Vidéosurveillance des salariés dans l'entreprise : une atteinte par nature disproportionnée aux droits de la personne

par *Manuela GRÉVY,* Maître de conférences à l'Institut des Sciences sociales du travail de Sceaux - Université Paris I Panthéon-Sorbonne

PLAN

Alors que l'usage de la vidéosurveillance (1) dans les lieux publics suscite quelques débats (2), tel n'est pas le cas dans les entreprises. Pourtant les enjeux y sont plus aigus encore. Parce que le système est mis en oeuvre par une personne privée et non une autorité publique, parce qu'encore, il est utilisé dans un rapport de subordination, parce qu'enfin, lorsque la vidéosurveillance est permanente, le salarié ne peut échapper à l'œil de la caméra (3).

La vidéosurveillance n'est pas un mode anodin, banal, de surveillance et de contrôle des salariés. Par nature, il s'agit dans les relations de travail d'une technique de défiance. Surtout, plus peut-être que toute autre technologie, « *l'assimilation naturelle de la caméra à l'œil attire sur la vidéosurveillance une forte charge symbolique* » (4). L'enregistrement du salarié dans ses faits et gestes, singulièrement lorsqu'il est continu, menace en effet celui-ci dans son identité, dans son intimité. Par sa prégnance, par sa technique même qui exclut l'erreur et l'oubli (5), contrairement à la surveillance humaine, la vidéosurveillance est un monstre froid qui met à nu le salarié.

Dès lors, la singularité de ce mode de surveillance et de contrôle oblige à s'interroger sur sa licéité même dans les relations de travail. De ce point de vue, le silence de la Cour de cassation est assourdissant. C'est tout l'intérêt d'une décision récente de la Commission nationale de l'informatique et des libertés (CNIL) qui, à l'occasion d'une plainte relative aux conditions d'installation et d'utilisation d'un système de vidéosurveillance dans une entreprise, a brisé quelque peu ce silence en posant les jalons d'une telle réflexion.

I. La licéité de la vidéosurveillance, un silence jurisprudentiel assourdissant

Affirmant de manière constante que *« l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps du travail* », la Chambre sociale de la Cour de cassation considère que « *seul l'emploi de procédé clandestin de surveillance est illicite* » (6). Plus précisément, « *tout enregistrement, quels qu'en soient les*

(1) Vidéosurveillance dénommée aujourd'hui par les pouvoirs publics « vidéo protection », tentative de décharger symboliquement le procédé de sa dimension liberticide.

(2) V. notamment les réflexions menées par la Ligue des Droits de l'Homme (www.ldh-france.org) ; v. aussi 29e Rapport d'activité de la CNIL, 2008, pp. 23 et s. (www.cnil.fr).

(3) Contrairement au citoyen qui ne fait que « passer » devant le dispositif.

(4) M. Cadoux, Vidéosurveillance et protection de la vie privée, Rapport CNIL du 29 oct. 1993.

(5) Mais cette observation ne saurait dispenser d'une interrogation sur la fiabilité de ces procédés, généralement indiscutée par principe alors qu'un enregistrement est susceptible d'interprétation (selon l'angle de vue par exemple), sans oublier les possibilités de falsification ; v. en ce sens, CA Aix-en-Provence : pour écarter un enregistrement vidéo opposé au salarié dont ce dernier contestait l'authenticité, la Cour d'appel relève que *« compte tenu des possibilités de montage et de trucage qu'offre l'évolution des techniques, ce document ne présente pas des garanties suffisantes d'authenticité, d'impartialité et de sincérité concernant tant sa date que son contenu pour qu'il puisse être considéré comme probant »* (M. Grévy, "Vidéosurveillance dans l'entreprise : un mode normal de contrôle des salariés ?", Dr. Social 1995, p. 329) ; v. aussi B.Bossu, Nouvelles technologies et surveillance du salarié, RJS 8-9/01 p.663, sp. n° 18.

(6) Soc. 14 mars 2000, Bull. V, n° 101 et Soc. 16 déc. 2008, n° 07-43993 relatifs à l'écoute des conversations téléphoniques d'un salarié ; Soc. 15 mai 2001, Bull. V, n° 167 relatif à la surveillance par une société extérieure ; Soc. 22 mai 1995, Bull. V, n° 164 relatif à une filature par un détective ; en sens contraire cependant, Soc. 26 nov. 2002, Bull. V, n° 352, Dr. Ouv. 2003 p. 249 n. F. Saramito, Dalloz 2003, SC 394, obs. A. Fabre, relatif également à une filature par un détective ; sur ce dernier arrêt, cf. *infra*.

motifs, d'images ou de paroles à leur insu, constitue un mode de preuve illicite » (7). Et jusqu'alors, la Haute juridiction n'a fait qu'appliquer à la vidéosurveillance cette règle générale.

C'est ainsi que, dans un premier arrêt du 20 novembre 1991 relatif à un licenciement pour faute grave à l'appui duquel l'employeur avait produit un enregistrement vidéo, la Chambre sociale a condamné le mode de preuve à raison de son caractère clandestin au visa de l'article 9 du Code de procédure civile, mais sans réserve aucune sur la nature du dispositif employé (8). Dix ans plus tard, la Cour de cassation a, par un arrêt du 31 janvier 2001 (9), confirmé la solution en rappelant l'obligation légale d'information, des salariés d'une part (10), du comité d'entreprise d'autre part (11). En revanche, elle a écarté le grief du pourvoi qui, se fondant sur l'article L. 120-2, devenu L. 1121-1 du Code du travail, contestait la faculté pour l'employeur d'opposer un enregistrement vidéo pour établir un vol constitutif d'une faute lourde du salarié. Et elle a relevé que le système de vidéosurveillance était installé dans un entrepôt de marchandises, et « *n'enregistrait pas l'activité des salariés affectés à un poste de travail déterminé* » pour en déduire que l'employeur était libre de faire tout usage d'un tel système, y compris sans information préalable des salariés (12). Cette « extériorité » du lieu surveillé, qui n'est pas considéré *stricto sensu* comme lieu de travail et échapperait en conséquence à toute règle de protection des droits des salariés, n'est guère convaincante dès lors qu'est en même temps retenue l'opposabilité de l'enregistrement pour fonder une faute justifiant la rupture du contrat de travail d'un salarié.

Plus encore, dans un arrêt du 7 juin 2006, alors que l'employeur avait détourné un système prétendument installé pour surveiller la clientèle et utilisé dans les faits pour surveiller également les salariés, la Cour de cassation a seulement reproché aux juges du fond de n'avoir pas tiré les conséquences de la méconnaissance de l'obligation d'information et de consultation du comité d'entreprise. En effet, la Cour d'appel avait déclaré « *recevable la production d'un enregistrement du salarié effectué par l'employeur à l'aide d'une caméra de vidéosurveillance en estimant qu'il ne pouvait être sérieusement prétendu que le salarié ignorait l'existence de caméras vidéo destinées à détecter les vols perpétrés dans l'entreprise et utilisées depuis de nombreuses années, ainsi qu'il ressort de la consultation du CHSCT produite par l'employeur et annoncée par des affichettes dans le magasin* ». A tort, dès lors qu'elle avait « *constaté que le système de vidéosurveillance de la clientèle mis en place par l'employeur était également utilisé par celui-ci pour contrôler ses salariés sans information et consultation préalables du comité d'entreprise, en sorte que les enregistrements du salarié constituaient un moyen de preuve illicite* » (13). Si le respect de l'obligation préalable d'information des représentants des salariés a été ici appliqué avec rigueur, la Cour de cassation est néanmoins restée sur le seul terrain du caractère clandestin du procédé, alors que l'utilisation détournée d'un système de collecte d'informations nominatives constitue une violation du principe de finalité posé par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (cf. *infra*).

Ainsi aux yeux des magistrats de la Cour de cassation, la vidéosurveillance n'est pas attentatoire aux droits fondamentaux du salarié et, par conséquent, ne relève pas de la sphère de protection attachée à ces droits. Envisagée exclusivement au regard de sa légalité dans le droit de la preuve, la vidéosurveillance est licite si le procédé a fait l'objet d'une information des salariés et de leurs représentants, illicite si le procédé est « *clandestin et, à ce titre, déloyal* » (14).

II. La licéité de la vidéosurveillance à l'aune des principes de finalité et de proportionnalité

Rapporter la vidéosurveillance à une quelconque technique de surveillance et de contrôle des salariés ne convainc pas tant celle-ci menace le salarié dans son identité, dans son intimité la plus secrète. Or, parce qu'*« au contrat, le salarié met à la disposition de l'employeur sa force de travail mais non sa personne »* (15), celui-ci doit pouvoir exiger une certaine opacité, même aux lieux et temps de la subordination. En altérant

(7) Soc. 20 nov. 1991, Bull. V, n° 519, Dr. Ouv. 1992 p. 253 ; Ph. Waquet, Un employeur peut-il filmer à leur insu ses salariés ?, Dr. Social 1992, p. 28.

(8) Prec. note précédente.

(9) Bull. V, n° 28.

(10) Cette obligation d'information est prévue aux articles L. 1222-3 et L. 1222-4 du Code du travail.

(11) Aux termes de l'article L. 2323-32 alinéa 3 du Code du travail, *« le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés ».*

(12) Dans le même sens, Soc. 19 avril 2005, Bull. V, n° 141.

(13) Bull. V, n° 206.

(14) Soc. 16 déc. 2008, n° 07-43993 ; v. aussi Civ. II, 7 déc. 2004, Bull. II n° 447.

(15) J. Rivero, Les libertés publiques dans l'entreprise, Dr. Social 1982, p. 423.

cette opacité, la vidéosurveillance est, par nature, susceptible de porter atteinte aux droits fondamentaux de la personne. De sorte que, dans les relations de travail, la licéité d'un tel procédé ne devrait pouvoir être appréciée qu'à l'aune des exigences de protection attachée à ces droits, articulées aux articles 8 de la Convention européenne de sauvegarde des droits de l'Homme, 9 du Code civil et L. 120-2, devenu L. 1121-1 du Code du travail (16). Tandis que les deux premiers textes protègent le droit au respect de la vie privée, définie comme la *« sphère secrète »* d'où chacun a « *le pouvoir d'écarter les tiers* » (17), le dernier précise 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* ». C'est à une telle démarche qu'invite la Commission nationale de l'informatique et des libertés (CNIL) dans une délibération récente.

Dans le cadre de sa mission de veiller au respect des dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (18) qui assure la protection des personnes face aux traitements de données à caractère personnel – parmi lesquelles figure la capture de l'image –, la CNIL a envisagé la licéité d'un tel mode de surveillance et de contrôle sur le terrain de la protection attachée aux droits fondamentaux de la personne. Saisie d'une plainte à l'encontre d'une société de prêt-à-porter qui s'est vu reprocher d'avoir installé et utilisé un système de vidéosurveillance dans des conditions irrégulières, la Commission a constaté (19) que le système, constitué de vingt-trois caméras installées en 1980 et 2007, était implanté au sein des trois magasins et du siège social. Au siège social, onze caméras filmaient les lieux ouverts au public (portes d'accès, magasin situé au rez-de-chaussée et premier étage) et ceux réservés au personnel où aucune marchandise n'est stockée (couloirs, réserve, ateliers de création). Les images étaient enregistrées en continu sur un support numérique, les responsables de la société pouvant se connecter à un serveur à distance, via internet, en saisissant l'adresse IP du serveur, leur identifiant de compte et leur mot de passe, afin de les visualiser. En outre, au siège, les images filmées étaient également accessibles à partir de deux postes de supervision situés à l'accueil et dans le bureau de la direction, le logiciel de supervision étant accessible sans mot de passe sur la station de supervision de l'accueil. La CNIL a également relevé que deux serveurs étaient libres d'accès, ne comportant ni verrouillage de la porte d'accès ni verrouillage de la session. S'agissant de la durée de conservation des images, il a été relevé que le logiciel de vidéosurveillance était paramétré pour les conserver pendant sept jours. Après une mise en demeure de la société à laquelle celle-ci ne s'est pas entièrement conformée (20), la CNIL a, par une délibération en date du 16 avril 2009, rendu une décision explicitant les différents manquements et prononçant, en conséquence, une sanction (21). Outre le non-respect des dispositions relatives aux systèmes de vidéosurveillance installés dans des lieux ouverts au public (22), la CNIL a constaté que l'information délivrée aux salariés, obligation prévue à l'article 32 de la loi du 6 janvier 1978 (23), n'était pas non plus suffisante. En effet, seuls les contrats de travail conclus depuis l'installation du système mentionnaient

(16) De la même manière qu'après avoir admis qu'une filature du salarié soit un procédé licite de surveillance s'il n'est pas clandestin (!), la Cour de cassation a finalement et heureusement condamné ce mode de preuve sur le terrain des droits fondamentaux : il résulte de l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, 9 du Code civil, 9 du nouveau Code de procédure civile et L. 120-2 du Code du travail *« qu'une filature organisée par l'employeur pour contrôler et surveiller l'activité d'un salarié constitue un moyen de preuve illicite dès lors qu'elle implique nécessairement une atteinte à la vie privée de ce dernier, insusceptible d'être justifiée, eu égard à son caractère disproportionné, par les intérêts légitimes de l'employeur »* (Soc. 26 nov. 2002, prec.).

(17) J. Carbonnier, *Droit civil*, tome I, n° 71, éd. 1980.

(18) Modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004.

(19) Dans le cadre de ses prérogatives de contrôle sur les lieux.

(20) Par délibération n° 2008-155 du 29 mai 2008, la Commission a mis en demeure la société, sous un délai d'un mois, de *« procéder à l'accomplissement des formalités préalables auprès de la CNIL pour l'ensemble des traitements automatisés de données à caractère personnel mis en œuvre, en particulier le dispositif de vidéosurveillance ; prendre toutes les mesures nécessaires afin que la mise en œuvre du système de vidéosurveillance soit strictement limitée à l'objectif de lutte contre le vol, et ne conduise pas à placer les salariés sous une surveillance constante ; retirer les caméras dont la présence n'est pas justifiée par cet impératif de sécurité des lieux ; communiquer à la CNIL l'intégralité des mesures prises au sein de la société (…) visant à respecter les dispositions de l'article 32 de la loi du 6 janvier 1978 (droit à l'information de toute personne auprès de laquelle sont recueillies des données à caractère personnel) ; prendre toute mesure de nature à garantir la sécurité et la confidentialité des informations collectées dans l'ensemble des traitements mis en œuvre afin que seules les personnes habilitées de par leurs fonctions y aient accès (accès au logiciel de supervision, aux serveurs informatiques) ; justifier auprès de la CNIL que l'ensemble des demandes précitées a bien été respecté, et ce dans le délai imparti »*.

(21) Délibération n° 2009-201, reproduite ci-après p. 85, publiée sur les sites internet de la CNIL (www.cnil.fr) et de Legifrance (www.legifrance.gouv.fr) : la CNIL a prononcé une sanction pécuniaire d'un montant de 10 000 euros et, *« eu égard à la nature et à la gravité des manquements commis (…) »*, a ordonné la publication de la délibération sur les sites préc.

(22) Loi du 21 janvier 1995 modifiée.

(23) Aux termes de l'article 32 de la loi n° 78-17 du 6 janvier 1978 modifiée, le responsable du traitement est tenu d'informer les personnes concernées par le traitement, notamment de sa finalité, du caractère obligatoire ou facultatif des réponses, des destinataires des informations ainsi que de leurs droit d'accès, de rectification et, le cas échéant, d'opposition.

l'existence du système (24), tandis que les salariés dont les contrats de travail avaient été signés avant la mise en place du système de vidéosurveillance n'avaient pas été informés individuellement. La CNIL a considéré qu'en tout état de cause, même lorsqu'elle a été délivrée, l'information était en l'espèce partielle *« puisque les finalités poursuivies, les destinataires des images et les modalités concrètes de l'exercice du droit d'accès dont disposent les personnes concernées, ne sont pas indiqués »* (25).

Surtout, la CNIL a considéré que la société a méconnu « *l'obligation de veiller au caractère loyal et licite des données et de ne pas les traiter de manière incompatible avec la finalité déterminée* ».

La loi du 6 janvier 1978 affirme en effet des règles cardinales relatives à la collecte et l'utilisation de données à caractère personnel et, en particulier, définit les conditions de licéité des traitements. Aux termes de l'article 6-1° de ce texte, les données à caractère personnel doivent être « *collectées et traitées de manière loyale et licite* ». Le 2° du même article impose que ces données soient collectées pour « *des finalités déterminées, explicites et légitimes* » et ne soient pas traitées « *ultérieurement de manière incompatible avec ces finalités* ». Enfin, l'article 6-3° précise que les données doivent être « *adéquates, pertinentes et non excessives au regard des finalités (…)* ».

En l'espèce, la CNIL avait mis la société en demeure, d'une part, de prendre toutes les mesures nécessaires afin que la mise en œuvre du système de vidéosurveillance soit strictement limitée à l'objectif de lutte contre le vol et ne conduise pas à placer les salariés sous une surveillance constante et, d'autre part, de retirer les caméras dont la présence n'était pas justifiée par cet impératif de sécurité des lieux (26). La société n'avait pris aucune mesure en soutenant que toutes les caméras seraient justifiées par la « *manipulation de marchandise* » et la « *circulation libre de l'ensemble du public et du personnel* ». Seuls les bureaux du personnel administratif « *où sont installés les salariés qui occupent un poste fixe et qui n'ont pas pour vocation d'être en contact constant avec la marchandise* » ne feraient pas l'objet de vidéosurveillance.

Affirmant *« que la mise en œuvre d'un système de vidéosurveillance doit obligatoirement respecter le principe de proportionnalité et être strictement nécessaire à l'objectif poursuivi »,* la CNIL a précisé que lorsqu'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'élément à prendre en compte lors de l'installation du système* ». Or en l'espèce, *« il ressort clairement des captures d'écran (…) que, contrairement aux dires de la société, des bureaux et des postes de travail fixes situés au deuxième étage du siège social sont filmés en continu, de telle sorte que les salariés sont placés sous la surveillance constante de leur employeur »*. Et d'en déduire qu'une « *telle surveillance des employés apparaît dès lors excessive et le dispositif de vidéosurveillance n'est, dès lors, pas strictement limité à l'objectif de lutte contre le vol et conduit à placer les personnes visées sous une surveillance disproportionnée au regard de l'objectif poursuivi* » (26 bis). En conséquence, la société a méconnu les dispositions de l'article 6 de la loi du 6 janvier 1978 modifiée.

A travers cette décision, la CNIL préfigure ce que pourrait être le contrôle judiciaire de la licéité d'un système de vidéosurveillance des salariés sur le terrain des droits fondamentaux de la personne. Son raisonnement, sur le fondement des dispositions de la loi du 6 janvier 1978 (27), conduit à examiner la licéité du dispositif de vidéosurveillance au regard, d'une part, de sa finalité, d'autre part, de sa proportionnalité, rejoignant ainsi les exigences énoncées à l'article L. 120-2, devenu L. 1121-1 du Code du travail (28). Et la CNIL de préciser que ces exigences doivent s'apprécier *in concreto*, à partir d'un examen des conditions dans lesquelles fonctionne le dispositif. Pour considérer, en l'espèce, que le fait de placer des salariés travaillant dans des lieux non ouverts au public sous la surveillance constante des caméras vidéo constitue un usage disproportionné de cet instrument au regard de la finalité alléguée par la société, la lutte contre le vol.

(24) Aux termes de la clause contractuelle *« la salariée est informée qu'un système de vidéosurveillance est installé dans tous les sites de l'entreprise »*.

(25) La CNIL a en revanche considéré en l'espèce que l'entreprise, qui s'est sur ce point conformée à sa mise en demeure de prendre toute mesure de nature à garantir la sécurité et la confidentialité des informations collectées dans l'ensemble des traitements mis en œuvre afin que seules les personnes habilitées de par leurs fonctions y aient accès, n'a pas méconnu ses obligations relatives à la sécurisation des données instituées par l'article 34 de la loi n° 78-17 du 6 janvier 1978 modifiée aux termes duquel *« le responsable de 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 ait accès »*

(26) cf. *supra* note n° 20.

(26 bis) Délibération n° 2009-201 préc., reproduite page suivante.

(27) Dont il faut rappeler l'ambition affichée à l'article 1er aux termes duquel *« l'informatique (…) ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »*.

(28) Selon ce texte, *« 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 »*.

Une interrogation demeure cependant sur l'appréciation de l'exigence de proportionnalité. Cette question est en effet décisive lorsque, comme en l'espèce, la surveillance est constante, le salarié se trouvant en permanence sous l'œil de la caméra. L'enregistrement continu des faits et gestes du salarié dissipe l'intimité et met en évidence des éléments qui ne relèvent pas de la sphère professionnelle, mais ressortent de la personne, de l'identité de l'individu. Dès lors, indépendamment de la finalité poursuivie – lutte contre le vol, contrôle de l'exécution du travail…, une vidéosurveillance permanente des salariés à leur poste de travail n'est-elle pas, en raison de sa nature même, excessive, disproportionnée au regard du degré d'atteinte ainsi portée à l'identité des salariés, ceux-ci perdant toute opacité inhérente au respect de leur personne ? En ce sens (29), eu égard à la nature et au degré de l'atteinte portée aux droits de la personne par la vidéosurveillance, la disproportion née du déséquilibre entre la nécessité de cette technologie et les effets dommageables qu'elle entraîne sur la personne même des salariés devrait suffire, en elle-même, à considérer comme illicite ce mode de surveillance et de contrôle dans l'entreprise.

Manuela Grévy

(29) Et comme semble le faire la Cour de cassation en matière de filature : cf. obs. d'A. Fabre sous Soc. 26 nov. 2002, prec.

Annexe

LIBERTÉS ET DROITS FONDAMENTAUX – Vidéosurveillance – 1° Proportionnalité et finalité du dispositif – Appréciation – 2° Personnes épiées – Salariés – Information – 3° Sécurisation des données.

CNIL

Délibération n° 2009-201 du 16 avril 2009

Société Jean-Marc Philippe

II. MOTIFS DE LA DÉCISION

A. Sur le manquement à l'obligation de veiller au caractère loyal et licite des données et de ne pas les traiter de manière incompatible avec la finalité déterminée

La Commission rappelle qu'aux termes du 1° de l'article 6 de la loi n° 78-17 du 6 janvier 1978, les données à caractère personnel doivent être collectées et traitées de manière loyale et licite. Le 2° du même article dispose que ces données sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités.

Dans sa délibération n° 2008-155 du 29 mai 2008, la CNIL avait mis la société en demeure d'une part, de prendre toutes les mesures nécessaires afin que la mise en œuvre du système de vidéosurveillance soit strictement limitée à l'objectif de lutte contre le vol et ne conduise pas à placer les salariés sous une surveillance constante et d'autre part, de retirer les caméras dont la présence n'était pas justifiée par cet impératif de sécurité des lieux.

Or, la société n'avait pris aucune mesure afin de limiter la surveillance de ses employés. Dans ses observations écrites du 16 avril 2009, la société soutient que toutes les caméras seraient justifiées par la *« manipulation de marchandise »* et la *« circulation libre de l'ensemble du public et du personnel ».* Seuls les bureaux du personnel administratif *« où sont installés les salariés qui occupent un poste fixe et qui n'ont pas pour vocation d'être en contact constant avec la marchandise »* ne feraient pas l'objet de vidéosurveillance.

La Commission considère que la mise en œuvre d'un système de vidéosurveillance doit obligatoirement respecter le principe de proportionnalité et être strictement nécessaire à l'objectif poursuivi. 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'élément à prendre en compte lors de l'installation du système.

Il ressort clairement des captures d'écran faites par la délégation de la CNIL que contrairement aux dires de la société, des bureaux et des postes de travail fixes situés au deuxième étage du siège social sont filmés en continu, de telle sorte que les salariés sont placés sous la surveillance constante de leur employeur. Une telle surveillance des employés apparaît dès lors excessive et le dispositif de vidéosurveillance n'est, dès lors, pas strictement limité à l'objectif de lutte contre le vol et conduit à placer les personnes visées sous une surveillance disproportionnée au regard de l'objectif poursuivi.

En conséquence, la Commission conclut que la société ne s'est pas conformée à la mise en demeure de la CNIL et n'a pas respecté les dispositions des 1° et 2° de l'article 6 de la loi n° 78-17 du 6 janvier 1978 modifiée.

B. Sur le manquement à l'obligation d'information des personnes

La Commission rappelle qu'aux termes de l'article 32 de la loi n° 78-17 du 6 janvier 1978 modifiée, le responsable du traitement est tenu d'informer les personnes concernées par le traitement, notamment de sa finalité, du caractère obligatoire ou facultatif des réponses, des destinataires des informations ainsi que de leurs droit d'accès, de rectification et, le cas échéant, d'opposition.

Dans sa délibération n° 2008-155 du 29 mai 2008, la CNIL avait mis la société en demeure de prendre toute mesure visant à garantir le respect de l'article 32, l'information délivrée quant au dispositif de vidéosurveillance étant jugée insatisfaisante.

Dans sa déclaration normale n° 1303553, la société avait indiqué avoir adopté une *« circulaire d'information à l'attention du personnel »* et un *« panneau d'information à l'attention de la clientèle »* sans y annexer les modèles. En outre, dans son courrier du 29 août 2008, la société avait informé la Commission qu'elle avait procédé à l'envoi de courriers à l'attention de son *« ancien personnel précisant la présence de caméras de vidéosurveillance »,* sans fournir à la CNIL un document l'attestant.

Lors de la séance de la formation restreinte du 16 avril 2009, des copies de ces courriers et d'un panneau d'affichage ont été produits par la société. Le courrier-type adressé à une dizaine

d'employés indiquait *« suite à la visite de la CNIL dans nos locaux nous sommes tenus de vous informer par écrit que tous les établissements de la société Jean-Marc Philippe sise ci-dessous sont équipés de caméras de vidéosurveillance ».* Lors de la séance, la société a également affirmé que plusieurs affichettes avaient été disposées à divers endroits, sans davantage de précision.

Or, la Commission constate que l'information délivrée aux employés de la société est manifestement insuffisante au regard des exigences de l'article 32 de la loi précitée. En effet, l'information inscrite dans les contrats de travail des personnes employées postérieurement à la mise en œuvre du dispositif de vidéosurveillance, à savoir *« la salariée est informée qu'un système de vidéosurveillance est installé dans tous les sites de l'entreprise »,* ainsi que celle mentionnée dans le courrier-type sont incomplètes puisque les finalités poursuivies, les destinataires des images et les modalités concrètes de l'exercice du droit d'accès dont disposent les personnes concernées, ne sont pas indiqués.

La Commission considère dès lors que la société ne s'est pas conformée à la mise en demeure de la CNIL n° 2008-155 du 29 mai 2008.

C. Sur le manquement à l'obligation de sécurité des données

La Commission rappelle que l'article 34 de la loi n° 78-17 du 6 janvier 1978 modifiée dispose que *« le responsable de 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 ait accès ».*

Dans sa délibération n° 2008-155 du 29 mai 2008, la CNIL avait mis la société en demeure de prendre toute mesure de nature à garantir la sécurité et la confidentialité des informations collectées dans l'ensemble des traitements mis en œuvre afin que seules les personnes habilitées de par leurs fonctions y aient accès (accès au logiciel de supervision, aux serveurs informatiques). En effet, la délégation de la CNIL avait constaté que l'accès au logiciel de supervision sur la station située à l'accueil ainsi que l'accès aux serveurs informatiques n'étaient pas sécurisés.

Dans son courrier du 29 août 2008, la société n'avait fourni aucun élément de réponse à la CNIL sur ce point. Or, dans ses observations du 16 avril 2009, la société a affirmé avoir isolé le serveur d'enregistrement dans un local muni d'un système de verrouillage dont l'accès est réservé aux responsables habilités. Quant au visionnage des images, il ne serait désormais accessible qu'au représentant légal de la société, après utilisation d'un mot de passe.

Eu égard aux pièces produites par la société lors de la séance de la formation restreinte du 16 avril 2009, la Commission considère que celle-ci s'est bien conformée à la mise en demeure n° 2008-155 en procédant à une meilleure sécurisation des données.

Sur les manquements constatés :

En conséquence, eu égard aux manquements constatés aux 1° et 2° de l'article 6 et à l'article 32 de la loi n° 78-17 du 6 janvier 1978 modifiée, la société Jean Marc Philippe, qui ne s'est que partiellement conformée à la mise en demeure n° 2008-155 du 29 mai 2008, verra prononcer à son encontre une sanction pécuniaire d'un montant de 10 000 euros.

Sur la publicité :

Eu égard à la nature et à la gravité des manquements commis ainsi qu'à la nécessité, d'une part, pour les personnes physiques de connaître les règles relatives à la protection de leurs données à caractère personnel et, d'autre part, pour les responsables de traitement de mieux appréhender les règles qui s'imposent à eux, la délibération de la Commission sera rendue publique sur le site internet de la CNIL et sur le site internet Légifrance.

PAR CES MOTIFS :

Conformément aux articles 45 et suivants de la loi du 6 janvier 1978 modifiée, la formation restreinte de la CNIL, après en avoir délibéré, décide : de prononcer une sanction pécuniaire de 10 000 euros à l'encontre de la société Jean-Marc Philippe, de publier la présente décision sur le site internet de la CNIL et sur le site internet Légifrance.

(A. Türk, prés. - M. Carrez, rapp.)