Date de publication sur legifrance: 20/09/2018

Commission Nationale de l'Informatique et des Libertés

Délibération n°SAN-2018-009 du 6 septembre 2018
Délibération de la formation restreinte n° SAN-2018-009 du 6 septembre 2018 prononçant une sanction pécuniaire à l'encontre de la société ASSISTANCE CENTRE D' APPELS

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ, Président, M. Alexandre LINDEN, Vice-président, Mme Dominique CASTERA, Mme Marie-Hélène MITJAVILE et M. Maurice RONAI, 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 la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;
Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 45 et suivants ;
Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par le décret n° 2007-451 du 25 mars 2007 ;
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° 2016-292C du 21 octobre 2016 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 auprès de la société ASSISTANCE CENTRE D'APPELS (ACA) ;
Vu la décision de la Présidente de la Commission n° 2017-049 du 26 juillet 2017 mettant en demeure la société ASSISTANCE CENTRE D'APPELS ;
Vu la décision de la Présidente de la Commission portant désignation d'un rapporteur devant la formation restreinte, en date du 19 avril 2018 ;
Vu le rapport de Madame Marie-France MAZARS, commissaire rapporteur, notifié par porteur à la société ASSISTANCE CENTRE D'APPELS le 1er juin 2018 ;
Vu les observations écrites de la société ASSISTANCE CENTRE D'APPELS reçues le 10 juillet 2018, 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 12 juillet 2018 :

- Madame Marie-France MAZARS, Commissaire, en son rapport ;

- En qualité de représentants de la société ASSISTANCE CENTRE D'APPELS :
- En qualité de conseil de la société ASSISTANCE CENTRE D'APPELS :
- […] ;
- […] ;
- […] ;

Les représentants de la société ASSISTANCE CENTRE D'APPELS ayant pris la parole en dernier ;
A adopté la décision suivante :

I- Faits et procédure

La société ASSISTANCE CENTRE D'APPELS (ci-après la société) est une société par

actions simplifiée, dont le siège social se situe ZA de la briqueterie à SAINT JACQUES SUR DARNETAL (76160). Un établissement secondaire de l'entreprise est situé au 37, rue Gustave Eiffel à GOUSSAINVILLE (95190).
La société a une activité de télésurveillance d'ascenseurs et de parkings. Elle emploie 14 personnes, dont 13 téléopérateurs, et a réalisé en 2017 un chiffre d'affaires de 816.691 euros.
Le 21 juin 2015, la Commission nationale de l'informatique et des libertés (ci-après CNIL ou la Commission) a été saisie d'une plainte concernant la mise en place d'un dispositif de vidéosurveillance/vidéoprotection dans les locaux de la société situés 39, rue Gustave Eiffel à GOUSSAINVILLE.
En application de la décision n° 2016-292C de la Présidente de la Commission du 21 octobre 2016, une délégation de la CNIL a procédé à une mission de contrôle dans les locaux de la société le 3 novembre 2016.
Au cours du contrôle, la délégation a constaté qu'un dispositif de pointage biométrique à des fins de contrôle des horaires des salariés était mis en œuvre, sans autorisation de la CNIL. Il a également été constaté qu'un dispositif d'enregistrement des appels téléphoniques était mis en place sans que les salariés en soient informés. En outre, il a été constaté que lors d'un appel entrant, les interlocuteurs n'étaient notamment pas informés de l'identité du responsable du traitement et du droit d'opposition dont ils disposent.
De plus, la délégation de la CNIL a constaté que les mots de passe permettant d'accéder à l'environnement *Windows* et au logiciel *[…]* contenant les données enregistrées *via* le boîtier biométrique étaient composés respectivement de 9 caractères alphanumériques et de 4 caractères numériques. La délégation a constaté, d'une part, que l'accès à l'outil de gestion de la société dénommé *[…]* s'effectue *via* un mot de passe composé de 6 caractères alphabétiques et, d'autre part, une absence de verrouillage automatique des sessions sur certains postes de travail. Enfin, elle a été informée que le mot de passe d'accès au logiciel *[…]* n'avait pas été modifié depuis 2011.
Le procès-verbal de constat n° 2016-292 dressé à l'issue de cette mission a été adressé à la société par courrier du 7 novembre 2016.
Au vu des manquements relevés, la Présidente de la CNIL a mis en demeure la société, par décision n° 2017-049 du 26 juillet 2017, dans un délai de trois mois de :

- *ne collecter et traiter que de données adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs, en particulier cesser d'utiliser le dispositif biométrique de reconnaissance de l'empreinte digitale pour contrôler les horaires des salariés et supprimer toutes les données qui ont été collectées par un tel dispositif ;*
- *procéder à l'information des personnes concernées , conformément aux dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée, notamment concernant le dispositif d'enregistrement des appels téléphoniques :*
- *procéder à l'information des salariés en portant notamment à leur connaissance les mentions relatives à l'identité du responsable de traitement, la finalité du traitement, les destinataires des données issues du dispositif, la durée de conservation des données traitées ainsi que les droits des personnes concernées***, le droit d'opposition pouvant en l'espèce prendre la forme d'une désactivation de l'enregistrement ou d'un accès à une ligne téléphonique non reliée au système d'enregistrement pour l'émission d'appels personnels ou internes à la société** *;*
- *procéder à l'information des interlocuteurs en cas d'appels sortants et entrants par une mention orale en début de conversation intégrant par exemple la possibilité de s'opposer à l'enregistrement ainsi qu'un renvoi vers un site internet ou vers une touche du téléphonique pour la délivrance de l'ensemble des mentions d'information prescrites ;*

- *prendre toute mesure nécessaire pour garantir la sécurité et la confidentialité des données à caractère personnel traitées, notamment en :*
- *mettant en place une politique rigoureuse et contraignante imposant des mots de passe robustes pour l'accès à l'environnement Windows, au logiciel […] , ainsi qu'à l'outil de gestion de la société […] : les mots de passe sont composés d'au minimum 12 caractères, contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial* ou *les mots de passe sont composés d'au moins 8 caractères, contenant 3 des 4 catégories de caractères (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) et s'accompagnent d'une mesure complémentaire comme par exemple la temporisation d'accès au compte après plusieurs échecs (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (ex : captcha) et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses (au maximum 10). Dans tous les cas, les mots de passe du personnel de la société doivent faire l'objet d'un renouvellement régulier ;*
- *instaurant un verrouillage automatique par défaut des sessions des postes informatiques en cas d'inactivité prolongée de celles-ci (au bout de 10 minutes, par exemple) ;*
- *justifier auprès de la CNIL que l'ensemble des demandes précitées a bien été respecté, et ce dans le délai imparti .*

Cette décision a été notifiée à la société le 31 juillet 2017.
En l'absence de réponse à l'échéance de la mise en demeure, un courrier de relance a été adressé à la société le 20 octobre 2017 qui l'a réceptionné le 24 octobre suivant.

Par courrier daté du 20 octobre 2017, la société a répondu à la mise en demeure de la Présidente. Elle précisait que le dispositif de pointage par code n'était plus opérationnel et que les données enregistrées étaient purgées régulièrement.
Toutefois, la Présidente de la CNIL a de nouveau demandé à la société, par courrier du 21 novembre 2017, de cesser d'avoir recours à un dispositif de pointage par reconnaissance de l'empreinte digitale (et non à un dispositif de pointage par code). Elle lui a également rappelé qu'elle était tenue d'assurer l'information des personnes quant au dispositif d'enregistrement des appels téléphoniques ainsi que la sécurité des données traitées.
Le 1er décembre 2017, la société a renvoyé à la Commission sa réponse datée du 20 octobre précédant, expliquant que celle-ci et le courrier de relance de la CNIL daté du même jour s'étaient croisés.
Considérant que ce courrier ne répondait pas à la demande de compléments du 21 novembre 2017, la Présidente de la CNIL a adressé un courrier de relance à la société le 12 janvier 2018, réceptionné le 17 janvier suivant.
Le 24 janvier 2018, la société a indiqué à la Présidente que le dispositif de pointage par biométrie n'était plus opérationnel. Elle a précisé qu'une note de service informant les salariés de la mise en place d'un dispositif d'enregistrement des appels téléphoniques avait été affichée sur un panneau d'information et qu'un verrouillage automatique des sessions des postes informatiques avait été mis en place.
Afin de vérifier si les mesures annoncées par la société avaient été mises en place, une délégation de la CNIL a procédé à une mission de contrôle sur place le 29 mars 2018, en application de la décision de la Présidente de la CNIL n° 2016-292C précitée.
La délégation a constaté que le dispositif biométrique permettant le contrôle des horaires des salariés était toujours installé et qu'aucune mesure de sécurité n'avait été mise en place sur les postes de travail des salariés. En outre, la délégation a constaté qu'étaient enregistrées au sein du logiciel […] , les traces de pointage par empreinte digitale entre le 30 août 2011 et le 28 mars 2018.

De plus, s'agissant de l'enregistrement des appels, la délégation a constaté que si une note informait les salariés de l'identité du responsable du traitement, du moment de l'enregistrement, de la durée de conservation des données et de la finalité poursuivie par le traitement, celle-ci ne contenait aucune information relative aux droits des personnes.

S'agissant de l'information des interlocuteurs de la société, la délégation a constaté qu'un message d'information était diffusé pour les appels entrants mais que celui-ci peut-être tronqué lorsque l'opérateur prenait l'appel avant la fin de sa diffusion. En outre, il a été constaté qu'aucun message d'information relatif à l'enregistrement des appels n'était délivré par les opérateurs aux interlocuteurs en cas d'appels sortants.

Le procès-verbal n° 2016-292/2 du 29 mars 2018 a été adressé à la société par courrier, reçu le 4 avril suivant.
Par la suite, la société a informé la CNIL, par courrier du 13 avril 2018, qu'elle avait désigné un délégué à la protection des données et mis en place plusieurs mesures afin de répondre aux exigences de la mise en demeure. Elle précisait notamment que le boîtier biométrique de reconnaissance de l'empreinte digitale de contrôle des horaires des salariés avait été démonté et qu'un verrouillage automatique des postes de travail avait été mis en place. Elle indiquait en outre que des mesures avaient été prises afin que le message d'information délivré pour les appels entrants ne soit pas tronqué.
Considérant que les manquements constatés avaient persisté après l'expiration du délai imparti dans la mise en demeure, la Présidente de la Commission a désigné Madame Marie-France MAZARS en qualité de rapporteur, le 19 avril 2018, sur le fondement de l'article 46 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après loi Informatique et Libertés ou loi du 6 janvier 1978 modifiée).
À l'issue de son instruction, le rapporteur a fait notifier à la société ASSISTANCE CENTRE D'APPELS, le 1er juin 2018, par porteur, un rapport détaillant les manquements à la loi qu'il estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de la Commission de prononcer une sanction pécuniaire qui ne saurait être inférieure à cinquante mille (50.000) euros et qui serait rendue publique.
Était également jointe au rapport une convocation à la séance de la formation restreinte du 12 juillet 2018 indiquant à la société qu'elle disposait d'un délai d'un mois pour communiquer ses observations écrites.
Le 10 juillet 2018, la société a produit des observations écrites sur le rapport, par l'intermédiaire de son conseil, réitérées oralement lors de la séance de la formation restreinte du 12 juillet suivant.

II- 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

Le 3° de l'article 6 de la loi du 6 janvier 1978 modifiée, dans sa version applicable au jour des faits, dispose que les données à caractère personnel *sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs .*
La société a été mise en demeure, le 26 juillet 2017, de cesser d'utiliser le dispositif biométrique de reconnaissance de l'empreinte digitale pour contrôler les horaires des salariés et de supprimer toutes les données collectées par celui-ci.
Malgré sa réponse indiquant que le dispositif de pointage par biométrie n'était plus opérationnel et qu'une purge régulière des données enregistrées était effectuée, la délégation a constaté, lors du second contrôle de la CNIL du 29 mars 2018, que le boîtier biométrique n'avait pas été désinstallé, que certains salariés continuaient de l'utiliser et que des données biométriques étaient conservées sur la période du 30 août 2011 au 28 mars 2018.

Le rapporteur soutient que jusqu'au jour du contrôle du 29 mars 2018, effectué après la mise en demeure de la Présidente de la CNIL, la société avait toujours recours au dispositif biométrique à des fins de contrôle des horaires des salariés et qu'aucune circonstance exceptionnelle imposant le recours à la biométrie à cette fin n'est invoquée par la société.
En défense, la société indique que le dispositif biométrique en cause a été acquis en 2011, par l'ancien dirigeant. Elle précise que celui-ci n'était plus utilisé depuis mars 2017 et que si les empreintes des anciens salariés étaient encore reconnues par le dispositif, ceux-ci ne pointaient plus.
En outre, la société soutient que le système en cause a été démonté et détruit depuis le second contrôle de la Commission.
En premier lieu , la formation restreinte relève que la société avait mis en place un dispositif biométrique ayant pour finalité la gestion des horaires des salariés sans autorisation de la CNIL, tel que constaté par la délégation de la CNIL le 3 novembre 2016.
À cet égard, la formation restreinte note que malgré la mise en demeure de la Présidente de la CNIL du 26 juillet 2017 et le courrier du 20 octobre 2017 demandant à la société de cesser d'utiliser le dispositif biométrique en question, il ressort des constats effectués par la délégation de la Commission, le 29 mars 2018, que celui-ci était toujours installé et que les données enregistrées dans le logiciel […) , depuis le 30 août 2011, n'avaient pas été purgées.
Si la formation restreinte note que selon la société les données collectées par le dispositif biométrique n'étaient plus utilisées par le service en charge de la paie, il est néanmoins établi que certains salariés continuaient de l'utiliser et donc que des données biométriques de salariés étaient enregistrées et conservées. Au surplus, rien ne permet d'établir, comme le soutient la société, que le dispositif biométrique était utilisé par les salariés en méconnaissance de directives données par elle, la société n'ayant produit aucun document attestant de telles instructions.
En deuxième lieu , la formation restreinte rappelle que les données biométriques ont la particularité d'être uniques et permettent donc d'identifier un individu à partir de ses caractéristiques physiques ou biologiques. À ce titre, elles bénéficient d'un régime particulièrement protecteur.
La formation restreinte rappelle que, depuis 2012, la Commission exclut l'utilisation de tout dispositif biométrique à des fins de gestion des horaires des salariés. Si le recours à un dispositif biométrique, pour une telle finalité, peut faire l'objet d'une demande d'autorisation sur le fondement du 8° du I de l'article 25 de la loi du 6 janvier 1978 modifiée, le responsable du traitement doit néanmoins démontrer qu'il existe des circonstances exceptionnelles fondées sur un impératif spécifique de sécurité.
En l'espèce, la formation restreinte note que la société ne justifie d'aucune circonstance exceptionnelle imposant le recours à la biométrie pour le contrôle des horaires des salariés.
Il résulte de ce qui précède que la société a procédé à une collecte de données excessives au regard des finalités pour lesquelles elles étaient collectées.
Sur la base de ces éléments, la formation restreinte considère que le manquement au 3° de l'article 6 de la loi du 6 janvier 1978 modifié est constitué, la société ne s'étant pas conformée à la décision de la Présidente de la CNIL n° 2017-049 du 26 juillet 2017 dans le délai imparti.

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

L'article 32 de la loi du 6 janvier 1978 modifiée, dans sa version applicable au jour des faits, dispose que :
I.- La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement

ou son représentant :
1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
2° De la finalité poursuivie par le traitement auquel les données sont destinées ;
3° Du caractère obligatoire ou facultatif des réponses ;
4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ;
5° Des destinataires ou catégories de destinataires des données ;
6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre dont celui de définir des directives relatives au sort de ses données à caractère personnel après sa mort ;
7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ;
8° De la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée.
Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°.
La société a été mise en demeure de procéder à l'information des personnes relative à la mise en place d'un dispositif d'enregistrement des appels téléphoniques, conformément à l'article 32 précité.
Lors du second contrôle du 29 mars 2018, la délégation a constaté que le message d'information diffusé pour les appels entrants pouvait être tronqué lorsque l'opérateur prend l'appel avant la fin de la diffusion de celui-ci. Elle a également constaté qu'aucun message d'information relatif à l'enregistrement des appels n'est délivré par les opérateurs aux interlocuteurs en cas d'appels sortants. Il a enfin été constaté que la note d'information intitulée Enregistrement des communications téléphoniques , destinée aux salariés de la société, ne contient aucune information relative à leurs droits.
Le rapporteur a relevé que la société n'avait fourni aucun élément attestant que la note d'information destinée aux salariés avait été complétée et que le message diffusé pour les appels entrants ne pouvait être tronqué. Il précisait donc ne pas être assuré que les personnes étaient dûment informées de la mise en œuvre d'un tel dispositif, de sa finalité, de l'identité du responsable du traitement et de leur droit de s'y opposer.
En défense, la société soutient que les enregistrements des appels téléphoniques entrants sont gérés par un prestataire extérieur et qu'elle ne saurait être tenue responsable du manquement relatif au défaut d'information des personnes s'agissant des appels entrants. Elle précise avoir informé ce dernier des problématiques rencontrées par courrier du 5 avril 2018 et n'avoir obtenu satisfaction auprès de lui que le 5 juillet suivant.
La formation restreinte relève que contrairement aux affirmations de la société, il lui appartient en tant que responsable du traitement, y compris lorsqu'elle fait appel à un prestataire, de s'assurer du respect des obligations et droits prévus par la loi Informatique et Libertés et notamment qu'une information complète relative à la mise en œuvre d'un traitement soit fournie aux personnes concernées, conformément à l'article 32 de la loi précitée.
Elle relève qu'il ressort des éléments fournis par la société que les demandes de correctifs ont été envoyées au prestataire à compter du 5 avril 2018 et sont donc postérieures au second contrôle de la CNIL. La société n'avait donc pas engagé de démarche auprès de son prestataire dans le délai imparti par la mise en demeure.
La formation restreinte relève enfin que la société n'apporte aucun élément attestant que la note d'information des salariés aurait été complétée s'agissant des droits qu'ils détiennent en vertu de la loi Informatique et Libertés .
Sur la base de ces éléments, la formation restreinte considère que le manquement à l'article 32 de la loi du 6 janvier 1978 modifié est constitué, la société ne s'étant pas conformée à la décision de la Présidente de la CNIL n° 2017-049 du 26 juillet 2017 dans le

délai imparti.

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

L'article 34 de la loi du 6 janvier 1978 modifiée, dans sa version applicable au jour des faits, dispose que : *Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* .

La société a été mise en demeure de mettre en place une politique rigoureuse et contraignante imposant des mots de passe robustes pour l'accès à l'environnement Windows, au logiciel […] , ainsi qu'à l'outil […] et d'instaurer un verrouillage automatique par défaut des sessions des postes informatiques en cas d'inactivité prolongée de celles-ci.

Par courrier du 24 janvier 2018, la société a précisé qu'un verrouillage automatique des sessions des postes de travail au bout de quatre heures d'inactivité avait été mis en place.

À l'occasion du second contrôle du 29 mars 2018, la délégation de la CNIL a constaté que le poste de travail disposant du logiciel *[…]* était accessible depuis un bureau ouvert à l'ensemble du personnel et que celui-ci n'était pas verrouillé automatiquement en cas d'inactivité prolongée. Il a également été constaté que le mot de passe permettant d'afficher l'historique des évènements enregistrés dans ce logiciel était composé de 4 chiffres. De plus, la délégation a constaté que les mots de passe d'accès aux sessions des opérateurs étaient composés de 6 caractères et que les enregistrements téléphoniques étaient accessibles à l'ensemble des opérateurs téléphoniques à partir du logiciel de gestion d'appels.

La délégation a enfin constaté que les postes de travail des employés n'étaient pas verrouillés automatiquement en cas d'inactivité.

Le rapporteur soutient que l'insuffisante robustesse des mots de passe et l'absence de verrouillage automatique des sessions des postes de travail ne permettent pas d'assurer la sécurité des données traitées par la société et d'empêcher que des tiers non autorisés tels que les téléopérateurs, mais aussi des personnes appelées à intervenir dans les locaux, n'aient accès auxdites données à caractère personnel.

En défense, la société ne conteste pas les faits constatés mais minimise le risque relatif aux données à caractère personnel qu'elle traite. Elle soutient notamment que ces données ne sont ni exposées sur Internet, ni accessibles à des tiers non autorisés dès lors que ses locaux sont sécurisés et ne reçoivent pas de public. Elle indique, en outre, que les données traitées ne sont ni des données sensibles ni des informations confidentielles.

La formation restreinte relève qu'il appartient à la société ASSISTANCE CENTRE D'APPELS de mettre en œuvre des mesures de sécurité destinées à assurer la sécurité des données à caractère personnel qu'elle traite.

La formation restreinte rappelle que les postes des agents doivent être paramétrés afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité et doivent être protégés par un mot de passe suffisamment robuste. Ces dispositions sont de nature à restreindre les risques d'une utilisation frauduleuse d'une application, en cas d'absence de l'agent de son poste de travail.

Dans sa délibération n° **2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe, la Commission préconise,** lorsqu'une authentification repose uniquement sur un identifiant et un mot de passe, que le mot de passe comporte au minimum 12 caractères contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial ou comporte au moins 8 caractères,

contenant 3 de ces 4 catégories de caractères et s'accompagne d'une mesure complémentaire comme par exemple 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.
La formation restreinte relève que si la société indique avoir mis en place des mots de passe forts sur tous les postes de travail, elle n'en fournit pas la preuve. Elle note également que le verrouillage automatique des postes de travail n'a été mis en place qu'en avril 2018, soit cinq mois après l'échéance du délai de mise en conformité qui lui était accordé.
Enfin, elle rappelle que l'obligation de sécurité visée à l'article 34 de la loi Informatique et Libertés concerne toutes les données à caractère personnel et non seulement les données dites sensibles .
Sur la base de l'ensemble de ces éléments, la formation restreinte considère que le manquement à l'article 34 de la loi du 6 janvier 1978 modifié est constitué, la société ne s'étant pas conformée à la décision de la Présidente de la CNIL n° 2017-049 du 26 juillet 2017 dans le délai imparti.

4.Sur la sanction et la publicité

Aux termes du I de l'article 45 de la loi du 6 janvier 1978 modifiée, dans sa version applicable au jour des faits :
Lorsque le responsable d'un traitement ne respecte pas les obligations découlant de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut le mettre en demeure de faire cesser le manquement constaté dans un délai qu'il fixe. En cas d'extrême urgence, ce délai peut être ramené à vingt-quatre heures.

Si le responsable du traitement se conforme à la mise en demeure qui lui est adressée, le président de la commission prononce la clôture de la procédure. Dans le cas contraire, la formation restreinte de la commission peut prononcer, après une procédure contradictoire, les sanctions suivantes :
1° Un avertissement ;
2° Une sanction pécuniaire, dans les conditions prévues à l'article 47, à l'exception des cas où le traitement est mis en œuvre par l'Etat ;
3° Une injonction de cesser le traitement, lorsque celui-ci relève de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25.
Lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la formation restreinte peut prononcer, sans mise en demeure préalable, et après une procédure contradictoire, les sanctions prévues au présent I.
Les alinéas 1er et 2ème de l'article 47 de la loi précitée, dans sa version applicable au jour des faits, précisent que :
Le montant de la sanction pécuniaire prévue au I de l'article 45 est proportionné à la gravité du manquement commis et aux avantages tirés de ce manquement. La formation restreinte de la Commission nationale de l'informatique et des libertés prend notamment en compte le caractère intentionnel ou de négligence du manquement, les mesures prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées, le degré de coopération avec la commission afin de remédier au manquement et d'atténuer ses effets négatifs éventuels, les catégories de données à caractère personnel concernées et la manière dont le manquement a été porté à la connaissance de la commission.
Le montant de la sanction ne peut excéder 3 millions d'euros .
La société soutient que la formation restreinte doit tenir compte, dans la détermination de

la sanction, de la spécificité de son activité et de ses difficultés financières mais aussi des délais de réaction de ses différents prestataires l'empêchant de se mettre en conformité.
Il a été démontré que les manquements aux articles 6-3°, 32 et 34 de la loi du 6 janvier 1978 modifiée ont persisté au-delà du délai imparti par la mise en demeure de la Présidente de la Commission.
La formation restreinte considère que la gravité des manquements est caractérisée au vu de la catégorie particulière de données à caractère personnel traitées par la société. Les données biométriques en ce qu'elles sont relatives notamment aux caractéristiques physiques et biologiques - permettant l'identification ou l'authentification unique d'une personne physique - bénéficient d'un régime particulièrement protecteur.

Eu égard auxdits manquements caractérisés et à la nature des données, mais également compte tenu de la conformité partielle de la société à la loi, au jour où la formation restreinte statue, et de la situation financière de la société, la formation restreinte estime que les faits de l'espèce justifient que soit prononcée une sanction pécuniaire d'un montant de 10.000 (dix mille) euros.
En outre, au regard des manquements constitués, de leur persistance durant 15 mois, malgré les nombreuses diligences effectuées à son égard par les services de la CNIL, la formation restreinte décide de rendre publique sa décision. Elle estime nécessaire de sensibiliser les responsables de traitement aux droits et obligations issus de la loi Informatique et Libertés , en particulier, à l'importance de répondre aux demandes de la Présidente de la Commission et de mettre effectivement en œuvre les mesures requises.

PAR CES MOTIFS

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

- **prononcer à l'encontre de la société ASSISTANCE CENTRE D'APPELS une sanction pécuniaire d'un montant de 10.000 (dix mille) euros ;**

- **rendre publique sa décision, qui sera anonymisée à l'expiration d'un délai de deux ans à compter de sa publication.**

Le Président

Jean-François CARREZ

Cette décision est susceptible de 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