CNIL

Décision n° 2013-029 du 12 juillet 2013
mettant en demeure la SAS BRESSE DIS qui exploite l'enseigne « E. LECLERC » à BOURG-EN-BRESSE

(N°131034/1)

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 de 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 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° 2006-147 du 23 mai 2006 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2012-363C du jeudi 8 novembre 2012 de la présidente de la Commission nationale de l'informatique et des libertés de procéder à une mission de contrôle auprès de la société SAS BRESSE DIS ;

Vu le procès-verbal de contrôle n° 2012-379 du 14 novembre 2012 ;

Vu la plainte n° 12022741 parvenue à la Commission le 19 juillet 2012 ;

Constate les faits suivants :

La société par actions simplifiée BRESSE DIS (ci-après « la société ») exploite un centre commercial de 6 500 m² sous l'enseigne « E. LECLERC » à Bourg-en-Bresse (ci-après « le centre commercial »). Ce centre, ouvert le 29 septembre 2010, est composé de deux ilots distants de 200 mètres. Le premier comprend notamment un hypermarché LECLERC ainsi qu'une galerie marchande de 38 boutiques et le second un espace multimédia de la même enseigne ainsi qu'une galerie marchande de 8 boutiques.

Le centre commercial compte approximativement 230 salariés.

En 2010, il a réalisé un chiffre d'affaires annuel de plus de 47 millions d'euros pour un résultat net supérieur à 700 000 euros.

La Commission nationale de l'informatique et des libertés (ci-après « CNIL » ou « la Commission ») a été saisie le 19 juillet 2012 d'une plainte qui dénonçait notamment la surveillance de certains salariés à l'aide des caméras implantées dans le centre commercial.

Par courrier du 20 septembre 2012, la Commission a indiqué au responsable du traitement le cadre légal permettant la mise en œuvre de dispositifs de vidéosurveillance et de vidéoprotection, notamment en matière de finalité, d'information des personnes et de sécurité des données.

Le centre commercial a précisé par courrier du 2 octobre 2012 que les images étaient conservées sur un support sécurisé pendant 15 à 20 jours, qu'elles n'étaient visibles que par le personnel de sécurité et par la direction et que des affichettes informant le public étaient apposées à chaque entrée du magasin.

En application de la décision n° 2012-363C du jeudi 8 novembre 2012 de la Présidente de la Commission nationale de l'informatique et des libertés, une délégation de la CNIL a procédé à un contrôle dans les locaux du centre commercial le 14 novembre 2012.

La délégation s'est notamment attachée à examiner les traitements de vidéosurveillance et de vidéoprotection. Elle a été informée que le centre commercial était équipé d'environ 180 caméras parmi lesquelles environ 130 filment des espaces ouverts au public tels que les lignes de caisse, les rayons de l'hypermarché, la galerie marchande, le parking ou la station de carburant.

53 autres caméras, filment en permanence des espaces non ouverts au public comme les réserves de l'hypermarché, les bureaux administratifs ou le poste de sécurité. Certaines d'entre elles permettent notamment de filmer des postes de travail, ainsi que les accès à certains bureaux, aux vestiaires d'une partie du personnel, au cabinet médical, aux salles de pause et aux sanitaires réservés aux employés.

Les finalités de ce dispositif, telles qu'indiquées par le responsable des lieux lors du contrôle sont la prévention des atteintes aux biens et aux personnes ainsi que la protection contre les incendies ou les accidents.

Les images des 180 caméras sont accessibles, en temps réel depuis les deux postes de sécurité du centre commercial, situés dans chacun des îlots ainsi que depuis les bureaux du président directeur général de la société et du directeur du centre commercial. Les enregistrements des images ne sont en revanche accessibles que depuis le poste de sécurité du premier îlot.

La délégation a également constaté que le directeur du centre commercial et son épouse (chef de rayon du centre commercial) avaient la possibilité de visionner les images depuis leur smartphone.

Au jour du contrôle, le centre commercial conservait 346 extractions vidéo de son dispositif, relatives notamment à des accrochages sur son parking, des chutes, des vols à l'étalage, des clients suspects, des altercations ou des employés.

Le centre commercial met également en œuvre un dispositif de « vidéoscanning » destiné à lutter contre la démarque inconnue. Ce dispositif, qui a fait l'objet d'une déclaration à la CNIL, se compose d'une caméra filmant les mains et la posture de l'hôte(sse) de chacune des

30 caisses. Couplé à l'édition du ticket de caisse, il permet de lutter contre la démarque inconnue et de lever, *a posteriori*, un éventuel doute quant aux articles scannés par les hôtes(sse)s de caisse ou au rendu monnaie.

Sur la qualification de ces faits au regard de la loi du 6 janvier 1978 modifiée

Un manquement à l'obligation d'accomplir les formalités préalables à la mise en œuvre du traitement

A l'exception du système de « vidéoscanning », la société n'a procédé à aucune déclaration auprès de la CNIL concernant le dispositif de vidéosurveillance installé dans les locaux du centre commercial.

Cela caractérise un manquement aux dispositions du chapitre IV de la loi « Informatique et Libertés » qui prévoit l'accomplissement de formalités préalables auprès de la CNIL avant la mise en œuvre d'un traitement automatisé de données à caractère personnel.

En particulier, le traitement de vidéosurveillance aurait dû faire l'objet d'une déclaration à la CNIL en application de l'article 22-I de la loi précitée.

Ces faits sont également réprimés par les articles 121-2, 131-13, 131-41 et 226-16 du code pénal combinés qui punissent d'une peine d'amende pouvant atteindre 1 500 000 euros le fait pour une personne morale, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi.

Un manquement à l'obligation de traiter les données de manière compatible avec les finalités pour lesquelles elles ont été collectées

La CNIL considère que les dispositifs de vidéosurveillance ne peuvent être mis en œuvre de manière légitime qu'à des fins de protection des biens et des personnes. Ces finalités sont d'ailleurs celles annoncées par le responsable des lieux lors du contrôle et corroborées par le règlement intérieur de la société dans lequel il est indiqué que des caméras sont installées *« pour des raisons de sécurité »*.

Le visionnage des séquences vidéo extraites du dispositif permet toutefois de constater que les images sont utilisées à d'autres fins que la protection des biens et des personnes. Plusieurs séquences concernent en effet des employés en train de pointer lors de prise de fonction et/ou lors de leur sortie de l'établissement.

Interrogé sur la conservation d'un de ces enregistrements, le responsable des lieux a indiqué à la délégation que cette séquence vidéo était conservée car l'employé filmé avait pointé pour sa sortie de l'établissement après avoir fait ses courses dans le magasin.

Il est par conséquent avéré que le dispositif de vidéosurveillance ne vise pas exclusivement à protéger les biens et les personnes et qu'il est également utilisé à des fins de contrôle des horaires des salariés, ce qui constitue un détournement de finalité au sens de l'article 6-2° de la loi « Informatique et Libertés ».

Cette disposition précise en effet que *« les données sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ».*

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

L'article 6-3° de la loi n° 78-17 du 6 janvier 1978 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 ».*

Il ressort du procès-verbal de contrôle que le dispositif de caméras mis en œuvre au sein du centre commercial conduit à une collecte de données excessives et non pertinentes.

En premier lieu, cette société employant approximativement 230 salariés met en œuvre un dispositif comportant 240 caméras dont environ 180 sont destinées à la surveillance des locaux (les 60 autres concernent le dispositif de « vidéoscanning » installé à chacune des caisses de l'hypermarché).

Par leur nombre et leurs emplacements ces caméras permettent de couvrir la quasi-totalité des locaux de l'entreprise, ce qui conduit à mettre sous surveillance permanente les salariés. A cet égard, l'installation de caméras dans les couloirs de la partie administrative de l'établissement permet de connaître toutes les allées et venues des employés du magasin dans cette zone, alors même que lesdits couloirs sont dénués de biens à protéger et qu'ils ne sont accessibles qu'au personnel du centre commercial et après passage devant l'employé du standard.

Cette configuration du dispositif engendre une collecte d'images disproportionnée au regard de la finalité du dispositif.

En deuxième lieu, la Commission considère de manière constante que le fait de filmer en continu les postes de travail de certains salariés est disproportionné, sauf circonstance particulière, par exemple lorsqu'un employé manipule des fonds en permanence.

En l'espèce, il a été constaté que les postes de travail situés dans les deux PC de sécurité entrent chacun dans le champ d'une caméra, permettant ainsi de visualiser tous les faits et gestes de l'employé chargé de visionner les images du dispositif. Une autre caméra filme en permanence le standard du centre commercial et le poste de travail qui s'y trouve. Le responsable des lieux lors du contrôle et le responsable du traitement *a posteriori* n'ont fait état d'aucune circonstance particulière permettant de justifier ces mises sous surveillance constante.

En troisième lieu, des caméras permettent de filmer les accès à certains locaux réservés aux salariés, tels que leurs bureaux, les toilettes, les vestiaires, le cabinet médical ou les salles de pause, ainsi que l'accès aux locaux du comité d'entreprise. Le placement sous surveillance de ces accès n'apparait pas pertinent au regard des finalités du traitement.

Enfin, la délégation a constaté la présence d'un nombre important de séquences vidéo extraites du dispositif. Plusieurs de ces séquences concernent des employés du centre commercial ou de ses prestataires alors même que leur visualisation ne révèle aucun comportement de nature à porter atteinte aux biens ou aux personnes. La conservation de ces extractions n'est donc pas pertinente au regard des finalités du dispositif.

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

Il a été constaté à l'occasion du contrôle que le centre commercial conserve toutes les extractions vidéo issues de son dispositif de vidéosurveillance sans limitation de durée. La délégation a notamment constaté la présence de 346 séquences dont la plus ancienne date du 22 décembre 2010, soit moins de trois mois après l'ouverture du centre commercial.

Cette absence de définition d'une durée de conservation des données est contraire aux dispositions de l'article 6-5° de la loi n° 78-17 du 6 janvier 1978 qui dispose que *« les données à caractère personnel sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées ».*

Il appartient en conséquence au centre commercial de définir et d'appliquer à ces données une durée de conservation des extractions vidéo, laquelle doit être raisonnable au regard des finalités poursuivies.

Il est rappelé qu'en application des articles 121-2, 131-37, 131-38 et 226-20 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 de 1 500 000 € d'amende.

Un manquement à l'obligation d'informer les personnes

Il résulte du procès-verbal qu'au jour du contrôle, les salariés étaient informés du dispositif de vidéosurveillance par une mention insérée dans le règlement intérieur de la société.

Cette mention est la suivante : « *Des caméras sont installées dans le magasin, les réserves et la cour de service pour des raisons de sécurité, l'entreprise présentant des risques particuliers de vols* ».

Cette mention n'est pas conforme aux dispositions de l'article 32 de la loi du 6 janvier 1978, lequel fait obligation au responsable du traitement de fournir à la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant des informations sur son identité, la finalité de ce traitement, le caractère obligatoire ou facultatif des réponses, les destinataires, les droits d'accès, de rectification et, le cas échéant, d'opposition aux données les concernant ainsi que des transferts de données envisagés à destination d'un Etat non-membre de la Communauté européenne.

En l'espèce, les destinataires des données ainsi que les droits reconnus aux personnes concernées en application des articles 38 à 40 de la loi « Informatique et Libertés » (droits d'accès, d'opposition et de suppression notamment), ne sont donc pas portés à la connaissance des salariés du centre commercial.

Le responsable des lieux a cependant indiqué lors du contrôle qu'une note d'information des salariés serait insérée dans les enveloppes contenant les bulletins de paie du mois de novembre 2012. Il a remis à la délégation une copie de cette note qui contient le passage suivant : « *Nous vous rappelons que le site est sous vidéosurveillance déclarée auprès de la CNIL et de la Préfecture* ». Cette mention ne comporte pas d'indications relatives à la finalité du traitement, aux destinataires des données, ni aux droits d'accès, de rectification et, le cas échéant, d'opposition des personnes concernées.

Enfin, il a été constaté lors du contrôle qu'aucune affichette n'avait été apposée aux entrées du centre commercial, contrairement à ce qui avait été annoncé par courrier du 2 octobre 2012, si bien que les salariés n'avaient pu être informés par cet intermédiaire.

Il est rappelé qu'en l'application des articles 121-2, 131-13, 131-41 et R. 625-10 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, 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 euros.

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

En premier lieu, la délégation a constaté que l'accès au terminal situé dans le poste de sécurité du premier îlot n'était pas protégé par un mot de passe. Cet ordinateur permet de visualiser en temps réel les images de l'ensemble du dispositif et de procéder à des extractions de certaines images à des fins de conservation.

En deuxième lieu, la délégation a également constaté que le mot de passe permettant d'accéder au logiciel de « vidéoscanning » ne se composait que de six caractères. Or, la CNIL recommande que les mots de passe permettant d'accéder à des données à caractère personnel se composent au minimum de 8 caractères alphanumériques et qu'ils soient régulièrement soumis à renouvellement.

En troisième lieu, la délégation a été informée que l'épouse du directeur du centre commercial avait la possibilité, depuis son téléphone mobile personnel, de visualiser les images issues du dispositif. Cette personne est responsable du rayon « bazar » et n'exerce pas de fonction au sein de la direction du centre commercial.

Sauf circonstances particulières, il ne fait pas partie des attributions principales d'un chef de rayon d'assurer la sécurité des biens et des personnes se rendant dans le centre commercial. Ces fonctions sont généralement dévolues à la direction du centre ainsi qu'au personnel en charge de la sécurité.

En conséquence, sauf à justifier de circonstances particulières, l'accès aux images du dispositif de vidéosurveillance doit être limité aux personnes en charge d'assurer la sécurité des biens et des personnes au sein de l'établissement et dont les fonctions nécessitent de prendre connaissance de ces images.

Ces faits constituent par conséquent un manquement à l'article 34 de la loi n° 78-17 du 6 janvier 1978 modifiée impose au responsable du traitement 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 en outre rappelé qu'en application des articles 121-2, 131-37, 131-38 et 226-17 du code pénal combinés, le fait pour une personne morale, de procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n°78-17 du 6 janvier 1978 précitée est puni d'une amende de 1 500 000 euros.

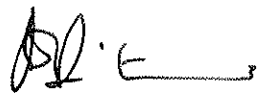
En conséquence, la SAS BRESSE DIS, sise Pôle commercial Cap Emeraude - 360 avenue du Capitaine Dhonne à BOURG-EN-BRESSE (01000) et exploitant l'enseigne « E. LECLERC » est mise en demeure, sous un délai de trois mois à compter de la notification de la présente décision, sous réserve des mesures qu'elle aurait déjà pu adopter à la suite du contrôle effectué dans ses locaux, de :

- procéder aux formalités auprès de la CNIL concernant la mise en œuvre du traitement relatif à la vidéosurveillance, sauf à renoncer à cette mise en œuvre ;
- cesser d'utiliser le dispositif de vidéosurveillance à des fins autres que celles de protection des biens et des personnes, notamment pour contrôler les horaires ou l'activité des salariés ;
- ne plus filmer : l'accès des bureaux du personnel, les postes de travail des employés chargés de visionner les caméras dans les PC de chacun des îlots et de l'agent d'accueil, l'accès aux toilettes réservées aux seuls salariés, la porte d'accès aux locaux du comité d'entreprise, l'accès aux vestiaires d'une partie du personnel, l'accès au cabinet médical réservé aux salariés du centre ainsi que l'accès aux salles de pauses. Sur ce point, la mise en conformité peut, par exemple, résulter de la réorientation des caméras ou du masquage des zones concernées ;
- ne plus effectuer d'extractions d'images du dispositif de vidéosurveillance qui aboutiraient à une collecte excessive de données concernant notamment certains salariés du centre commercial et certains salariés de la société ;
- limiter à 30 jours au maximum la durée de conservation des enregistrements de vidéosurveillance et procéder, sauf nécessité liée à la gestion d'un contentieux en cours, à la purge des enregistrements dépassant cette durée de conservation ;
- informer les salariés des conditions prévues par l'article 32 de la loi du 6 janvier 1978 modifiée ;
- instaurer un mot de passe d'au moins 8 caractères alphanumériques et régulièrement renouvelé afin d'accéder à l'ordinateur du PC de sécurité du premier îlot ainsi qu'au logiciel relatif au « vidéoscanning » ;
- limiter l'accès aux images aux personnes en charge de la sécurité des biens et des personnes et dont les fonctions nécessitent cet accès ;
- 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 la SAS BRESSE DIS s'est conformée à la présente mise en demeure, il sera considéré que la procédure est close et il lui sera adressé un courrier en ce sens.

À l'inverse, s'il est constaté que la société ne s'est pas conformée à la présente mise en demeure, un rapporteur pourra être désigné et demander à la formation restreinte de la Commission de prononcer l'une des sanctions prévues par l'article 45 de la loi du 6 janvier 1978 modifiée.

La Présidente



Isabelle FALQUE-PIERROTIN