispositifs en cause ont été désactivés, que les salariés ont fait l'objet d'une information exhaustive sur les traitements dont ils font l'objet et les droits qu'ils peuvent exercer, et qu'elle a spontanément collaboré avec la CNIL et déployé des mesures de mise en conformité. La société fait en outre valoir le nombre limité des personnes concernées, sa " situation […] sur le marché [qui] ne justifie pas une publicité qui pourrait avoir des effets pédagogiques ou illustratifs ", ainsi que le fait qu'elle n'aurait retiré aucun bénéfice, ni tout autre avantage, de la mise en œuvre des dispositifs en cause, de sorte que la publicité présenterait pour elle des effets disproportionnés.

118. La formation restreinte considère que ni le caractère passé des manquements, ni les mesures de mise en conformité prises par la société, fussent-elles rapides, ne remettent en cause le caractère justifié d'une publicité de la décision au regard de la gravité des manquements et du fait qu'ils portent sur la surveillance de salariés. Une telle publicité permet d'informer toute personne susceptible d'être soumise à la mesure de son temps de travail et au contrôle de sa productivité à travers de tels logiciels. De même, cette publicité permet d'informer toute personne soumise à la mise en œuvre d'un dispositif de vidéosurveillance sur son lieu de travail des droits dont elle dispose. Néanmoins, la formation restreinte considère que, compte tenu du nombre limité des personnes concernées eu égard à la taille réduite de la société, laquelle a de surcroît indiqué en cours d'instruction avoir, depuis les opérations de contrôle, réduit sa masse salariale, et du retrait immédiat du logiciel par cette dernière lors de ces contrôles, une publicité de la décision sans que la société y soit nommément identifiée, est suffisante à cette fin.

PAR CES MOTIFS

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

• prononcer à l'encontre de la société […] une amende administrative d'un montant de quarante mille euros (40 000 €) pour manquements aux articles 5, paragraphe 1 c), 6, 12, 13, 32 et 35 du RGPD ;

• rendre publique, sur le site web de la CNIL et sur le site web de Légifrance, sa délibération, qui n'identifiera pas nommément la société dès la publication.

Le président

Philippe-Pierre CABOURDIN

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