



T2012263

COUR DE CASSATION

**AVIS DE Mme ROQUES,
AVOCAT GÉNÉRAL RÉFÉRENDAIRE**

Arrêt n° 1249 du 10 novembre 2021 – Chambre sociale

Pourvoi n° 20-12.263

**Décision attaquée : 14 mai 2019 de la cour d'appel de Saint Denis
de la Réunion**

Mme [Y] [L]

**C/
SELAS Pharmacie Mahoraise**

1. Faits et procédure

Par contrat à durée indéterminée en date du 7 janvier 2003, Mme [Y] [L] (la salariée) a été embauchée par la SELAS Pharmacie Mahoraise en qualité de caissière.

Par courrier du 1^{er} juillet 2016, elle a été convoquée à un entretien préalable à un éventuel licenciement avec mise à pied conservatoire.

Elle a été licenciée pour faute grave par lettre recommandée avec avis de réception datée du 19 juillet 2016.

Contestant la régularité et le bien-fondé de son licenciement, la salariée a saisi le tribunal du travail de Mamoudzou qui, dans une décision rendue le 18 décembre 2017, a constaté que son licenciement pour faute grave était valable, l'a déboutée de ses demandes et l'a condamnée aux dépens ainsi qu'à verser une somme à son employeur au titre de ses frais irrépétibles.

Dans un arrêt en date du 14 mai 2019, la cour d'appel de Saint Denis de la Réunion a notamment confirmé ce jugement en toutes ses dispositions.

C'est l'arrêt attaqué par la salariée qui, dans un moyen unique, conteste la légalité des preuves apportées par son employeur pour établir les fautes graves qu'il lui reproche mais également l'appréciation faites par les juges du fond de la gravité des faits qui lui sont imputés.

2. Discussion et avis

La majeure partie des branches du moyen pose des questions quant à la licéité de certaines preuves produites par l'employeur et obtenues au moyen d'un système de vidéo-surveillance installé dans la pharmacie dans laquelle la salariée travaillait.

Cette dernière soutient que ce dispositif a été installé et utilisé en méconnaissance d'un certain nombre de règles.

- *sur la légalité des preuves obtenues au moyen d'un système de vidéo-surveillance installé sur le lieu de travail de la salariée*

Le débat entre les parties porte essentiellement sur la nature du dispositif installé par l'employeur.

En effet, tandis que la salariée soutient qu'il s'agit d'un système de vidéo-surveillance qui incluait également le contrôle de l'activité des salariés, l'employeur estime qu'il ne s'agit que d'un système de vidéo-protection qui échappe à certaines règles prescrites notamment par le code du travail et la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Aux termes de l'article L021-1 du code du travail applicable à Mayotte, dans sa version en vigueur au jour du licenciement, « *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.* »

L'article L. 442-6 en son dernier aliéna, dans sa version applicable au litige, dispose que « *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.* »

En l'absence de comité d'entreprise, notamment pour les entreprises de moins de 50 salariés, ces attributions relèvent du ou des délégués du personnel, s'il y en a de désignés dans l'entreprise, conformément aux dispositions des articles L. 431-1 et L. 432-4 de ce même code.

Par ailleurs, la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa version applicable au litige, prescrit un certain nombre de formalités à accomplir en cas d'installation d'un système de traitement automatisé de données à caractère personnel¹.

L'article 6 de cette loi prévoit notamment qu'« *Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :*

- 1° Les données sont collectées et traitées de manière loyale et licite ;*
- 2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. [...]*».

¹ L'article 2 de cette loi qui définit son champ d'application prévoit notamment que :

« *Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.*

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »

L'article 7 dispose qu'« *Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :*

- 1° Le respect d'une obligation légale incombant au responsable du traitement ;*
- 2° La sauvegarde de la vie de la personne concernée ;*
- 3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;*
- 4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;*
- 5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée. »*

L'article 22 de ce texte prévoit que l'installation d'un tel système doit donner lieu à une déclaration préalable à sa mise en œuvre auprès de la CNIL, cette déclaration devant préciser notamment la ou les finalités du traitement de données, la nature des données ainsi collectées, la ou les catégories de personnes concernées ainsi que la durée de conservation des informations traitées².

L'article 32 énumère les informations qui doivent être communiquées aux personnes dont les données personnelles sont ainsi recueillies, parmi lesquelles figurent « *l'identité du responsable du traitement et, le cas échéant, de celle de son représentant* » et « *la finalité poursuivie par le traitement auquel les données sont destinées* ».

Lorsqu'elle est saisie de plaintes à l'encontre de système de vidéo-surveillance, la CNIL s'attache à vérifier que celui-ci est bien utilisé conformément à la finalité déclarée et que l'information délivrée aux personnes susceptibles d'être soumises à ce système est suffisamment complète et précise notamment en ce qui concerne la finalité effective du système, l'identité des destinataires des données collectées et le droit d'accès à ces données³.

Enfin, l'article L. 251-1 du code de la sécurité intérieure dispose que « *Les enregistrements visuels de vidéoprotection répondant aux conditions fixées aux articles L. 251-2 et L. 251-3 sont soumis aux dispositions du présent titre, à l'exclusion de ceux qui sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques, qui sont soumis à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. »*

² Cf. Article 30 de cette même loi qui prévoit également que « *Le responsable d'un traitement déjà déclaré ou autorisé informe sans délai la commission :*
- de tout changement affectant les informations mentionnées » dans sa déclaration.

³ Cf. À titre d'exemple la délibération n° 2009-201 du 16 avril 2009

En vertu de dispositions de l'article L251-2 de ce même code, « *Il peut être également procédé à ces opérations [de vidéo-protection] dans des lieux et établissements ouverts au public aux fins d'y assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol.* »

L'article L. 252-1, dans sa version applicable au litige, précise que « *L'installation d'un système de vidéoprotection dans le cadre du présent titre est subordonnée à une autorisation du représentant de l'Etat dans le département et, à Paris, du préfet de police donnée, sauf en matière de défense nationale, après avis de la commission départementale de vidéoprotection.* »

S'il convient d'opérer une distinction entre vidéo-protection et vidéo-surveillance, comme cela est indiqué au rapport, la chambre s'attache à l'usage effectif du système ainsi installé et non à sa vocation initiale, telle que décrite dans les déclarations faites auprès des diverses autorités administratives ou les informations délivrées aux IRP.

Ainsi, si le système avait été initialement installé en vue de la protection des biens et/ou des personnes mais est, par la suite, utilisé pour contrôler l'activité des salariés, la chambre exige qu'il remplisse les conditions requises pour cet usage, sous peine d'être considéré comme un mode de preuve illégal⁴.

Dans notre espèce, la note de service du 27 novembre 2015, signée par certains salariés, les informe que le système de surveillance vidéo installé dans la pharmacie a vocation à prévenir les atteintes aux biens et aux personnes.

Toutefois, lors de la déclaration auprès de la CNIL par courrier daté du 1^{er} décembre 2014, l'employeur avait mentionné également comme finalité de ce dispositif la « *lutte contre la démarque inconnue* ».

Par ailleurs, cette déclaration évoquait l'installation de quatre caméras, sans précision sur leurs localisations dans les locaux.

⁴ Cf. Par exemple Soc., 7 juin 2006, pourvoi n° 04-43.866, Bull. 2006, V, n° 206, Soc., 10 janvier 2012, pourvoi n° 10-23.482, Bull. 2012, V, n° 2 ou Soc., 11 décembre 2019, pourvoi n° 18-11.792 : « *Mais attendu que selon l'article L. 2323-32 du code du travail, antérieur à la loi n° 2015-994 du 17 août 2015, le comité d'entreprise est informé et consulté, préalablement à la décision de mise en oeuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés ; Et attendu qu'ayant constaté que l'outil de traçabilité GC45, destiné au contrôle des opérations et procédures internes, à la surveillance et la maîtrise des risques, permettait également de restituer l'ensemble des consultations effectuées par un employé et était utilisé par l'employeur afin de vérifier si le salarié procédait à des consultations autres que celles des clients de son portefeuille, la cour d'appel en a exactement déduit que l'employeur aurait dû informer et consulter le comité d'entreprise sur l'utilisation de ce dispositif à cette fin et qu'à défaut, il convenait d'écarter des débats les documents résultant de ce moyen de preuve illicite ; »*

Au regard des finalités du dispositif, telles que décrites par l'employeur et du fait que les locaux étaient ouverts au public, la CNIL n'a pas considéré que le dispositif devait faire l'objet d'une déclaration auprès d'elle.

Toutefois, la « *démarque inconnue* », qui correspond au pourcentage du chiffre d'affaires d'un commerce équivalant au coût des produits volés, disparus ou cassés, peut être le fait de clients ou de salariés.

Installer un système de vidéo-surveillance ayant pour but de la prévenir peut donc impliquer la surveillance des salariés.

Par ailleurs, selon la note de service précitée, ce sont cinq et non quatre caméras qui ont été installées. L'une d'elles filmait « *l'espace ordonnance* », deux autres étaient dirigées vers des rayons, les deux dernières étant « *à l'étage (bureau et réserve)* ».

Dans sa décision en date du 31 août 2016, l'inspectrice du travail, saisie d'une demande d'autorisation du licenciement d'une autre salariée, indique qu'« *en réalité, il existe cinq caméras dans la surface de vente de la pharmacie, dirigées sur les postes de caisses, que l'employeur possède dans son bureau un matériel informatique doté d'un écran permettant une vidéosurveillance dans la pharmacie, soit huit vues sur les trois postes de caisse, tenus par une caissière et deux pharmaciens assistants* ». Ces constatations n'ont pas été remises en cause devant les juridictions administratives, saisies par l'employeur.

La localisation et le nombre de caméras installées n'étaient donc pas conformes à la déclaration faite auprès de la CNIL et certaines pouvaient matériellement servir à contrôler l'activité des salariés.

En outre, il résulte des termes du jugement du tribunal du travail que l'employeur a utilisé les images enregistrées par ces caméras pour vérifier et expliquer les erreurs de stocks qu'il avait constatées, en contrôlant les opérations de caisse passées par les deux caissières, qui ont ensuite fait l'objet de procédures de licenciement.

Ainsi, il a bien fait usage de ce dispositif pour contrôler l'activité de la salariée pendant son temps de travail.

Il ne s'agit donc pas que d'un système de vidéo-protection mais aussi d'un dispositif de vidéo-surveillance.

Or, l'information des salariés par l'employeur n'a pas été faite loyalement selon moi puisqu'il ne leur a pas été indiqué que les vidéos réalisées étaient conservées pendant plusieurs jours et qu'il pourrait consulter les enregistrements pour contrôler leur activité.

Il n'est pas non plus justifié d'une information et d'une consultation du comité d'entreprise ou du délégué du personnel avant la mise en place de ce dispositif, conformément à l'article L. 442-6 précité. En effet, s'il n'est pas établi que l'entreprise employait au moins 50 salariés, il résulte des écritures d'appel de l'employeur qu'une de ses salariés, également visée par une procédure de licenciement, était délégué du personnel et aurait donc dû être consultée préalablement.

En outre, dès lors que certaines des caméras étaient installées dans des locaux non ouverts au public, selon la note de service précitée, et qu'il n'excluait pas d'utiliser ce dispositif pour contrôler l'activité de ses salariés, l'employeur aurait dû faire une déclaration auprès de la CNIL plus complète que celle dont il justifie, pour qu'elle puisse, à tout le moins, véritablement s'assurer de l'application ou non des dispositions de la loi du 6 janvier 1978.

Enfin, l'employeur ne justifie pas non plus de l'obtention d'une autorisation préfectorale d'installation de ce dispositif puisqu'il est seulement fait mention d'une demande en ce sens dans les pièces produites.

C'est pourquoi, j'estime que l'employeur a utilisé illégalement le dispositif de vidéo-surveillance qu'il avait fait installé.

Les juges du fond ne pouvaient valablement retenir que les enregistrements vidéos constituaient un mode de preuve licite des fautes commises par la salariée.

Si l'arrêt encourt la cassation sur ce point, cela ne signifie pas pour autant que l'employeur ne pouvait se prévaloir de ces éléments de fait.

- *sur la possibilité de tenir compte de ces preuves malgré leur illégalité*

Comme le souligne le rapport, votre jurisprudence a évolué s'agissant de la recevabilité des preuves obtenues par un moyen illicite.

Dans un arrêt récent⁵, vous avez énoncé qu' « *Il y a donc lieu de juger désormais que l'illicéité d'un moyen de preuve, au regard des dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée par la loi n° 2004-801 du 6 août 2004, dans sa version antérieure à l'entrée en vigueur du Règlement général sur la protection des données, n'entraîne pas nécessairement son rejet des débats, le juge devant apprécier si l'utilisation de cette preuve a porté atteinte au caractère équitable de la procédure dans son ensemble, en mettant en balance le droit au respect de la vie personnelle du salarié et le droit à la preuve, lequel peut justifier la production*

⁵ Cf. Soc., 25 novembre 2020, pourvoi n° 17-19.523

d'éléments portant atteinte à la vie personnelle d'un salarié à la condition que cette production soit indispensable à l'exercice de ce droit et que l'atteinte soit strictement proportionnée au but poursuivi. »

Cette évolution, qui avait déjà été amorcée par de précédents arrêts⁶, se fonde sur la jurisprudence de la Cour Européenne des Droits de l'Homme (CEDH) qui, dans plusieurs décisions, a également consacré la possibilité d'admettre, sous certaines conditions, des preuves obtenues au moyen de dispositifs de surveillance des salariés.

Dans son [arrêt du 5 septembre 2017, affaire Barbulescu c. Roumanie](#), la cour a énoncé des critères à prendre en compte pour s'assurer que les droits du salariés, et notamment le droit au respect de sa vie privée, n'ont pas été méconnus.

Elle a ainsi invité les autorités nationales à tenir compte de :

- l'existence d'une information des salariés sur la possibilité de faire l'objet d'une mesure de surveillance ;
- l'ampleur de la surveillance et du degré d'intrusion dans la vie privée ;
- la justification de cette mesure par des motifs légitimes ;
- la possibilité d'adopter des mesures moins intrusives ;
- des conséquences de la surveillance pour les employés qui en ont été l'objet ;
- et de l'existence de garanties appropriées, notamment l'information fournie aux employés concernés ou aux représentants du personnel sur la mise en place et sur l'ampleur de la vidéosurveillance, ou la possibilité d'introduire une réclamation.

La CEDH a fait application de ces critères dans un [arrêt du 17 octobre 2019, affaire López Ribalda et autres c. Espagne](#) dans lequel était aussi posée la question de « *l'admission comme preuves au cours de la procédure des enregistrements obtenus au moyen de la vidéosurveillance* » au regard des dispositions de l'article 6 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

Dans cette affaire, les enregistrements en cause avaient été obtenus au moyen de caméras de surveillance dissimulées, installées par l'employeur qui soupçonnait certains de ses salariés de commettre des vols.

S'agissant de la violation de l'article 6, la cour a ainsi indiqué ce qui suit :

« 150. La Cour n'a donc pas à se prononcer, par principe, sur l'admissibilité de certaines sortes d'éléments de preuve, par exemple des éléments obtenus de manière illégale au regard du droit interne. Elle doit examiner si la procédure, y compris la manière dont les éléments de preuve ont été recueillis, a été équitable dans son ensemble, ce qui implique l'examen de l'illégalité en question et, dans le cas où se

⁶ Cf. [Soc., 9 novembre 2016, pourvoi n° 15-10.203](#), Bull. 2016, V, n° 209 et [Soc., 30 septembre 2020, pourvoi n° 19-12.058](#)

trouve en cause la violation d'un autre droit protégé par la Convention, de la nature de cette violation (P.G. et J.H. c. Royaume-Uni, précité, § 76, et Gäfgen c. Allemagne [GC], no 22978/05, § 163, CEDH 2010).

151. Pour ce qui est de la nature de l'illégalité ou de la violation de la Convention constatée, si l'utilisation d'éléments de preuve obtenus au moyen d'une mesure jugée contraire à l'article 3 suscite toujours de graves doutes quant à l'équité de la procédure (Gäfgen, précité, § 165), pour déterminer si l'utilisation comme preuves d'informations obtenues au mépris de l'article 8 ou en violation du droit interne a privé le procès du caractère équitable voulu par l'article 6, il faut prendre en compte toutes les circonstances de la cause et se demander en particulier si les droits de la défense ont été respectés et quelles sont la qualité et l'importance des éléments en question. Il convient de rechercher en particulier si le requérant s'est vu offrir la possibilité de remettre en question l'authenticité de l'élément de preuve et de s'opposer à son utilisation. Il faut prendre également en compte la qualité de l'élément de preuve, y compris le point de savoir si les circonstances dans lesquelles il a été recueilli font douter de sa fiabilité ou de son exactitude (Schenk, précité, §§ 46-48, P.G. et J.H. c. Royaume-Uni, précité, §§ 77-79, et Gäfgen, précité, § 164). Si un problème d'équité ne se pose pas nécessairement lorsque la preuve obtenue n'est pas corroborée par d'autres éléments, il faut noter que lorsqu'elle est très solide et ne prête à aucun doute, le besoin d'autres éléments à l'appui devient moindre (Gäfgen, loc. cit.). »

La Cour de cassation peut opérer un contrôle de proportionnalité direct afin de déterminer, à partir des faits constants résultant de la décision attaquée, si l'atteinte à un droit fondamental protégé par la Convention est justifiée par la nécessité d'assurer l'effectivité d'une autre norme, celle-ci pouvant trouver sa source dans le droit européen ou dans le droit interne.

Dans notre espèce, les juges du fond ne se sont pas livrés à un tel contrôle puisqu'ils ont estimé tant en première instance qu'en appel qu'il s'agissait d'un dispositif de vidéo-protection qui ne contrevenait pas aux règles applicables.

Devant la chambre, la salariée n'invoque ni une violation de sa vie privée, ni un manquement au droit à un procès équitable, comme cela pouvait être le cas dans les précédentes espèces⁷.

Son argumentation repose exclusivement sur l'illégalité, et donc l'irrecevabilité, des enregistrements vidéos faits par son employeur au regard de dispositions de droit interne.

Par ailleurs, la décision d'appel se limite à énoncer les faits reprochés à la salariée et à indiquer que leur matérialité « *est corroborée par les enregistrements vidéo de la pharmacie* ».

Si la cour d'appel a adopté les motifs des premiers juges, qui étaient, eux, plus détaillés s'agissant des fautes reprochées à la salariée et des preuves produites par

⁷ Arrêts des 30 septembre et 25 novembre 2020 précités en notes de bas de page 5 et 6

l'employeur, cette dernière contestait la réalité de ces fautes et la fiabilité des preuves produites, y compris celles qui ne résultaient pas de la vidéo-surveillance. Tout au plus admettait-elle avoir pu commettre des erreurs de caisse à raison du changement de logiciel.

Or, les constatations faites par les juges du fond ne vous permettent pas, selon moi, de procéder au contrôle de proportionnalité, quand bien même les parties produisent un certain nombre de pièces dans le cadre du présent pourvoi.

Enfin, je partage le point de vue de Mme l'avocate générale Trassoudaine qui, dans son avis complémentaire sous l'arrêt du 25 novembre 2020, écrivait que « *c'est aux juges du fond, juges du fait et du droit qu'il incombe en premier lieu de procéder à la mise en balance des intérêts en présence en considération des éléments de fait qu'ils apprécient souverainement.* »

C'est pourquoi, **je suis d'avis de casser l'arrêt de la cour d'appel de Saint Denis de la Réunion** tout en rappelant la solution énoncée dans votre décision du 25 novembre 2020 qui permettra à la cour d'appel de renvoi de se livrer au contrôle de proportionnalité requis.