COUR DE CASSATION

AVIS DE Mme TRASSOUDAINE-VERGER,
AVOCAT GENERAL

Arrêt n°1119 du 25 novembre 2020 - Pourvoi n° X1719523

Décision attaquée : 16 mars 2017 de la cour d'appel de Paris

M. A... X...
C/
la société Agence France presse

_____

Observation liminaire : une consultation de la Commission nationale informatique et libertés (CNIL) sollicitée dans le cadre de la présente instance est annexée au présent avis.

Pour mémoire, M. X... a été licencié pour faute grave, pour avoir adressé à une entreprise cliente et en même temps concurrente de l'AFP, cinq demandes de renseignements par voie électronique en usurpant l'identité de sociétés clientes.

L'employeur, alerté par l'une de ces entreprises, a fait intervenir un expert informatique, en présence d'un huissier et du responsable interne de la sécurité des systèmes d'information, pour exploiter les fichiers de journalisation conservés sur ses serveurs. M. X... a été identifié comme étant l'auteur des messages litigieux grâce à l'adresse IP fournie par l'entreprise ayant donné l'alerte.

Estimant qu'une déclaration préalable d'utilisation des logs et fichiers de journalisation et adresses IP qui constitue un traçage informatique n'étaient pas soumis à une déclaration à la CNIL, la cour d'appel a jugé le licenciement justifié.

Le salarié invoque l'illicéité de ce moyen de preuve, la violation des articles 2 et 22 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ensemble les articles L.1234-1, L.1234-5 et L.1234-9 du code du travail, l'article 9 du code de procédure civile et l'article 6 § 1 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales.

La consultation de la CNIL a porté sur la question[1] de savoir si les informations collectées, avant toute déclaration à cet organisme, par un système de traitement automatisé de données personnelles comme la collecte des adresses IP, permettant d'identifier indirectement une personne physique ou encore le traçage des fichiers de journalisation constituent un moyen de preuve illicite, en violation des articles 2 et 22 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

La CNIL confirme que les fichiers de journalisation d'un système d'information constituent des **traitements de données à caractère personnel** au sens de l'article 2 de la loi du 6 janvier 1978 modifiée, *dans la mesure où* ***ils comportent des informations qui concernent des personnes identifiables, à savoir les activités sur les applications et réseaux informatiques des employés***.

En tant que tels, ces outils étaient soumis, jusqu'à l'entrée en application du RGPD[2], au régime de formalités préalables prévu par le chapitre IV de la loi de 1978. Il convient donc de déterminer la formalité applicable à la mise en oeuvre du traitement litigieux, opéré en 2015.

L'article 22 - I prévoit : *A l'exception de ceux qui relèvent des dispositions prévues aux articles 25, 26 et 27 ou qui sont visés au deuxième alinéa de l'article 36,* ***les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés***.

A l'évidence - et cela n'est d'ailleurs pas soutenu - le traitement automatisé litigieux n'entre pas dans le champ d'application de l'article 25, relatif aux traitements soumis à autorisation de la CNIL, ni dans celui des articles 26 et 27, relatifs aux traitements soumis à demande d'avis avant leur mise en oeuvre.

Il ne fait pas davantage l'objet d'une dispense de déclaration prévue au II de l'article 22 et à l'article 67. Il n'est pas allégué que ce type de traitement a fait l'objet d'une décision de dispense de déclaration par la CNIL en application de l'article 24-II.

Il convient de rechercher alors si le traitement relève d'une déclaration "normale" selon les modalités de l'article 23 ou "simplifiée" dans le cas où la CNIL a adopté une norme simplifiée.

---

[1] posée par les 4ème et 5ème branches du 3ème moyen du salarié.

[2] Issu du règlement UE n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE(règlement général sur la protection des données), le RGPD a été intégré dans le droit français par la loi 2018-493 du 20 juin 2018 relative à la protection des données personnelles qui est venue modifier la loi 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Celle-ci a pris, le 13 janvier 2005, une délibération n°2005-002 portant adoption d'une norme destinée à **simplifier l'obligation de déclaration des traitements mis en oeuvre pour les organismes publics et privés pour la gestion de leurs personnels**.

Il est prévu, à l'article 2 que le traitement peut avoir tout ou partie des finalités suivantes, en particulier *la mise à disposition des personnels d'outils informatiques, la mise en oeuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux, **à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés***.

Selon l'article 3,c), les données traitées pour la réalisation de ces finalités peuvent être *les données de connexion enregistrées pour assurer la sécurité et le bon fonctionnement des applications et des réseaux informatiques, **à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés***.

Dans l'affaire qui vous est soumise, le traitement litigieux dont le but était d'identifier l'auteur de fausses demandes de renseignement émises au nom de sociétés clientes, permettait le contrôle individuel de l'activité des employés au sens de l'article 3,c). Ne pouvant relever de la déclaration "simplifiée", il appartenait au responsable du traitement de faire une déclaration "normale" selon les modalités de l'article 23.

Toutefois, **l'article 22-III prévoit une exception** : *les traitements pour lesquels le responsable a désigné un **correspondant à la protection des données à caractère personnel** chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi **sont dispensés des formalités prévues aux articles 23 et 24.***

*La désignation du correspondant est **notifiée à la Commission nationale de l'informatique et des libertés**. Elle est **portée à la connaissance des instances représentatives du personnel.***

*Le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions. **Il tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande** et ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions. Il peut saisir la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions.*

En cas de non-respect des dispositions de la loi, le responsable du traitement est enjoint par la Commission nationale de l'informatique et des libertés de procéder aux formalités prévues aux articles 23 et 24. En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation, de la Commission nationale de l'informatique et des libertés.

Il était dans les débats au fond - et rappelé dans les mémoires déposés devant vous - que M. X... avait été désigné correspondant informatique et liberté au sein de l'AFP[3]. L'arrêt relève dans l'énoncé des moyens (p 12) que *M. X... fait valoir pour l'essentiel que le contrôle mis en oeuvre par l'AFP, à l'aide d'un système d'exploitation des données individualisés associé aux fichiers de journalisation, est illicite à défaut de déclaration à la CNIL, d'information du salarié en sa qualité de correspondant informatique et liberté -CIL- au sein de l'agence...*

[3] Cf. conclusions d'appel p 8 et 9 du salarié et p 23 de l'employeur.

Au regard de ces principes, de la désignation d'un correspondant informatique et liberté (CIL) dans l'entreprise et des dispositions de l'article 22 III, si une déclaration préalable n'était pas nécessaire, contrairement à ce que soutient le moyen, le traitement automatisé devait faire l'objet d'une mention par le CIL - en l'occurrence M. X... - sur le registre du traitement automatisé.

La cour d'appel ne s'est pas placée sur ce terrain mais sur celui de l'absence de soumission à déclaration préalable au motif que l'utilisation des logs et fichiers de journalisation et adresses IP constitue un traçage informatique. Cette motivation n'est pas satisfaisante, en tout cas insuffisante pour justifier le rejet.

Toutefois, la protection liée à la possible identification de la personne physique par un traitement automatisé est un droit relatif et non un droit absolu en ce qu'il ne porte pas atteinte aux droits fondamentaux. Ainsi, la déclaration préalable de l'usage d'un tel traitement prévue par la loi suffit à neutraliser cette protection.

La question doit être posée dès lors, de la mise en balance du droit à la protection du salarié et de l'intérêt pour l'employeur d'assurer la protection de l'entreprise à la lumière de la jurisprudence de la CEDH.

A cet égard, la CEDH a rendu le 17 octobre 2019 en grand chambre, un arrêt Lopez Ribalda et autres c. Espagne (aff. 1874/13 et 8567/13) à propos de caissières d'un supermarché licenciées pour motif disciplinaire après avoir été **filmées à leur insu sur leur lieu de travail** par l'employeur, alors que le droit national prévoit une obligation de notification préalable de la surveillance. **Pour la Cour de Strasbourg, un impératif prépondérant relatif à la protection d'intérêts publics ou privés importants peut justifier l'absence d'information préalable.**

Il est intéressant de relever que l'affaire avait donné lieu à un arrêt de la 3ème section de la Cour du 9 janvier 2018 qui avait conclu à la violation de l'article 8 de la Convention (droit au respect de la vie privée) et à la non-violation de l'article 6 de la Convention (droit à un procès équitable). C'est sur demande du gouvernement espagnol que l'affaire a été portée en grand chambre.

La Cour a jugé qu'il y a lieu de **mettre en balance le droit au respect de la vie privée et l'intérêt pour l'employeur « d'assurer la protection de ses biens et le bon fonctionnement de l'entreprise »**. Pour cela, plusieurs critères doivent être pris en compte par les tribunaux internes pour statuer sur le caractère proportionné d'une mesure de vidéosurveillance.

Ces critères sont ceux posés dans l'**arrêt Barbulescu c/ Roumanie[4] relatif à la surveillance des communications électroniques des salariés**, selon lequel il doit être tenu compte :
– de l'existence d'une information des salariés sur la possibilité de faire l'objet d'une mesure de surveillance ;
– de l'ampleur de la surveillance et du degré d'intrusion dans la vie privée ;
– de la justification de cette mesure par des motifs légitimes ;
– de la possibilité d'adopter des mesures moins intrusives ;
– des conséquences de la surveillance pour les employés qui en ont été l'objet ;

[4] Gd chambre, 7 septembre 2017, n° 61496/08.

– 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.

Pour justifier sa décision, la CEDH a notamment retenu que :

- **la mise en place de la vidéosurveillance se justifiait par des raisons légitimes**, à savoir les soupçons, nourris par le directeur du magasin en raison des pertes importantes constatées sur plusieurs mois, que des vols avaient été commis. ... d'où **l'intérêt légitime pour l'employeur d'adopter des mesures afin de découvrir les responsables des pertes constatées et de les sanctionner, dans le but d'assurer la protection de ses biens et le bon fonctionnement de l'entreprise**,

- **l'ampleur de la mesure de surveillance et le degré d'intrusion dans la vie privée des requérantes** : la mesure était **limitée en ce qui concernait les espaces et le personnel surveillés** – les caméras ne couvraient que les caisses susceptibles d'être à l'origine des pertes constatées – **et sa durée dans le temps n'avait pas dépassé ce qui était nécessaire pour confirmer les soupçons de vol**,

- **l'ampleur de la mesure dans le temps**, dix jours, qui a cessé dès que les employés responsables ont été identifiés ... seuls le responsable du magasin, la représentante légale de l'entreprise et la déléguée syndicale ont visionné les enregistrements obtenus au moyen de la vidéosurveillance litigieuse avant que les requérantes n'en soient informées,

- les **conséquences** de la surveillance litigieuse ont été importantes pour les requérantes qui ont licenciées sur la base des enregistrements obtenus par ce moyen. Néanmoins la vidéosurveillance et les enregistrements n'ont pas été utilisés par l'employeur à d'autres fins que celle de trouver les responsables des pertes de produits constatées et de les sanctionner.

- dans les circonstances de l'espèce, il n'existait pas d'autre moyen permettant d'atteindre le but légitime poursuivi et la mesure devait dès lors être jugée «**nécessaire**»,

- s'agissant enfin de **savoir si les requérantes avaient été informées de la mise en place de la vidéosurveillance**, la cour rappelle que **l'information donnée à la personne faisant l'objet d'une surveillance et son ampleur ne sont que l'un des critères à prendre en compte pour apprécier la proportionnalité d'une telle mesure dans un cas donné**. Toutefois, si une telle information fait défaut, les garanties découlant des autres critères revêtiront d'autant plus d'importance.

Sur le terrain de l'article 6 de la Convention, la Cour relève que les requérantes se plaignent de l'admission et de l'utilisation comme preuves par les juridictions du travail d'enregistrements obtenus en violation de leur droit au respect de leur vie privée.

Elle rappelle qu'elle a pour seule tâche, aux termes de l'article 19 de la Convention, d'assurer le respect des engagements résultant pour les États contractants de la Convention [...] **Si l'article 6 garantit le droit à un procès équitable, il ne réglemente pas pour autant l'admissibilité des preuves en tant que telles, matière qui relève au premier chef du droit interne** [...] En principe, des questions telles que le poids attaché par les tribunaux nationaux à tel ou tel élément de preuve ou à telle ou telle conclusion ou appréciation dont ils ont eu à connaître échappent au contrôle de la Cour [...]

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 trouve en cause la violation d'un autre droit protégé par la Convention, de la nature de cette violation**[5].

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[6], 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**[7]. 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**[8] [...]

À la lumière de ce qui précède, la Cour considère que l'utilisation comme preuves des images obtenues par vidéosurveillance n'a pas porté atteinte au caractère équitable de la procédure en l'espèce.

Dans l'affaire qui vous est soumise examinée à la lumière des arrêts Barbulescu et Lopez Ribalda, un contrôle de proportionnalité me paraît souhaitable compte tenu du contexte. Et le moyen qui invoque la violation des dispositions de l'article 9 du code de procédure civile et de l'article 6 § 1 de la CESDH y incite.

Cette démarche suppose un infléchissement de votre jurisprudence car à ma connaissance, vous n'avez pas encore, en ce domaine, opéré de la sorte.

Plutôt que de procéder à une cassation "sèche", vous pourriez opportunément inviter la cour de renvoi à rechercher si l'employeur, en mettant en oeuvre un traitement automatisé aux fins d'identifier l'auteur des messages litigieux, a commis une atteinte à la vie privée du salarié. Le fait de ne pas accomplir les formalités de déclaration prévues par la loi de 1978 est-il constitutif d'une atteinte disproportionnée à la protection du salarié au regard du but poursuivi par l'employeur de protection de ses biens et du bon fonctionnement de l'entreprise ?

---

[5] P.G. et J.H. c. Royaume-Uni, précité, § 76, et Gäfgen c. Allemagne[GC], no 22978/05, § 163, CEDH 2010.

[6] Gäfgen, précité, § 165.

[7] Schenk, précité, §§ 46-48, P.G. et J.H. c. Royaume-Uni, précité, §§ 77-79, et Gäfgen, précité, § 164

[8] Gäfgen, loc. cit.

Vous avez certes la possibilité d'effectuer le contrôle de proportionalité de manière directe - de mon point de vue, un certain nombre d'éléments relevés par l'arrêt le permettent comme je vais le démontrer - mais cette voie n'a pas ma préférence car 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.

Pour effectuer un contrôle direct, il peut être retenu des constatations souveraines de l'arrêt attaqué non remises en cause par le moyen les éléments suivants :

- **la recherche de l'auteur des messages litigieux se justifiait par des raisons légitimes** à la suite de **l'alerte donnée par une entreprise extérieure** à la fois cliente et concurrente sur des dysfonctionnements - *l'envoi de cinq fausses demandes de renseignement sur le service de rediffusion des dépêches AFP émises à partir de la même adresse IP 158.50.204 entre 12 h 14 et 15 h au nom de diverses personnes appartenant à cinq sociétés différentes, partenaires de distribution importants de l'entreprise - de nature à altérer les liens avec ceux-ci*. **D'où l'intérêt légitime pour l'employeur d'adopter des mesures afin de découvrir l'expéditeur des messages et de le sanctionner, dans le but d'assurer la protection de ses biens et le bon fonctionnement de l'entreprise**.

- **l'ampleur de la mesure du traitement et le degré d'intrusion dans la vie privée du salarié** : l'atteinte a été limitée à l'identification de l'expéditeur des faux messages, à partir de l'adresse IP fournie par l'entreprise ayant donné l'alerte. La recherche a été effectuée par un expert informatique en présence du responsable sécurité des systèmes d'information de l'AFP sous le contrôle d'un huissier. Elle a consisté dans le recoupement des informations des fichiers de journalisation extraites des données du gestionnaire centralisé de logs de l'AFP.

- l'ampleur de la mesure dans le temps : il s'agit de la mise en oeuvre d'un contrôle a posteriori, motivé par l'alerte donnée par un tiers extérieur à l'entreprise. Sa durée a été limitée et n'a pas dépassé ce qui était nécessaire à l'identification (contrôle sur la plage horaire de 12 h 02 à 16 h 02 le jour de l'envoi des messages et de l'adresse IP utilisée pour cet envoi).

- **les conséquences du traitement litigieux** ont été importantes pour le salarié qui a été licencié sur la base des informations obtenues par ce moyen. Néanmoins, celles-ci n'ont pas été utilisées à d'autres fins que celles de l'identifier en tant qu'auteur des messages et de le sanctionner.

- **l'existence de garanties appropriées** : la nécessité d'effectuer la déclaration préalable du traitement automatisé **n'est que l'un des critères à prendre en compte pour apprécier la proportionnalité d'une telle mesure dans un cas donné**. Toutefois, si une telle formalité fait défaut, les garanties découlant des autres critères revêtiront d'autant plus d'importance.

- le **caractère nécessaire de la mesure pour atteindre le but légitime poursuivi**. Il vous appartiendrait de procéder à cette recherche dans le cadre d'un contrôle direct car la cour d'appel n'a appréhendé le traitement automatisé que sous l'angle de sa licéité en tant que moyen de preuve. Il est possible de considérer que l'utilisation des fichiers de journalisation a été pour l'employeur un **moyen approprié, compte tenu de leur fonction et du caractère intrusif circonscrit** pour atteindre le but légitime poursuivi d'identification de l'auteur des messages litigieux afin d'assurer la protection de ses biens et le bon fonctionnement de l'entreprise.

Dans le cas d'un contrôle indirect, il appartiendrait à la cour de renvoi, outre l'examen des autres critères, de rechercher si l'employeur avait d'autres moyens que la mise en oeuvre du traitement automatisé pour atteindre le but légitime poursuivi et si la mesure était nécessaire.

Sur le terrain de l'article 6§1 de la CESDH, il peut être retenu que le salarié a eu accès au compte rendu du traitement litigieux et aux modalités de son déroulement au cours de la procédure, a eu la possibilité d'en contester l'authenticité et de s'opposer à son utilisation en tant que preuve.

S'agissant de la prise en compte de **la qualité de l'élément de preuve, les circonstances dans lesquelles il a été recueilli ne font pas douter de sa fiabilité ou de son exactitude** : les fichiers journaux ont pour fonction de permettre la traçabilité de l'activité d'un réseau et d'apporter la preuve de cette activité, leur intérêt résidant dans leur capacité à identifier directement ou indirectement un individu ou un équipement ayant participé à cette activité. Conservés sur le serveur de l'entreprise pour une durée limitée, ils ont vocation à être utilisés a posteriori pour retrouver les traces d'un incident.

La cour d'appel **ne s'appuie pas seulement sur cet élément** mais sur ceux produits par l'entreprise qui a alerté l'employeur et qui lui a fourni les références de l'adresse IP. Elle a relevé encore qu'en sa qualité de responsable de la valorisation et du contrôle des usages numériques qui sont faits des produits de l'AFP et le fait qu'il travaillait à la direction commerciale et marketing, le salarié pouvait accéder aux fichiers clients de l'entreprise lui permettant d'envoyer les fausses demandes. Ces éléments viennent corroborer les informations obtenues via le traitement automatisé.

Avis de cassation partielle sur la 4ème branche du 3ème moyen du pourvoi du salarié en invitant la cour de renvoi à procéder à un contrôle de proportionnalité