Le : 18/06/2019

Date de publication sur legifrance: 18/06/2019

Commission Nationale de l'Informatique et des Libertés

Délibération n°SAN-2019-006 du 13 juin 2019
Délibération de la formation restreinte n° SAN-2019-006 du 13 juin 2019 prononçant une sanction à l'encontre de la société UNIONTRAD COMPANY

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Alexandre LINDEN, président, M. Philippe-Pierre CABOURDIN, vice-président, Mme Anne DEBET et Mme Sylvie LEMMET, membres ;

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

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

Vu la loi n° 78-17 du 6 janvier 1978 modifiée 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 modifiée 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° 2018-031C du 2 février 2018 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le Secrétaire général de procéder ou de faire procéder à une mission de vérification de l'ensemble des traitements de données à caractère personnel mis en œuvre par la société UNIONTRAD COMPANY ;

Vu la décision de la Présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 29 janvier 2019 ;

Vu le rapport de M. Éric PÉRÈS, commissaire rapporteur, du 11 février 2019 ;

Vu les observations écrites versées par la société UNIONTRAD COMPANY le 12 mars 2019;

Vu les observations en réponse du commissaire rapporteur du 26 mars 2019 ;

Vu les observations en réponse versées par la société UNIONTRAD COMPANY le 11 avril 2019 ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 18 avril 2019 :
M. Éric PÉRÈS, commissaire, entendu en son rapport ;

En qualité de représentant de la société UNIONTRAD COMPANY :
[…] ;

En qualité de conseils de la société UNIONTRAD :

[…].

La société ayant eu la parole en dernier ;

Après en avoir délibéré, a adopté la décision suivante :

Faits et procédure

La société UNIONTRAD COMPANY (ci-après la société) est une société par actions simplifiée dont le siège est situé 90 avenue des Champs-Élysées à Paris (75008). Elle a pour activité la traduction assermentée et libre de documents (traduction juridique, financière, état civil). La société emploie neuf salariés et a réalisé un chiffre d'affaires de 885 739 euros en 2017 et un résultat net négatif de 110 844 euros.

Entre 2013 et 2015, la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission) a été saisie de quatre plaintes concernant la mise en place d'un dispositif de vidéosurveillance dans les locaux de la société. Dans le cadre de l'instruction de ces plaintes, la CNIL a, à deux reprises, par lettres des 18 octobre 2013 et 2 juin 2016, appelé l'attention de la société sur les règles encadrant la mise en place d'un dispositif de vidéosurveillance et de vidéoprotection et sur la nécessité que le dispositif ne porte pas une atteinte excessive au respect de la vie privée des employés sur le lieu de travail. La Commission a, en outre, demandé à la société de lui transmettre des éléments d'information complémentaires sur le dispositif mis en place. La société a confirmé, par lettres des 6 février 2014 et 1er juillet 2016, que ce dispositif se justifiait dans un souci de sécurité des biens et des personnes et qu'il n'était pas utilisé pour surveiller les activités du personnel.

Malgré les rappels explicites du cadre légal applicable aux dispositifs de vidéosurveillance, quatre nouvelles plaintes ont été adressées à la CNIL en 2017, soulignant la présence de caméras dans l'espace de travail des salariés, les plaçant sous surveillance constante.

En application de la décision n° 2018-031C de la Présidente de la Commission du 2 février 2018, une délégation de la CNIL a procédé à une mission de contrôle dans les locaux de la société le 16 février 2018.

Au cours du contrôle, la délégation a constaté la présence de trois caméras dans les locaux de la société dont une caméra installée dans le bureau des traducteurs, non accessible au public. Cette caméra filmait six postes de travail et une armoire contenant des documents de travail de l'entreprise.

La délégation a relevé que le dispositif de vidéosurveillance n'a fait l'objet d'aucune information formelle à destination des salariés. Elle a observé que la caméra installée dans le bureau des traducteurs permettait de visualiser en continu les postes de travail. L'opération de contrôle a également permis d'établir que la durée de conservation des images excédait celle nécessaire à la finalité indiquée par la société et que par ailleurs, les mesures mises en place par la société pour l'accès aux postes informatiques et à la boîte de messagerie professionnelle ne permettaient pas d'assurer la sécurité et la confidentialité des données.

Le procès-verbal n° 2018-031 dressé à l'issue du contrôle sur place a été notifié à la société par lettre du 20 février 2018.

Des éléments complémentaires ont été fournis par la société par lettre du 12 mars 2018 et courriel du 22 mars 2018.

Au vu des manquements relevés après prise en compte des éléments complémentaires fournis, la Présidente de la CNIL a mis en demeure la société, par décision n° 2018-029 du 26 juillet 2018, dans un délai de deux mois, de :

modifier le dispositif de vidéosurveillance afin qu'il soit proportionné au regard de la finalité poursuivie, conformément aux dispositions désormais applicables du c) de l'article 5 du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des données, et en particulier :
cesser de placer les salariés sous surveillance constante, par exemple, en réorientant ou en déplaçant les caméras ou encore en procédant à la mise en œuvre de masques dynamiques lors de la visualisation des images, notamment concernant la caméra située dans le bureau des traducteurs ;

mettre en œuvre une politique de durée de conservation des données à caractère personnel qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées, conformément aux dispositions du e) de l'article 5 du Règlement précité désormais applicable, en particulier, ne pas conserver les enregistrements des images du dispositif de vidéosurveillance au-delà d'une période de quinze jours ;

procéder à l'information des personnes dont les données sont traitées, notamment s'agissant du dispositif de vidéosurveillance, conformément aux dispositions des articles 12 et 13 du Règlement (UE) 2016/679 désormais applicable, et en particulier :
informer toute personne, par exemple par l'apposition de panneaux, de la mise en œuvre d'un système de vidéosurveillance, en précisant la finalité du traitement, la durée de conservation et les personnes destinataires des données, l'identité du responsable du traitement et les modalités d'exercice des droits ;

prendre toute mesure, pour l'ensemble des traitements de données à caractère personnel mis en œuvre, permettant de préserver la sécurité de ces données et d'empêcher que des tiers non autorisés y aient accès en application de l'article 32 du Règlement (UE) 2016/679 désormais applicable, notamment :

veiller à ce que l'accès aux postes informatiques des salariés soit soumis à une authentification de chaque utilisateur, par exemple via un identifiant et un mot de passe individuels ;

mettre en œuvre une politique de gestion des mots de passe contraignante, tant au niveau du logiciel de consultation des images installé sur le poste informatique du dirigeant que des comptes Windows des salariés, selon l'une des modalités suivantes :
les mots de passe sont composés d'au minimum douze caractères, contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial ;
les mots de passe sont composés d'au moins huit caractères, contenant trois des quatre catégories de caractères (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) et s'accompagnent d'une mesure complémentaire comme 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 dix) ;
un stockage des mots de passe sous une forme hachée (par exemple, à l'aide de l'algorithme SHA256 avec l'utilisation d'un sel) ;
dans tous les cas, les mots de passe doivent faire l'objet d'un renouvellement régulier ;

mettre en œuvre des mesures permettant d'assurer la traçabilité des accès à la boîte de messagerie utilisée, par exemple en mettant en œuvre pour chaque employé des accès individualisés et en supprimant les accès à la boîte de messagerie pour les salariés quittant la société .

Cette décision a été notifiée à la société le 30 juillet 2018.

La société a, par lettre datée du 10 septembre 2018, répondu à la mise en demeure sur les différents manquements qui lui étaient reprochés. Elle a indiqué à la Commission que la caméra installée dans le bureau des traducteurs ne permettait plus de visualiser que deux salariés sans que les postes de travail soient filmés en continu. Elle a précisé que la durée de stockage des

images avait été modifiée et fixée à quinze jours, les images étant détruites automatiquement passé ce délai. Néanmoins, elle a confirmé que l'accès aux postes de travail des salariés se faisait sans mot de passe afin que chaque salarié puisse avoir accès aux fichiers des projets des autres salariés en cas d'absence. Elle a également confirmé que la session Windows du poste du dirigeant était accessible sans mot de passe, afin notamment que le comptable ou le chef de projets puisse y avoir accès. De même, elle a indiqué que les échanges entre la société et ses clients s'effectuent au moyen d'une adresse de messagerie générique accessible par l'ensemble des salariés au moyen d'un mot de passe partagé de huit caractères. S'agissant de l'information des salariés sur l'existence des caméras, la société a affirmé que cette installation était très visible et qu'un grand panneau était affiché à l'entrée des locaux, comportant le nom et le numéro de téléphone du responsable.

Dans la mesure où les justificatifs produits par la société apparaissaient insuffisants, où ses affirmations contredisaient les constatations effectuées lors du contrôle sur place du 16 février 2018 et où elle avait manifesté son intention de ne pas prendre de mesures permettant d'assurer la sécurité des données, une délégation de la CNIL a procédé à une nouvelle mission de contrôle sur place le 10 octobre 2018, sur la base de la décision de la Présidente de la CNIL n° 2018-031C précitée.

Lors de cette mission, la délégation a constaté que la caméra présente dans le bureau des salariés filmait de manière constante des salariés, sans modification depuis le contrôle initial du 16 février 2018. Elle a également constaté qu'aucune information matérialisée à destination des salariés n'avait été effectuée, précisant notamment la finalité du traitement, la durée de conservation, les personnes destinataires des données, l'identité du responsable de traitement et les modalités d'exercice des droits. La délégation a enfin constaté qu'aucune politique de gestion des mots de passe n'avait été mise en œuvre s'agissant de l'accès aux postes informatiques des salariés ou à la messagerie électronique de la société.

Le procès-verbal n° 2018-031-2 du 10 octobre 2018 a été notifié à la société le 19 octobre 2018.

À la suite du contrôle sur place, la société a spontanément informé la CNIL, par lettre du 15 octobre 2018, qu'elle avait procédé à l'obstruction partielle de la caméra filmant le bureau des traducteurs, avec du ruban adhésif, et qu'elle avait redirigé la caméra vers l'armoire comportant les documents (bons de commande et traductions assermentées) à protéger. Elle a également indiqué avoir établi une note d'information à destination du personnel relative à l'installation de caméras dans les locaux. La société a affirmé avoir créé des mots de passe sur tous les postes informatiques respectant le nombre et les catégories de caractère recommandés.

Aux fins d'instruction de ces éléments, la Présidente de la Commission a désigné Monsieur Éric PÉRÈS en qualité de rapporteur, le 29 janvier 2019, sur le fondement de l'article 47 de la loi du 6 janvier 1978 modifiée dans sa version applicable au jour de la désignation.

À l'issue de son instruction, le rapporteur a fait notifier par porteur à la société UNIONTRAD COMPANY, le 12 février 2019, un rapport détaillant les manquements au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données (ci-après le Règlement) qu'il estimait constitués en l'espèce.

Ce rapport proposait à la formation restreinte de la Commission de prononcer une injonction de mettre en conformité le traitement avec les dispositions des articles 5 1. c), 12, 13 et 32 du Règlement, assortie d'une astreinte de 1 000 euros par jour de retard à l'issue d'un délai de deux jours suivant la notification de la délibération de la formation restreinte ainsi qu'une amende administrative d'un montant de soixante-quinze mille (75 000) euros qui serait rendue publique. Il proposait également que cette décision soit rendue publique et anonymisée à l'expiration d'un délai de deux ans à compter de sa publication.

Était également jointe au rapport une convocation à la séance de la formation restreinte du 18 avril 2019 indiquant à la société qu'elle disposait d'un délai d'un mois pour communiquer ses

observations écrites.

Le 8 mars 2019, la société a formulé une demande de huis-clos en raison de la confidentialité liée à son activité de traduction. Le président de la formation restreinte a rejeté sa demande par lettre du 21 mars 2019.

Le 12 mars 2019, la société, par l'intermédiaire de son conseil, a produit des observations. Le rapporteur y a répondu le 26 mars 2019.

Le 11 avril 2019, la société a produit de nouvelles observations en réponse à celles du rapporteur.

Lors de la séance de la formation restreinte du 18 avril 2019, la société a renouvelé sa demande de huis clos, à l'égard de laquelle le président de la formation restreinte a confirmé son refus d'y faire droit, considérant qu'aucun risque d'atteinte à l'ordre public ou à la protection de secrets protégés par la loi n'était caractérisé. L'ensemble des observations présentées au cours de l'instruction ont été réitérées oralement par le rapporteur et la société. Au vu des éléments apportés par la société, le rapporteur a décidé de baisser le montant initialement proposé pour l'amende administrative et proposé un montant de 50 000 euros.

Motifs de la décision

1. Sur le manquement à l'obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données

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

La société a été mise en demeure par décision datée du 26 juillet 2018 et notifiée le 30 juillet 2018, dans un délai de deux mois, de modifier le dispositif de vidéosurveillance afin qu'il soit proportionné au regard de la finalité poursuivie. Il lui était en particulier demandé de cesser de placer les salariés sous surveillance constante, par exemple en réorientant ou en déplaçant les caméras ou encore en procédant à la mise en œuvre de masques dynamiques lors de la visualisation des images, concernant la caméra située dans le bureau des traducteurs.

La société a, dans sa lettre de réponse du 10 septembre 2018, affirmé que la caméra litigieuse ne permettait de visualiser que deux personnes partiellement et qu'elle ne permettait pas de filmer de manière continue le poste de travail de salariés.

La délégation a constaté, lors du second contrôle réalisé le 10 octobre 2018, que le dispositif de vidéosurveillance installé dans le bureau des traducteurs ne présentait aucune modification depuis le contrôle initial du 16 février 2018 et qu'il permettait toujours une surveillance constante et permanente des six salariés.

Par lettre du 15 octobre 2018, la société a informé la Commission avoir procédé à l'obstruction partielle de la caméra avec du ruban adhésif et redirigé la caméra vers l'armoire contenant les documents à protéger. La photographie produite établissant que la caméra était toujours orientée sur au moins un poste de travail, le rapporteur a considéré que la société ne s'était pas mise en conformité à l'issue du délai imparti dans la mise en demeure.

Dans son mémoire du 12 mars 2019, la société a indiqué en défense avoir procédé au retrait de la caméra, comme l'établit le procès-verbal d'huissier de justice du 8 mars 2019 et avoir de bonne foi appliqué le régime de la vidéoprotection à la caméra installée dans le bureau des traducteurs au lieu de celui applicable à la vidéosurveillance.

En premier lieu, s'agissant de la proportionnalité du dispositif de vidéosurveillance, la formation

restreinte relève que la société a indiqué avoir mis en place un tel dispositif pour assurer la sécurité des personnes et des biens. Trois caméras sont installées dans les locaux de la société, dont une dans le bureau des traducteurs, non accessible au public, qui filme en continu les salariés présents et l'armoire contenant les documents à traduire.

La formation restreinte considère que la mise en œuvre d'un système de vidéosurveillance doit obligatoirement respecter le principe de proportionnalité et que la collecte de données personnelles réalisées via ce dispositif doit être strictement nécessaire à l'objectif poursuivi.

En effet, l'article 5 1. c) du règlement (UE) n° 2016/679 du 27 avril 2016 relatif à la protection des données pose le principe de minimisation des données, c'est-à-dire que les données à caractère personnel collectées doivent être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

A cet égard, dès lors qu'un dispositif de vidéosurveillance est susceptible de viser des membres du personnel, le nombre, l'emplacement, l'orientation, les périodes de fonctionnement des caméras ou la nature des tâches accomplies par les personnes concernées, sont autant d'éléments à prendre en compte lors de l'installation du système.

Il en résulte que, si la surveillance de zones sensibles peut être justifiée par des impératifs de sécurité, le placement sous surveillance permanente de salariés, attentatoire à leur vie privée, ne peut toutefois intervenir que dans des circonstances exceptionnelles tenant, par exemple, à la nature de la tâche à accomplir. Il en est ainsi lorsqu'un employé manipule des objets de grande valeur ou lorsque le responsable de traitement est à même de justifier de vols ou de dégradations commises sur ces zones. Au demeurant, l'article L. 1121-1 du code du travail prévoit que 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 .

En l'espèce, la formation restreinte relève qu'aucune circonstance exceptionnelle justifiant de placer les traducteurs, qui sont des traducteurs assermentés, sous surveillance permanente n'est démontrée par la société. Cette dernière invoque la nécessité de protéger les documents traduits. Pour autant, si la nature des documents peut justifier la mise en place de mesures particulières de protection, il convient d'envisager, préalablement à l'utilisation d'un dispositif de vidéosurveillance conduisant à filmer de manière constante les salariés, des procédés alternatifs tels que la sécurisation des accès sur le lieu de travail. Or de tels procédés alternatifs n'ont pas été envisagés par la société, qui ne fait d'ailleurs pas état de vols ou de dégradations survenus dans ses locaux, susceptibles de justifier la mise en place d'un tel dispositif.

Dans ces conditions, l'utilisation d'un dispositif de vidéosurveillance conduisant à placer des salariés sous une surveillance permanente n'apparaît pas justifiée et doit être considérée comme manifestement disproportionnée et excessive au regard de la finalité déclarée.

En second lieu, s'agissant de l'absence de mise en conformité dans le délai fixé par la mise en demeure, la formation restreinte note que deux lettres de la CNIL, adressées à la société dans le cadre de l'instruction de plaintes les 18 octobre 2013 et 2 juin 2016, lui a expressément rappelé la nécessité de mettre en place un dispositif de vidéosurveillance proportionné au regard des finalités mises en œuvre. Ces lettres indiquaient précisément que ce dispositif ne pouvait avoir pour effet de placer sous une surveillance constante un employé ou un groupe d'employés à leurs postes de travail, sauf circonstance exceptionnelle liée à la sensibilité du poste occupé. Malgré ces lettres et la mise en demeure de la Présidente de la CNIL du 26 juillet 2018, il ressort des constats effectués par la délégation de la Commission le 10 octobre 2018 que le dispositif de vidéosurveillance mis en place dans le bureau des traducteurs permettait toujours de filmer des salariés de manière constante et ce, contrairement aux affirmations de la société soutenant que les salariés n'étaient pas filmés en continu.

La formation restreinte relève, en outre, que si la société a pris une mesure le 15 octobre 2018

consistant en l'apposition de ruban adhésif sur la caméra, ce procédé sommaire ne permettait pas d'atteindre la conformité, puisqu'il ressort des pièces du dossier qu'au moins un salarié était encore filmé en continu à son poste de travail.

La formation restreinte retient ensuite que la société a procédé au retrait de la caméra litigieuse le 8 mars 2019, comme cela ressort du procès-verbal d'huissier de justice produit en défense. Elle constate que cette mise en conformité est intervenue tardivement, dans la mesure où ce n'est qu'à la notification du rapport que la société a pris des mesures permettant de ne plus filmer de manière permanente le poste de travail des salariés, alors que cela lui était demandé depuis le 18 octobre 2013.

La formation restreinte retient, en tout état de cause, que la société ne s'est pas mise en conformité à l'expiration du délai fixé dans la mise en demeure du 26 juillet 2018.

Sur la base de ces éléments, la formation restreinte considère que le manquement à l'article 5 1. c) du Règlement est constitué.

2. Sur le manquement à l'obligation d'informer les personnes

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

L'article 13 du Règlement prévoit que : 1. Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes :
a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;
b) le cas échéant, les coordonnées du délégué à la protection des données ;
c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;
d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;
e) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent ; et
f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale (…) ;
2. En plus des informations visées au paragraphe 1, le responsable de traitement fournit à la personne concernée, au moment où les données à caractère personnel sont obtenues, les informations complémentaires suivantes qui sont nécessaires pour garantir un traitement équitable et transparent :
a) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
b) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données ;
c) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point a), ou sur l'article 9, paragraphe 2, point a), l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;
d) le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
e) des informations sur la question de savoir si l'exigence de fourniture de données à caractère

personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ;
f) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphe 1 et 4, et, au moins en pareil cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée (…).

La société a été mise en demeure de procéder à l'information des personnes dont les données étaient traitées, notamment s'agissant du dispositif de vidéosurveillance placé dans le bureau des traducteurs, conformément aux articles 12 et 13 précités, la mise en demeure citant différentes modalités d'information possibles.

A l'occasion du second contrôle du 10 octobre 2018, la délégation a constaté qu'aucune information formelle à destination des salariés, comportant les éléments prévus par l'article 13 du Règlement, n'avait été mise en œuvre. Elle a toutefois été informée que la société s'engageait à rédiger une note d'information à destination des salariés sur le dispositif de vidéosurveillance.

Le rapporteur reproche à la société de ne pas s'être conformée aux injonctions formulées dans la mise en demeure dans le délai imparti et de n'avoir initié des mesures relatives à l'information des salariés quant au dispositif de vidéosurveillance qu'à l'issue du second contrôle.

En défense, la société fait valoir, d'une part, que c'est en raison d'une confusion entre les régimes applicables aux dispositifs de vidéoprotection et de vidéosurveillance qu'elle a pu délivrer une information qui n'était pas satisfaisante au regard des dispositions de l'article 13 du Règlement et, d'autre part, que le dispositif de vidéosurveillance ayant été retiré, elle n'avait plus à effectuer d'information relative à la mise en place d'un tel dispositif.

La formation restreinte relève que la caméra ayant été retirée du bureau des traducteurs, la société n'a effectivement plus, à ce jour, à délivrer d'information aux salariés relative à ce dispositif. Elle relève toutefois que le retrait est intervenu tardivement, puisque c'est uniquement au stade de la procédure de sanction que la mesure a été prise, presque six mois après l'expiration du délai fixé dans la mise en demeure.

La formation restreinte considère en outre que, dès le contrôle sur place du 16 février 2018, le dirigeant de la société a été interrogé par la délégation sur la mise en place d'une information formelle à destination des salariés sur le dispositif de vidéosurveillance placé dans le bureau des traducteurs. La nécessité d'une information spécifique à destination des salariés a lui a donc été rappelée dès février 2018. La société a d'ailleurs été mise en demeure de dispenser une information à destination des salariés, conforme aux dispositions des articles 12 et 13 du Règlement.

Si la société a partiellement complété le panneau d'information présent dans le hall d'accueil dans le délai fixé par la mise en demeure, la formation restreinte relève qu'il s'agit d'un panneau relatif à la vidéoprotection, à destination des visiteurs, qui ne comporte pas les éléments visés à l'article 13 du Règlement. Les mesures d'information particulières, indiquées dans la mise en demeure, qui devaient être prises à destination des salariés n'avaient pas été réalisées puisque la formation restreinte note qu'au jour du second contrôle, le 10 octobre 2018, aucune information formelle à destination des salariés n'avait été mise en œuvre.

La formation restreinte relève que la société a établi, postérieurement à ce contrôle, comme elle l'avait indiqué à la délégation, une note d'information à destination des salariés qui reste toutefois incomplète au regard des exigences de l'article 13 du Règlement.

La société, malgré la bonne foi invoquée, disposait de toutes les informations requises quant aux éléments devant être portés à la connaissance des salariés. Elle n'était donc toujours pas en conformité à l'issue du délai de mise en demeure, ni lors du second contrôle réalisé le 10 octobre

2018.

Sur la base de ces éléments, la formation restreinte considère que le manquement aux articles 12 et 13 du Règlement est constitué.

3. Sur le manquement à l'obligation d'assurer la sécurité et la confidentialité des données

Aux termes de l'article 32 du règlement (UE) n° 2016/679 du 27 avril 2016 :

(…) 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 les 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 (…).

La société a été mise en demeure de remédier aux défauts de sécurité relatifs à l'accès aux postes informatiques des salariés afin qu'ils soient soumis à une authentification de chaque utilisateur. La mise en demeure a également enjoint à la société de mettre en place une politique de gestion des mots de passe contraignante au niveau du logiciel de consultation des images installé sur le poste informatique du dirigeant et au niveau des comptes Windows des salariés, ainsi que de mettre en œuvre des mesures permettant d'assurer la traçabilité des accès à la boîte de messagerie professionnelle générique et de supprimer les accès à cette boîte de messagerie pour les salariés quittant la société.

Par lettre du 10 septembre 2018, la société a confirmé que l'accès aux postes de travail des salariés et à la session Windows du poste du dirigeant se fait sans mot de passe. Elle a précisé que l'accès à la messagerie professionnelle générique pour les échanges avec les clients et la société s'effectuent au moyen d'une adresse de messagerie générique accessible par l'ensemble des salariés via un mot de passe partagé, composé de huit caractères.

Lors du contrôle du 10 octobre 2018, la délégation a confirmé les constats effectués lors du premier contrôle, à savoir que l'ensemble des salariés continuaient d'utiliser un identifiant et un mot de passe uniques et partagés pour accéder à la messagerie professionnelle et que les accès aux postes informatiques des salariés n'étaient toujours pas soumis à authentification. La société a néanmoins informé la délégation qu'elle envisageait de réunir les salariés afin de trouver une solution à la mise en œuvre d'une politique de gestion des mots de passe des postes informatiques compatible avec le fonctionnement de l'entreprise.

La délégation a constaté qu'au jour du contrôle du 10 octobre 2018, aucune politique de gestion des mots de passe contraignante n'avait été mise en place pour les postes informatiques et qu'aucune mesure n'avait été prise pour assurer la traçabilité à l'accès à la messagerie professionnelle.

Il était ainsi reproché à la société de ne pas s'être mise en conformité, s'agissant des mesures à prendre permettant d'assurer la sécurité et la confidentialité des données.

Dans son mémoire du 11 avril 2019, la société fait valoir que chaque salarié dispose désormais d'un identifiant personnel et d'un mot de passe répondant aux recommandations de la CNIL, telles que définies dans sa délibération n° 2017-012 du 19 janvier 2017, comme cela ressort du procès-verbal d'huissier de justice du 10 avril 2019.

La formation restreinte relève que si la société s'est mise en conformité au cours de l'instruction,

s’agissant de l’authentification de chaque utilisateur lors de l’accès aux postes informatiques des salariés et de la mise en œuvre d’une politique de mots de passe contraignante, elle ne l’avait pas fait à l’expiration du délai de mise en demeure, ni lors du second contrôle du 10 octobre 2018. Elle ne l’a fait que postérieurement à l’issue de l’engagement d’une procédure de sanction.

La formation restreinte constate, en outre, que la société n’a apporté aucune réponse s’agissant des mesures à mettre en œuvre afin d’assurer la traçabilité des accès à la boîte de messagerie professionnelle générique. Elle note cependant que la société s’engage à révoquer les accès en cas de départ définitif d’un salarié.

Sur la base de l’ensemble de ces éléments, la formation restreinte considère que le manquement à l’article 32 du Règlement est constitué.

4. Sur la sanction et la publicité

L’article 20-III de la loi du 6 janvier 1978 modifiée dispose : Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi, le président de la Commission nationale de l’informatique et des libertés peut également, le cas échéant après lui avoir adressé l’avertissement prévu au I du présent article ou, le cas échéant en complément d’une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l’une ou de plusieurs des mesures suivantes : (…) 2° Une injonction de mettre en conformité le traitement avec les obligations résultant de la présente loi ou du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité (…), qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l’Etat, d’une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte ; (…) 7° À l’exception des cas où le traitement est mis en œuvre par l’État, une amende administrative ne pouvant excéder 10 millions d’euros ou, s’agissant d’une entreprise, 2 % du chiffre d’affaires annuel mondial total de l’exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l’article 83 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, 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.

L’article 83 du RGPD prévoit : 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. Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l’article 58, paragraphe 2, points a) à h), et j). Pour décider s’il y a lieu d’imposer une amende administrative et pour décider du montant de l’amende administrative, il est dûment tenu compte, dans chaque cas d’espèce, des éléments suivants : a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu’elles ont subi; b) le fait que la violation a été commise délibérément ou par négligence ; c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées; d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu’ils ont mises en œuvre en vertu des articles 25 et 32; e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant; f) le degré de coopération établi avec l’autorité de contrôle en vue de remédier à la violation et d’en atténuer les éventuels effets négatifs; g) les catégories de données à caractère personnel concernées par la violation; h) la manière dont l’autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation; i) lorsque des mesures visées à l’article 58, paragraphe 2, ont été précédemment ordonnées à l’encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures; j) l’application de codes de conduite approuvés en application de l’article

40 ou de mécanismes de certification approuvés en application de l'article 42; et k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

En premier lieu, s'agissant de l'injonction de mettre en conformité le traitement avec les dispositions des articles 5 1 c), 12, 13 et 32 du Règlement, la formation restreinte relève que la société a procédé au retrait de la caméra placée dans le bureau des traducteurs. Elle considère dès lors qu'il n'y a plus lieu de maintenir l'injonction tendant à modifier le dispositif de vidéosurveillance afin que les salariés ne soient plus placés sous une surveillance constante.

La formation restreinte considère également que le dispositif de vidéosurveillance ayant été retiré, la société n'a plus à délivrer d'information relative à la mise en œuvre d'un tel dispositif. En conséquence, il n'y a plus lieu de maintenir l'injonction relative au manquement à l'obligation d'information des personnes concernées.

En revanche, la formation restreinte constate que la société n'a pas mis en place de mesures permettant d'assurer la traçabilité des accès individuels à la boîte de messagerie professionnelle partagée. En effet, afin d'assurer la sécurité et la confidentialité des données personnelles ou de déterminer l'origine d'un incident de sécurité, il convient de procéder à la détermination des personnes habilitées à accéder aux données et de tracer les actions effectuées sur le système informatique en vue notamment d'identifier les accès illicites et les risques d'atteinte à l'intégrité des données. Pour ce faire, il convient de s'assurer que les utilisateurs sont authentifiés au moyen de comptes individuels avant d'accéder aux données et que ces accès à la messagerie générique font l'objet d'une journalisation.

Faute pour la société de s'être mise totalement en conformité sur ce manquement, il y a lieu de maintenir l'injonction.

En second lieu, la société soutient qu'une amende administrative de 75 000 euros serait disproportionnée compte tenu des critères fixés par l'article 83 du Règlement, de ses capacités financières et des sanctions précédemment prononcées par la formation restreinte. Elle met en avant les mesures prises pour atténuer le dommage subi par ses salariés, son degré de coopération avec la Commission, sa confusion entre les régimes de vidéoprotection et de vidéosurveillance et les graves difficultés financières qu'elle rencontre depuis trois ans.

Tout d'abord, la formation restreinte estime que, dans le cas d'espèce, les manquements précités justifient que soit prononcée une amende administrative à l'encontre de la société pour les motifs suivants.

La formation restreinte rappelle que les manquements aux articles 5 1 c), 12, 13 et 32 du Règlement ont persisté au-delà du délai imparti par la mise en demeure de la Présidente de la Commission et que ce n'est qu'à la notification du rapport de sanction que la société a pris des mesures pour se mettre partiellement en conformité. La société n'a ainsi, contrairement à ce qu'elle soutient, pas activement collaboré avec les services de la Commission jusqu'à l'engagement de la procédure de sanction.

Plus particulièrement, s'agissant du manquement relatif au dispositif de vidéosurveillance, la formation restreinte souligne que la société a placé sous une surveillance constante les traducteurs de la société pendant plusieurs années sans motif valable et sans qu'aucune mesure ne soit prise à cet égard à la suite des lettres adressées à la société par la CNIL en 2013 et 2016, du contrôle sur place du 16 février 2018, de la mise en demeure adressée à la société le 26 juillet 2018 et du second contrôle sur place réalisé le 10 octobre 2018. De surcroît, la formation restreinte relève que la société a apporté des réponses en contradiction avec les constats établis lors des opérations de contrôle. En tout cas, ce n'est qu'en mars 2019 que la société a procédé au retrait de la caméra litigieuse, une fois la procédure de sanction engagée. La société ne peut donc se prévaloir d'avoir mis en place des moyens visant à limiter l'atteinte subie par les salariés, dès

lors que la caméra a été retirée très tardivement, plusieurs mois après l'expiration du délai de mise en demeure. Elle ne peut davantage se prévaloir d'une quelconque confusion du cadre légal applicable au vu des échanges qui ont eu lieu entre la société et les services de la Commission, lui enjoignant de cesser de placer ses salariés sous une surveillance constante.

En outre, la formation restreinte souligne la particulière sensibilité du dispositif de vidéosurveillance des salariés sur leur lieu de travail. Elle rappelle que le premier contrôle sur place de la CNIL a été décidé à la suite du dépôt de huit plaintes entre 2013 et 2017 relatives au dispositif de vidéosurveillance et que la finalité du traitement invoqué – la sécurité des biens s'agissant de la protection des documents confidentiels à traduire – ne requiert pas que les traducteurs assermentés soient filmés en continu. Une réorientation de la caméra ou la mise en place de masques dynamiques étaient par exemple possibles.

S'agissant du manquement relatif à l'information des personnes, la formation restreinte souligne que la société a été mise à même, grâce à l'injonction formulée dans la mise en demeure, de comprendre la nécessité d'informer les salariés sur la mise en place d'un dispositif de vidéosurveillance et des mentions requises qui y avaient été expressément énumérées. Toutefois, force est de constater qu'une information satisfaisante n'a pas été délivrée aux personnes dans le délai fixé par la mise en demeure.

S'agissant du manquement relatif à la sécurité et la confidentialité des données, la formation restreinte relève que la société n'a pas remédié à l'absence de sécurisation de l'accès aux postes informatiques des salariés à l'issue du délai fixé par la mise en demeure. Ce n'est que le 10 avril 2019, comme en atteste le procès-verbal d'huissier de justice produit par la société, que celle-ci s'est mise en conformité en mettant en place un identifiant personnel et un mot de passe pour chaque salarié pour l'accès aux postes informatiques ainsi qu'à la session Windows du dirigeant. La formation restreinte relève que les démarches entreprises par la société pour assurer la sécurité des données ont été réalisées tardivement.

Enfin, la société ne s'est pas mise en conformité, à la date de la présente délibération, afin d'assurer la traçabilité des accès individuels à la boîte de messagerie professionnelle générique.

Ensuite, la formation restreinte rappelle que le § 3 de l'article 83 du Règlement prévoit qu'en cas de violations multiples, comme c'est le cas en l'espèce puisque trois manquements sont caractérisés, le montant total de l'amende ne peut excéder le montant fixé pour la violation la plus grave. Dans la mesure où il est reproché à la société un manquement à l'article 5 du Règlement, le montant maximum de l'amende pouvant être retenu s'élève à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. A cet égard, si la société fait valoir, à titre de comparaison, le montant des sanctions pécuniaires précédemment prononcées par la formation restreinte, cela est sans incidence. Il s'agit de sanctions pécuniaires prononcées avant l'entrée en application du Règlement et pour certaines, avant la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. Le plafond maximal du montant des sanctions était, dans le cas des décisions citées par la société, de 150 000 euros sous l'empire de la loi no 2011-334 du 29 mars 2011 puis de 3 millions d'euros sous l'empire de la loi pour une République numérique.

La formation restreinte souligne la pluralité des manquements en cause ainsi que leur persistance et leur gravité, en particulier s'agissant du caractère disproportionné du dispositif de vidéosurveillance. Elle tient particulièrement compte du nombre de plaintes à l'origine de la procédure de mise en demeure et de la durée dans laquelle se sont inscrits ces manquements. Elle relève également le comportement réticent de la société à prendre en compte la législation applicable à la protection des données personnelles et son manque de diligence afin de remédier aux manquements constatés, malgré les échanges effectués avec les services de la Commission depuis plusieurs années.

Toutefois, la formation restreinte tient compte des mesures que la société a prises au cours de l'instruction de la procédure de sanction pour se mettre en conformité, du fait qu'il s'agit d'une microentreprise et de sa situation financière, afin de déterminer le montant d'une amende

administrative juste et proportionnée mais qui doit également être dissuasive.

Il résulte de tout ce qui précède et de la prise en compte des critères fixés à l'article 83 du RGPD qu'une amende administrative à hauteur de 20 000 euros est justifiée et proportionnée, ainsi qu'une sanction complémentaire de publication pour une durée d'un an.

PAR CES MOTIFS

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

prononcer une injonction de mettre en conformité le traitement avec les dispositions de l'article 32 du règlement (UE) n° 2016/679 du 27 avril 2016 relatif à la protection des données,
en particulier mettre en place des mesures permettant de s'assurer que seules les personnes habilitées puissent accéder à la boîte de messagerie et que les opérations effectuées soient tracées. A cette fin, les utilisateurs se connectant à la boîte de messagerie devront être préalablement authentifiés avec un compte individuel et les accès à la messagerie générique devront faire l'objet d'une journalisation afin de garantir leur traçabilité,
assortie d'une astreinte de 200 euros par jour de retard à l'issue d'un délai de deux mois suivant la notification de la présente délibération, les justificatifs de la mise en conformité devant être adressés à la formation restreinte dans ce délai ;

prononcer à l'encontre de la société UNIONTRAD COMPANY une amende administrative d'un montant de 20 000 (vingt mille) euros ;

rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération qui sera anonymisée à l'expiration d'un délai d'un an à compter de sa publication.

Le Président

Alexandre LINDEN

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.

Nature de la délibération: SANCTION