

Date de publication sur legifrance: 24/07/2018

Commission Nationale de l'Informatique et des Libertés

Décision n°MED-2018-024 du 2 juillet 2018

Décision n° MED-2018-024 du 2 juillet 2018 mettant en demeure la société « Institut des techniques informatiques et commerciales »

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 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, abrogée par 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 son article 45 ;

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 ;

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° 2018-027C 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 auprès de l'Institut des techniques informatiques et commerciales ;

Vu le procès-verbal de contrôle n° 2018-027 du 15 février 2018 ;

Vu la saisine n°17002291 ;

Vu les autres pièces du dossier ;

1. Les faits constatés

L'Institut des techniques informatiques et commerciales (ci-après l'ITIC ou la société) est une SARL sise 190 bis boulevard de Charonne et créée en 1986. C'est une école privée d'enseignement supérieur qui délivre des formations de niveau bac +2 à bac +5 dans le secteur économique tertiaire (comptabilité, informatique, ressources humaines, commerce, etc.).

L'école compte entre 600 et 800 étudiants inscrits chaque année et emploie entre 10 et 15 salariés (personnel administratif), outre 60 enseignants intervenants. Elle a réalisé un chiffre d'affaires d'environ [...] euros en 2016, pour un résultat en bénéfice d'environ [...] euros.

Les locaux de l'entreprise sont répartis sur deux sites : 190 bis boulevard de Charonne et 133 boulevard de Charonne (salle de cours, cafétéria, bureaux administratifs).

En application de la décision n° 2018-027C du 2 février 2018 de la Présidente de la Commission nationale de l'informatique et des libertés (ci-après CNIL ou la Commission), une délégation de la CNIL a procédé à une mission de contrôle sur place auprès des deux sites de l'ITIC le 15 février 2018. La mission a notamment eu pour objet de vérifier la conformité à la loi du 6 janvier 1978 modifiée (ci-après Loi informatique et libertés) de l'ensemble des traitements de données à caractère personnel mis en œuvre par la société.

La délégation a constaté que vingt-quatre caméras ont été installées dans les locaux de la société situés 190 bis boulevard de Charonne, filmant notamment des bureaux, les salles de cours, les salles de vie commune et la cour de la copropriété. Seize caméras ont été installées dans les locaux de la société situés 133 boulevard de Charonne, filmant notamment la cafétéria et les salles de cours. Les caméras sont fixes, filment en couleur sans prise de son et sur détection de mouvement.

Le dispositif de vidéosurveillance a été déclaré à la CNIL le 12 mai 2009 sous le numéro 1361738.

La délégation a constaté qu'un panneau d'information relatif à la vidéosurveillance était installé à l'entrée des locaux sis 190 bis boulevard de Charonne et qu'aucun panneau n'était apposé au 133 boulevard de Charonne, ni dans la cour de la copropriété du 190 bis boulevard de Charonne. Le directeur de la société a également informé la délégation que les élèves sont informés de la présence d'un système de vidéosurveillance par le biais des conditions générales jointes au contrat d'inscription. Les salariés (personnel administratif et enseignants) ne font l'objet d'aucune information particulière relative au système de vidéosurveillance.

Il a été constaté que les images issues des systèmes de vidéosurveillance sont enregistrées et peuvent être consultées, en direct ou non, depuis le bureau de la direction pour les caméras du 190 bis boulevard de Charonne, et depuis le bureau du personnel administratif pour les caméras du 133 boulevard de Charonne. La délégation a également constaté que l'accès au logiciel de visionnage ne nécessite aucun mot de passe pour se connecter au compte administrateur du logiciel. Elle a également été informée que la session Windows du poste de travail du directeur ne nécessite pas de mot de passe et n'est jamais déconnectée.

À l'occasion de son contrôle, la délégation a constaté la présence d'enregistrements issus de la vidéosurveillance remontants au 28 décembre 2017.

2. Les manquements au regard des dispositions de la loi du 6 janvier 1978 modifiée

Un manquement à l'obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données

La société a justifié la mise en œuvre de son dispositif par la protection des biens et des

personnes (vols, agressions, dégradations) et pour éviter les débordements des étudiants. Elle a également précisé à la délégation que le système de vidéosurveillance n'était pas utilisé pour effectuer une surveillance des salariés ni des étudiants.

En premier lieu, la délégation a constaté que le dispositif de vidéosurveillance installé filmait par détection de mouvement, donc en continu dès qu'une ou plusieurs personnes se trouvaient dans une pièce, l'ensemble des salles de classe (également lieu de travail des enseignants intervenants) et des lieux de vie des étudiants (caméras 1 à 14 du dispositif grande centrale et CAM 01 et 04 du dispositif petit écran).

La CNIL considère de manière constante que si des caméras peuvent filmer les accès de l'établissement (entrées et sorties) et les espaces de circulation, il est exclu de filmer les lieux de vie pendant les heures d'ouverture de l'établissement, sauf circonstances exceptionnelles non démontrées en l'espèce.

En effet, la seule évocation de deux vols par la société n'apparaît pas justifier de placer les personnes dans une situation de surveillance constante, pas plus que l'évocation de soucis de violence entre étudiants et entre des enseignants et étudiants avant la mise en place du dispositif, ces derniers n'étant étayés par aucun élément factuel (tel qu'un dépôt de plainte ou un compte rendu d'incident).

La configuration de ce dispositif conduit à lui conférer un caractère excessif en ce qu'il place les étudiants et les enseignants dans une situation de surveillance permanente.

En second lieu, la délégation a été informée que la caméra dénommée CAM 03, installée dans les locaux situés au 190 boulevard de Charonne, filmait le bureau de la responsable des inscriptions. Ce système permet également de filmer de manière continue le poste de travail d'une salariée.

Or, la CNIL considère de manière constante que le fait de filmer en continu les postes de travail de certains employés est disproportionné, sauf circonstance particulière, par exemple lorsqu'un employé manipule des fonds ou des objets de valeur ou lorsque le responsable de traitement est à même de justifier de vols ou de dégradations commises sur ces zones.

En l'espèce, la délégation a été informée que cette caméra a notamment pour objet de visionner le bureau de la responsable des inscriptions. Dans ces circonstances, la mise sous surveillance constante de la salariée n'apparaît pas justifiée et doit être considérée comme manifestement disproportionnée et excessive au regard de la finalité déclarée.

Il résulte de ce qui précède que l'ensemble de ces faits constitue un manquement aux obligations prévues au 3° de l'article 6 de la loi n°78-17 du 6 janvier 1978 qui dispose que *les données à caractère personnel collectées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs*.

Un manquement à l'obligation d'informer les personnes

En premier lieu, la délégation a constaté que les conditions générales d'inscription, annexées au contrat d'inscription signé par l'élève ou son représentant légal s'il est mineur, comprennent une mention relative à la vidéosurveillance. Elle a été informé qu'aucune information n'est en revanche communiquée au personnel administratif de l'école, pas plus qu'aux enseignants, ni dans leur contrat de travail ni dans le règlement

intérieur.

Si les conditions générales annexées au contrat d'inscription contiennent une mention relative à la vidéosurveillance, ces informations concernent le droit à l'image, donc le respect de la vie privée tel que posé par l'article 9 du Code civil.

L'article 6 des conditions générales d'inscription (intitulé Sur le droit à l'image de étudiants) indique simplement que *l'établissement est équipé de caméras utilisées dans un but de surveillance du comportement des étudiants et du respect par ces derniers du règlement intérieur* . Le reste de la clause est relatif à la cession à la société desdits droits à l'image par l'étudiant ou son représentant légal.

Les personnes concernées ne sont pas informées notamment de l'identité du responsable du traitement, des destinataires, de la durée de conservation des images ou des droits des personnes.

Il en va de même pour les employés administratifs et les enseignants, pour lesquels aucune information n'est communiquée quant au traitement de données déployé.

En second lieu, la délégation a constaté qu'aucun panneau d'information n'était apposé dans la cour de copropriété du 190 bis boulevard de Charonne, pourtant filmée en continu par la caméra CAM 06 du dispositif petit écran .

La délégation a également constaté que la signalisation de la vidéosurveillance à l'entrée des bâtiments était incomplète dans les locaux du 190 bis boulevard de Charonne, et inexistante dans les locaux du 133 boulevard de Charonne. Le panneau à l'entrée de l'école au niveau du numéro 190 bis se contente d'indiquer l'existence du système de vidéosurveillance, et le directeur de l'établissement en sa qualité de responsable du traitement.

Ces faits constituent un manquement au I de l'article 32 de la loi n°78-17 du 6 janvier 1978 modifiée, applicable au jour des constats, qui imposait de fournir à la personne concernée un certain nombre d'informations quant au traitement de données mis en œuvre et notamment l'identité du responsable de traitement, sa finalité, ses destinataires, l'indication des droit des personnes, ainsi que les données et catégories de personnes concernées.

Il est rappelé qu'en application des articles 131-41 et R625-10 du Code pénal combinés, le fait pour la personne morale responsable d'un traitement de ne pas informer, dans les conditions prévues à l'article 32 de la loi du 6 janvier 1978 modifiée, la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est puni d'une peine d'amende pouvant atteindre 7 500 €.

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

La délégation a constaté qu'un poste informatique permettait l'accès aux images en temps réel et aux images enregistrées tant dans les locaux situés 190 bis boulevard de Charonne que ceux situés 133 boulevard de Charonne. Dans ce dernier lieu, les images sont retransmises sur un écran présent dans le bureau du personnel administratif.

L'accès à la session Windows du poste informatique dans le bureau de direction situé 190 bis boulevard de Charonne n'est pas protégé par un mot de passe. La session n'est en outre jamais déconnectée. Le bureau est simplement fermé à clef en cas d'absence.

En outre, le logiciel utilisé pour la visualisation des images dans les deux locaux ne nécessite la saisie d'aucun mot de passe au démarrage et se connecte au compte administrateur (intitulé [...]) du logiciel.

L'ensemble de ces mesures ne permet pas au responsable du traitement de s'assurer de la sécurité des données, notamment d'empêcher des tiers non autorisés d'y avoir accès.

Ces faits constituent donc un manquement à l'article 34 de la loi 78-17 du 6 janvier 1978 modifiée disposant 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* .

Il est rappelé qu'en application des articles 226-17 et 131-41 du Code pénal combinés, le fait pour une personne morale de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi 78-17 du 6 janvier 1978 modifiée précitée est puni d'une peine d'amende pouvant atteindre 1 500 000 €.

Un manquement à l'obligation de respecter une durée de conservation des données

La déclaration effectuée auprès de la CNIL le 12 mai 2009 (n° 1361738) concernant ce système de vidéosurveillance indique une durée de conservation des données de 30 jours. Or, il ressort des constatations opérées que des enregistrements datés du 28 décembre 2017 étaient accessibles au jour du contrôle, donc remontant à 49 jours.

Ces faits constituent un manquement aux obligations découlant du 5° de l'article 6 de la loi du 6 janvier 1978 modifiée, applicable au jour des constats, qui prévoit que les données à caractère personnel sont conservées pendant une durée qui n'excède pas celle nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Il est rappelé qu'en application des articles 226-20 et 131-41 du Code pénal combinés, le fait pour une personne morale, de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni d'une peine d'amende pouvant atteindre 1 500 000 €.

- modifier le dispositif de vidéosurveillance afin qu'il soit proportionné au regard de la finalité poursuivie, conformément aux dispositions du c) de l'article 5 du Règlement (UE) 2016/679 désormais applicable, et en particulier :
- **cesser de filmer les salles de classe ainsi que les espaces de pause, cafétérias, et espaces autorisés pour le déjeuner** pendant les heures d'ouverture de l'école ;
- **cesser de placer des 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 CAM 03 du bureau de l'accueil ;
- 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 du Parlement européen et du Conseil du

27 avril 2016, désormais applicable, et en particulier :

- **compléter les mentions d'information** dans les conditions générales d'inscription en ajoutant notamment l'identité du responsable du traitement, la durée de conservation des données, l'indication des droits des personnes et de la manière de les exercer ;
- **informer le personnel** de l'identité du responsable du traitement, la finalité du traitement, la durée de conservation des données, l'indication des droits des personnes et de la manière de les exercer ;
- **informer toute personne, par exemple** par l'apposition de panneaux d'information à chacune des entrées des deux locaux de la société et dans la cour de copropriété, 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 chaque utilisateur soit doté d'un compte individuel** à l'utilisation du logiciel de consultation des images issues de la vidéosurveillance ;
- **mettre en place un système de verrouillage** automatique des sessions Windows au bout d'un certain temps d'inactivité ;
- **mettre en œuvre une politique de gestion des mots de passe contraignante**, tant au niveau du logiciel de consultation des images issues de la vidéosurveillance que du compte Windows des ordinateurs où sont consultables les images, selon l'une des modalités suivantes :
 - 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 ;
 - 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 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) ;
- **configurer le logiciel de vidéosurveillance et les sessions Windows** afin que les mots de passe ne soient plus enregistrés par défaut ;
- **cesser de diffuser les images** issues de la vidéosurveillance dans des locaux accessibles à l'ensemble du personnel administratif de l'école ;
- mettre en œuvre une politique de durée de conservation des données à caractère personnel conforme aux dispositions du e) de l'article 5 du Règlement (UE) 2016/679, désormais applicable, et qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées, notamment en ne conservant pas les enregistrements des images du dispositif de vidéosurveillance au-delà d'un mois ;
- justifier auprès de la CNIL que l'ensemble des demandes précitées a bien été respecté, et ce dans le délai imparti.

À l'issue de ce délai, si l'Institut des techniques informatiques et commerciales s'est conformé 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 l'Institut des techniques informatiques et commerciales ne s'est pas conformé à la présente mise en demeure, un rapporteur sera désigné qui pourra demander à la formation restreinte de prononcer l'une des sanctions prévues par l'article 45 de la loi du 6 janvier 1978 modifiée.

La Présidente

Isabelle FALQUE-PIERROTIN