Le : 11/12/2019

Date de publication sur legifrance: 10/12/2019

Commission Nationale de l'Informatique et des Libertés

Décision n°MED-2019-025 du 5 novembre 2019
Décision n° MED 2019-025 du 5 novembre 2019 mettant en demeure la société BOUTIQUE.AERO

La Présidente de la Commission nationale de l'informatique et des libertés,

Vu la Convention n° 108 du Conseil de l'Europe 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 le Code pénal ;

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° 2019-015C du 20 décembre 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 auprès de la société BOUTIQUE.AERO ;

Vu le procès-verbal de contrôle n° 2019-015/1 du 20 mars 2019 ;

Vu les autres pièces du dossier ;

La société BOUTIQUE.AERO (ci-après la société), sise 6 allée Henry Potez à Blagnac (31700), est une société par actions simplifiée à associé unique spécialisée dans le secteur d'activité du commerce de gros de fournitures et équipements aéronautiques. Elle emploie 7 salariés et a réalisé un chiffre d'affaires de 1 751 700,00 € en 2017.

Le 29 octobre 2018, la direction régionale des entreprises, de la concurrence, de la consommation, du travail et de l'emploi en Occitanie (DIRECCTE) a signalé à la Commission nationale de l'informatique et des libertés (ci-après CNIL ou la Commission) la présence, dans le magasin de la société BOUTIQUE.AERO, d'un dispositif de vidéosurveillance dont certaines caméras filment en continu les postes de travail des salariés.

En application de la décision n° 2019-015C du 20 décembre 2018 de la Présidente de la Commission nationale de l'informatique et des libertés, une délégation de la CNIL a procédé à une mission de contrôle sur place auprès de la société le 20 mars 2019. La mission a notamment eu pour objet de vérifier la conformité à 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), au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le Règlement), à la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 et aux dispositions prévues par les articles L. 251-1 et suivants du code de la sécurité intérieure, de l'ensemble des traitements de données à caractère personnel mis en œuvre par la société.

À l'occasion de ce contrôle, la délégation a été informée que la société BOUTIQUE.AERO met en œuvre, depuis 2010, un dispositif de vidéosurveillance comportant quatorze caméras dans sa boutique de vente de produits aéronautiques.

La délégation a constaté que :
- trois caméras (X1, E1, R3) étaient désactivées au jour du contrôle ;
- huit caméras (B2, B3, B4, B6, B7, B5, R2, R1) filmaient l'espace de vente ouvert au public ;
- deux caméras (B1 et E1) filmaient en continu un poste de travail correspondant à la caisse du magasin et à un emplacement pour la préparation de commandes, non ouvert au public ;
- une caméra (C1) filmait une zone non ouverte au public correspondant à un couloir desservant plusieurs bureaux de salariés.

La société a informé la délégation qu'elle avait effectué une demande d'autorisation préfectorale pour l'installation du dispositif le 10 février 2019.

Elle a précisé que la finalité du traitement consiste à prévenir les atteintes aux salariés et aux biens ainsi qu'à localiser les salariés.

Elle a également informé la délégation qu'aucun registre des traitements n'était tenu.

La délégation a relevé que les images des caméras de vidéosurveillance étaient accessibles en temps réel depuis une connexion au logiciel de gestion accessible, en interne et également en externe, à partir de l'URL […]. Les personnes habilitées pour accéder aux images sont le gérant de la société ainsi que l'ensemble des salariés. L'accès peut se faire à partir de chaque poste informatique du magasin au moyen de mots de passe préenregistrés depuis un compte générique et un compte individuel. Il peut se faire également depuis une connexion à partir d'un poste informatique extérieur au moyen de ses identifiants.

Les images vidéo des caméras sont accessibles par les salariés de la société par le biais de la connexion au logiciel de gestion, y compris depuis l'extérieur du réseau informatique interne de la société.

La délégation a constaté que l'accès au logiciel susmentionné est effectué à partir d'un protocole http.

La société a également informé la délégation que le prestataire en charge de la maintenance informatique a connaissance des identifiants de connexion à ce logiciel et peut accéder aux images à distance.

Par ailleurs, la société a indiqué à la délégation que l'information relative à la présence d'un dispositif de vidéoprotection était délivrée aux salariés par une mention inscrite dans leur contrat de travail.

Un manquement à l'obligation de collecter des données adéquates, pertinentes et limitées

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)* .

D'une part, la société a informé la délégation qu'elle mettait en œuvre le dispositif de vidéosurveillance notamment aux fins de localisation des salariés.
En effet, le gérant de la société a indiqué à la délégation qu'il souhaitait être en mesure de localiser les salariés lorsqu'il n'était pas sur place. Il a précisé consulter les images à distance depuis son domicile. La délégation a en effet constaté qu'il était possible de se connecter au logiciel de gestion de la société depuis l'extérieur du réseau interne afin de consulter les images de vidéosurveillance.

En particulier, la délégation a constaté que la caméra dénommée Entrepôt Stock (E1) permet la visualisation d'un emplacement de travail non ouvert au public pour la préparation de commandes.

Ce dispositif de vidéosurveillance conduit à placer le salarié occupant le poste concerné sous surveillance permanente.

Si l'utilisation du dispositif vidéo à des fins de prévention des atteintes aux biens et aux personnes peut être considérée comme légitime, tel n'est pas le cas de la localisation des salariés par le gérant à des fins de surveillance. La Commission considère avec constance que les employés ont droit au respect de leur vie privée sur leur lieu de travail. Or le placement sous surveillance permanente des salariés à des fins de localisation est attentatoire à leur vie privée. Ainsi le fait de filmer en continu le poste de travail d'un salarié est disproportionné, sauf circonstance particulière 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.

En l'espèce, le responsable de traitement ne fait état d'aucune circonstance particulière telle que des vols, dégradations ou agressions de nature à justifier la mise sous surveillance constante de salariés à des fins de localisation. Un tel dispositif constitue une ingérence dans la vie privée des salariés sur leur lieu de travail et porte atteinte à leur liberté individuelle.

Au demeurant, l'article L. 1121-1 du Code du travail prévoit à cet égard 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* .

Ces faits constituent un manquement aux obligations de l'article 5-1 c) du Règlement.

Un manquement à l'obligation d'informer les personnes

L'article 13 du Règlement exige du responsable de traitement qu'il fournisse, au moment où les données sont collectées, les informations relatives à son identité et ses coordonnées, celles du délégué à la protection des données, les finalités du traitement et sa base juridique, les destinataires des données à caractère personnel, le cas échéant les transferts de données à caractère personnel, la durée de conservation des données à caractère personnel, les droits dont bénéficient les personnes ainsi que le droit d'introduire une réclamation auprès d'une autorité de contrôle.

La délégation a constaté qu'aucune information spécifique n'est délivrée aux salariés concernant la mise en place du dispositif vidéo qui conduit à collecter et traiter leurs données à caractère personnel.
En effet, l'information qui leur est délivrée dans leur contrat de travail ne porte que sur la présence du dispositif de vidéoprotection à des fins de protection contre le vol. En particulier, le contrat de travail du salarié, qui est filmé de manière continue dans une zone non ouverte au public, contient la mention suivante : *M. X reconnaît avoir été informé que les établissements et locaux de l'entreprise sont placés sous vidéo-protection et qu'il est du devoir de chacun d'utiliser ce dispositif pour lutter contre le vol et signaler tout fait anormal* .
Le contrat de travail ou un éventuel document annexé à ce dernier ne contient pas l'ensemble des mentions d'information prévues par l'article 13 du Règlement.
Ces faits constituent un manquement aux obligations de l'article 13 du Règlement.

Un manquement à l'obligation de veiller à la sécurité des données personnelles traitées par un sous-traitant

L'article 28 du Règlement prévoit que le traitement effectué par un sous-traitant pour un responsable de traitement est régi par un contrat qui prévoit, notamment, que le sous-traitant *ne*

traite les données à caractère personnel que sur instruction documentée du responsable de traitement et qu'il *veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité* .

La société a informé la délégation que le prestataire informatique a connaissance, pour les besoins de ses missions, des identifiants de connexion au logiciel de gestion de la société et peut accéder aux images vidéo à distance.

La délégation a constaté que la société n'a pas conclu de contrat avec le prestataire en charge de la maintenance informatique comportant les obligations contenues à l'article 28 du Règlement.

La relation entre la société et le prestataire informatique n'est donc encadrée par aucune clause contractuelle garantissant la sécurité et la confidentialité des données par le prestataire ni de clause relative à l'obligation pour le prestataire de n'agir que sur instruction de la société.

Ces faits constituent un manquement aux obligations de l'article 28 du Règlement.

Un manquement à l'obligation d'établir un registre des activités de traitement

L'article 30.1 du Règlement prévoit que le responsable de traitement tient un registre des activités de traitement effectuées sous sa responsabilité qui doit comporter les informations relatives :

- aux nom et coordonnées du responsable de traitement,
- aux finalités du traitement,
- à une description des catégories de personnes concernées et des catégories de données à caractère personnel,
- aux catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales,
- aux délais prévus pour l'effacement des catégories de données,
- à une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32 paragraphe 1.

L'article 30 précise que ces obligations ne s'appliquent pas à une entreprise comptant moins de 250 employés, sauf si le traitement n'est pas occasionnel.

La société a informé la délégation qu'elle ne tenait aucun registre des activités de traitement effectuées sous sa responsabilité.

Or la délégation a constaté qu'au jour du contrôle la société utilise depuis 2010 un dispositif vidéo dans sa boutique afin de localiser les salariés, de prévenir les atteintes aux salariés et aux biens. Elle réalise à ce titre un traitement de données à caractère personnel qui n'est pas occasionnel.

Ces faits constituent dès lors un manquement aux obligations de l'article 30 du Règlement.

Un manquement à l'obligation d'assurer la sécurité et la confidentialité des données

L'article 32 du Règlement dispose notamment que *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* .

<u>En premier lieu</u>, la délégation a constaté que l'ensemble des salariés peut, à partir de la connexion au logiciel de gestion de la société, accéder aux images filmées des caméras en direct.

Tous les salariés peuvent ainsi accéder aux images vidéo alors que l'accès à ces données n'est pas strictement nécessaire à l'accomplissement de leurs missions.

Or la société doit définir des profils d'habilitation afin de limiter les accès des utilisateurs aux seules données dont ils ont besoin, l'ensemble des salariés n'ayant pas à accéder aux images vidéo en temps réel.

En deuxième lieu, la délégation a également constaté que la connexion au logiciel de gestion peut se faire à partir de chaque poste informatique du magasin, après s'être connecté à un compte générique puis un compte individuel.

Or les mots de passe et identifiant des comptes génériques et individuels sont pré-enregistrés et automatiquement complétés.

Tout utilisateur peut donc accéder aux postes informatiques et à la connexion au logiciel de gestion de la société sans authentification préalable, le pré-enregistrement des mots de passe et identifiants équivalant à une absence de mot de passe et d'identifiants.

Par conséquent, l'authentification des utilisateurs n'est pas assurée ce qui peut conduire des tiers non autorisés à accéder à des données personnelles, telles que les images vidéo.

En troisième lieu, la délégation a constaté que la connexion au logiciel de gestion de la société se fait sans chiffrement via le protocole http.

L'accès aux images vidéo des caméras par la connexion au logiciel de gestion de la société repose sur une connexion non chiffrée, qui permet la lecture en clair des flux contenant des données personnelles transmis entre l'utilisateur et le serveur hébergeant le site. La mise en place d'un protocole de chiffrement est donc destinée à assurer la sécurité des données personnelles lors des flux transmis entre l'utilisateur et le serveur hébergeant le site.

L'ensemble de ces faits constitue un manquement aux obligations de l'article 32 du Règlement.

- Sous un délai de dix (10) jours à compter de la notification de la présente décision, **et sous réserve des mesures qu'elle aurait déjà pu adopter, de :**

- **cesser de traiter les images issues du dispositif vidéo à des fins de localisation des salariés et ne traiter que des données pertinentes, adéquates et limitées à ce qui est nécessaire au regard des finalités de protection des biens et des personnes dans les conditions prévues à l'article 5-1 du règlement (UE) 2016/679 ;** en particulier adapter le dispositif vidéo déployé afin de ne pas filmer en continu les salariés sur leur poste de travail, par exemple en supprimant ou réorientant les caméras ;

- **prendre toute mesure de sécurité pour l'ensemble des traitements de données à caractère personnel mis en œuvre dans les conditions prévues à l'article 32 du règlement (UE) 2016/679 ,** en particulier pour l'accès aux flux vidéo des caméras, de manière à préserver la sécurité de ces données et empêcher que des tiers non autorisés y aient accès, notamment :
- s'agissant de l'accès en interne via le logiciel de gestion de la société, en restreignant la connexion à celui-ci à des comptes individuels au moyen d'un identifiant et d'un mot de passe qui ne soient pas pré-enregistrés ;
- en définissant des habilitations pour accéder aux flux vidéo aux seules personnes pour lesquelles cela est strictement nécessaire à l'accomplissement de leurs missions ;
- en sécurisant la connexion au logiciel de gestion de la société via l'utilisation d'un protocole de chiffrement (par exemple HTTPS).

- Sous un délai de deux (2) mois à compter de la notification de la présente décision, **et sous réserve des mesures qu'elle aurait déjà pu adopter, de :**

- **établir un registre des activités de traitement** comprenant l'ensemble des informations prévues à l'article 30 du règlement (UE) 2016/679 ;

- **procéder à l'information des personnes concernées, conformément aux dispositions des articles 12 et 13 du règlement (UE) 2016/679**, notamment en portant à la connaissance des salariés les informations relatives au dispositif vidéo par exemple, au sein d'un document annexé au contrat de travail ou par le biais d'une note de service qui leur sera remise contre émargement ou au sein du règlement intérieur mis à jour ;

- **établir un contrat ou un autre acte juridique au titre du droit de l'Union ou du Code civil avec la société de prestation informatique,** qui régit les traitements de données à caractère personnel réalisés par cette dernière et comporte l'ensemble des mentions visées à l'article 28-3) du règlement (UE) 2016/679 ;

- **justifier auprès de la CNIL que l'ensemble des demandes précitées a bien été respecté, et ce dans les délais impartis.**

À l'issue de ces délais, si la société BOUTIQUE.AERO s'est conformée à la présente mise en demeure, il sera considéré que la présente procédure est close et un courrier lui sera adressé en ce sens.

À l'inverse, si la société BOUTIQUE.AERO ne s'est pas conformée à la présente mise en demeure à l'issue des délais respectifs, un rapporteur sera désigné qui pourra demander à la formation restreinte de prononcer l'une des mesures correctrices prévues par l'article 20 de la loi du 6 janvier 1978 modifiée.

La Présidente

Marie-Laure DENIS