Prospective

SURVEILLANCE NUMÉRIQUE : TENDANCES ET CONSÉQUENCES EN MATIÈRE DE SANTÉ ET SÉCURITÉ AU TRAVAIL

La surveillance du salarié par son employeur n'est pas nouvelle. Elle est induite dès lors qu'il existe une relation de subordination entre les deux parties, et constitue un des moyens de contrôle que possède l'employeur. Elle lui permet de vérifier que les conditions de réalisation du travail sont bien respectées. Elle est également légitimée par des questions de sécurité et par le fait que l'employeur est légalement responsable de la santé et de la sécurité des salariés et dispose, de ce fait, d'un droit de regard. Cependant, elle peut aussi influer de façon délétère sur le travail, lorsqu'il en est fait un usage excessif. Par ailleurs, depuis 2020, avec la crise de la Covid-19, le développement du télétravail et l'essor de nouvelles technologies, cette surveillance a changé de dimension et de nature. Il s'agit ici de préciser ce que l'on entend par surveillance numérique, d'estimer la réalité de son déploiement en France, les opportunités qu'elle peut présenter, ses possibles dérives et les risques qu'elle peut entraîner. Le cadre réglementaire qui permet d'en limiter l'usage est évoqué, ainsi que les mesures recommandées par l'INRS et ses homologues pour prévenir les risques professionnels qui peuvent en découler.

DIGITAL SURVEILLANCE: TRENDS AND OCCUPATIONAL SAFETY AND HEALTH CONSEQUENCES – Surveillance of employees by their employers is nothing new. It can occur once there is a subordinate relationship between two parties, and is a means of control for the employer. It allows them to check for compliance with the terms governing the implementation of work. It is also justified for security reasons and because the employer is legally responsible for the health and safety of their employees, and as such, has a right to monitor. However, it can also have a negative influence on work, when it is done excessively. Moreover, since 2020 with the Covid-19 crisis, the development of teleworking and the boom in new technology, the dimension and nature of this surveillance has changed. Here, the notion of digital surveillance is specified, as well as the way in which it is deployed in France, and the opportunities and possible drawbacks along with the risks it may cause are discussed. The legal framework which makes it possible to limit its use is addressed, as well as the measures recommended by INRS and its counterparts to prevent any resulting occupational risks.

JENNIFER CLERTÉ
INRS, mission Veille et prospective

NADIÈGE FÉLICIE
INRS, département Études, veille et assistance documentaires

Surveillance numérique : de quoi parle-t-on ?

Si la surveillance existe dans le travail dès lors qu'il existe un lien de subordination[1], sa pratique a connu diverses étapes, liées principalement aux évolutions technologiques. C'est ce que rappelle Hubert Bouchet, commissaire à la Commission nationale de l'informatique et des libertés (Cnil) et spécialiste du monde du travail, au titre du Conseil économique et social, en 2009[2]. Ainsi, au cours de la période industrielle, la surveillance était circonscrite au lieu de travail et s'opérait principalement par le biais de vigiles contrôlant la présence effective des ouvriers et de contremaîtres ou de cadres surveillant la bonne réalisation →

des activités et leur rendement. Rapidement, la surveillance de la présence sur site a été automatisée grâce aux « pointeuses ». Au-delà de leur fonction de contrôle, ces équipements ont aussi permis aux services de ressources humaines de mieux gérer les plannings et à ceux de la comptabilité d'établir plus facilement les fiches de paye. Les systèmes de vidéosurveillance, apparus dans les entreprises à partir des années 1980, constituent la troisième phase de cette évolution.

La quatrième phase a été amorcée avec le développement des technologies de l'information et de la communication (TIC) et d'Internet. Les outils informatiques permettent désormais aux employeurs de surveiller le flux d'informations émis par leurs salariés. Cette nouvelle étape, appelée « cybersurveillance » ou « surveillance numérique », a conduit à un changement de nature et de dimension de la faculté de surveiller de l'employeur. Celle-ci ne s'opère plus systématiquement par le biais d'un individu, elle ne connaît plus non plus de limite claire dans l'espace ou le temps ; elle peut s'étendre au-delà du site de l'entreprise et des horaires de travail. On parle souvent dans la littérature d'une surveillance dite « panoptique », c'est-à-dire un système de surveillance en continu des individus, qui permet d'observer l'intégralité de leurs faits et gestes sans être vu. Celle-ci peut s'opérer par le biais des équipements de travail (logiciels, boîtes mail, visioconférences, machines…) ou des environnements de travail, *via* des caméras, des capteurs…, sans que le travailleur n'en ait toujours conscience. Son caractère potentiellement intrusif (au-delà de la vie professionnelle) et systématique (tout au long des journées de travail) pose la question de ses limites. La question de l'identité numérique d'un travailleur et de son activité sur les réseaux sociaux, dont les frontières privées/professionnelles sont souvent floues, constitue également une question difficile à trancher.

Enfin, avec le développement des technologies d'intelligence artificielle (IA), une nouvelle phase semble se profiler, où la surveillance pourrait prendre une dimension encore plus problématique, du fait du caractère prédictif auquel pourraient prétendre certains systèmes[3].

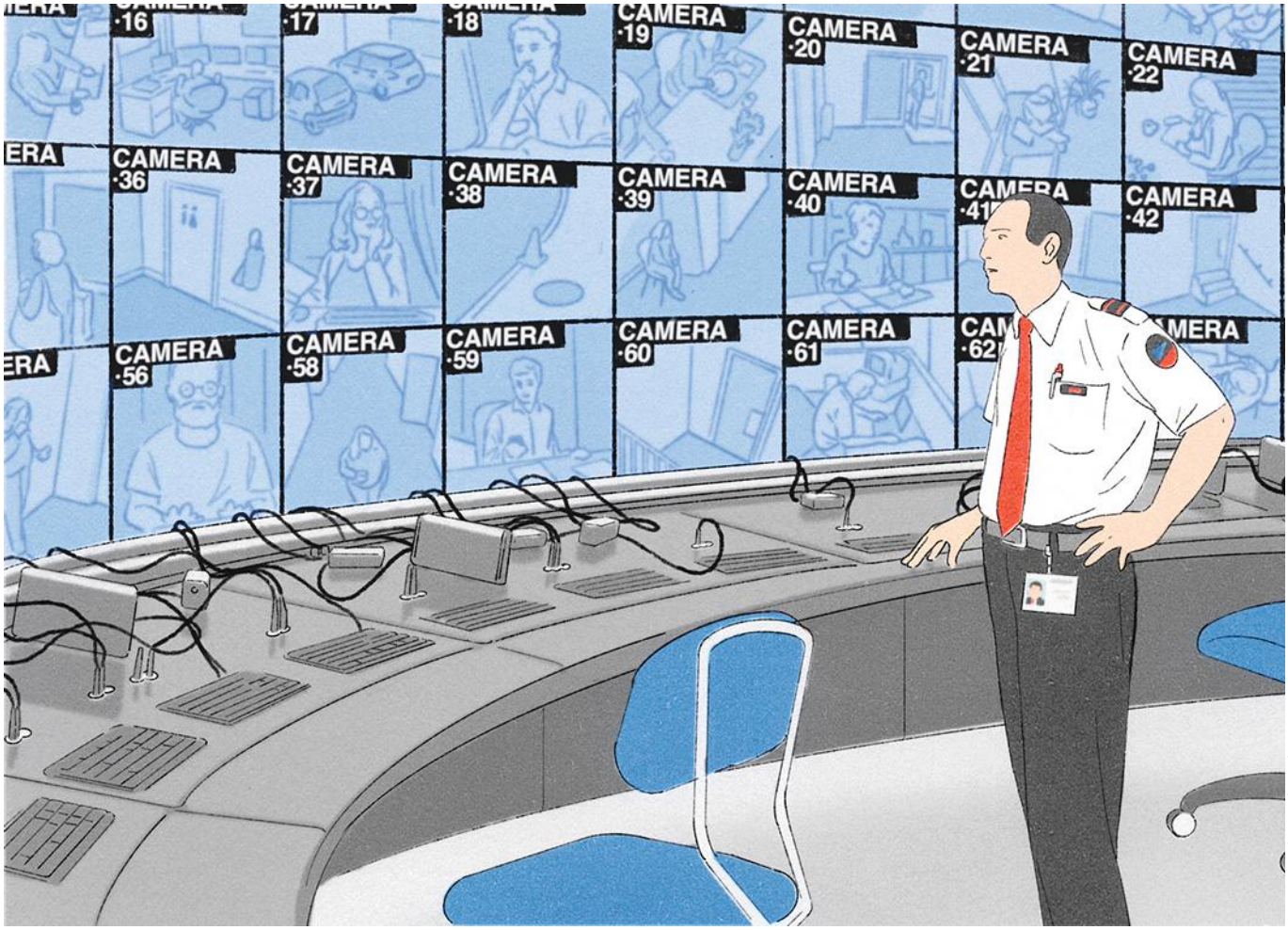
Une tendance accrue depuis la crise sanitaire

Au-delà des aspects technologiques qui ont permis ces évolutions, la surveillance au travail a été amplifiée en même temps qu'elle a changé de nature, à l'occasion de la pandémie de Covid-19. Dans les secteurs de la santé ou de la restauration, la nécessité de limiter les expositions au virus a, d'une part, conduit à l'adoption de mesures de surveillance des salariés empiétant sur le domaine de la vie privée (prise de température, extension du certificat de vaccination à de nombreux secteurs). L'instauration du télétravail obligatoire pour toutes les activités qui le permettaient a, d'autre part, amené une partie des managers, déstabilisés par ces nouvelles modalités de travail à distance, à recourir à des technologies de « *tracking* » permettant de suivre la présence effective et l'activité de leurs collaborateurs. De nombreux articles ont ainsi rapporté les excès de certains chefs d'équipe obligeant leurs collaborateurs à garder leur caméra allumée toute la journée, ou espionnant leur activité grâce à des logiciels illégaux en France[4]. Outre-Atlantique, un rapport canadien de l'initiative *Cybersecure Policy Exchange* et de la *Ryerson University* a été publié en août 2021 sur le sujet[5]. Revue de la littérature à l'appui, ce rapport établit que le recours à la surveillance est justifié de différentes façons : pour des raisons de responsabilité ou de gestion des risques, pour assurer la protection de la confidentialité ou enfin pour améliorer la productivité en influant sur le rendement économique des travailleurs. C'est cette dernière tendance qui s'est accentuée. Ainsi en 2019, 66 % des entreprises américaines ont déclaré surveiller l'usage d'Internet par leurs salariés et 45 % suivaient le temps actif sur clavier.

Si la loi française protège relativement bien les salariés, en exigeant notamment que le recours à des outils de surveillance soit soumis à l'avis des comités sociaux et économiques (CSE), certaines fonctionnalités d'outils numériques risquent tout de même d'être détournées de leur finalité initiale, de façon à permettre la surveillance du salarié à son insu. L'enquête Conditions de travail de 2019 montre ainsi que 35 % des salariés déclarent avoir un rythme de travail imposé par un contrôle informatisé[6]. Le rapport annuel de la Cnil pour l'année 2021 relève pour sa part une forte hausse des plaintes concernant les cas de surveillance abusive de salariés, impliquant dans 83 % des cas l'usage de dispositifs de vidéosurveillance (*via* des caméras dans l'entreprise, mais aussi *via* les webcams des ordinateurs du personnel). Ces plaintes concernent plus particulièrement des petites et moyennes entreprises, qui ne disposent pas en interne d'experts en matière juridique pouvant les alerter sur le caractère illégal de ce type de surveillance.[7]

De l'ambivalence du recours à la surveillance numérique

Si le plus souvent, l'idée même de surveillance par le biais de la technologie est associée à l'idée d'intrusion et de suspicion, certaines études se sont attachées à montrer qu'elle pouvait s'avérer au contraire utile aux managers dans l'exercice de leur fonction, à partir du moment où elle était perçue comme légitime par les salariés.



© Lucas Burtin pour l'INRS/2023

C'est le cas d'une étude conduite à l'EM Lyon en 2017[8] qui montre que les outils numériques constituent des outils « disciplinants » pour les salariés qui ont été informés de leur mise en place, limitant par exemple le temps passé sur Internet à des fins personnelles durant le temps de travail. Cet effet disciplinant peut cependant s'accompagner d'un effet d'éviction[9] lorsque ces outils sont perçus comme un signal de méfiance à l'égard des salariés de la part du management. L'étude conclut que l'équilibre entre ces deux effets réside dans la perception de leur légitimité par les salariés.

Cette légitimité repose sur deux éléments principaux :

- **Une communication transparente sur la finalité de la surveillance,** qui ne devrait pas cacher une fin moins acceptable pour les salariés : le malaise que peut susciter ce type de surveillance émane en effet principalement du fait qu'elle s'opère souvent par le biais d'un usage détourné de certains outils. C'est ce que souligne un rapport du Conseil national du numérique (CNNum[10]) au sujet des outils de communication instantanée tels que Slack, plateforme de communication collaborative qui, au-delà de faciliter la communication à distance des salariés, permettent à leur manager de surveiller de façon permanente leur présence à leur poste. Ce type de surveillance et l'injonction supposée d'une réponse immédiate peut représenter pour les salariés une cause de stress et d'anxiété.

  La finalité de cette surveillance peut cependant aussi être fondée sur l'intérêt même du travailleur. Elle peut notamment être utilisée à des fins de prévention. La géolocalisation peut par exemple être utile, afin de conseiller le parcours de circulation le plus sûr aux salariés en déplacement, ou détecter le fait qu'ils sont au volant pour transférer certains appels téléphoniques directement sur leur messagerie.

  Dans le cadre de ses travaux de prospective sur les usages de l'IA en prévention[11], l'INRS a ainsi montré l'intérêt que pourraient constituer à l'avenir les technologies d'IA pour surveiller les environnements de travail présentant des dangers ou surveiller les travailleurs isolés, afin de prévenir la survenue d'accidents ou de suivre leur état de santé.
- **Son caractère raisonné :** il est par ailleurs important que cette surveillance s'inscrive

→

dans un espace de temps et de lieu défini. Le caractère systématique, permanent ou inopiné de la surveillance dite « panoptique », que permettent les outils numériques, peut en effet induire un niveau de stress élevé, comme l'a montré une étude conduite par l'INRS au sujet des téléopérateurs de centres d'appels, concernant la relation entre facteurs organisationnels et contraintes psychosociales[12]. Cette étude soulignait en particulier les effets délétères des systèmes de double écoute, permettant aux superviseurs d'écouter en temps réel et d'enregistrer les conversations des opérateurs. Cette pratique a pour finalité de s'assurer que les employés utilisent bien les éléments d'un discours normalisé et que leurs interactions avec les clients sont conformes au standard préconisé. Cependant, elle se trouve également associée à une faible latitude décisionnelle qui, combinée à une forte exigence psychologique, induit un niveau de stress chronique élevé, mis en cause dans le développement de diverses pathologies (manifestations anxiodépressives, TMS, syndromes métaboliques), et constitue une source d'absentéisme.


© Annie Spratt

Ce type de surveillance pose encore davantage question dans le cas de travailleurs indépendants qui, par définition, n'ont pas de lien de subordination avec leurs donneurs d'ordres. Sophie Bernard, chercheuse et professeure de sociologie à l'université Paris – Dauphine, montre ainsi dans son ouvrage *#UberUsés*[13] comment le système des plateformes s'inscrit directement dans ce modèle de « surveillance panoptique » ; par exemple, les chauffeurs Uber sont soumis en permanence à un contrôle du système algorithmique qui fixe leurs objectifs et évaluent leurs performances, sans que celui-ci soit transparent pour eux.

De nouvelles évolutions en cours

Les nouvelles technologies d'IA et leurs capacités prédictives laissent par ailleurs entrevoir de nouvelles applications possibles en matière de surveillance, qui pourraient créer de nouvelles problématiques dans le domaine professionnel. Valerio De Stefano et Antonio Aloisi, professeurs de droit (universités de York et de Madrid), rapportent par exemple dans leur ouvrage *Your boss is an algorithm*[14] comment une IA développée par IBM permet de prédire à 95 % le risque de démission de salariés. Du fait des dérives possibles dans l'usage de ces nouveaux outils, les auteurs appellent de leurs vœux une plus grande implication des travailleurs dans la mise en œuvre des systèmes de management algorithmique, et souhaitent que les instances représentatives du personnel se saisissent de la question de la transformation digitale en cours.

Quel cadre juridique ?

Étant donné que ces évolutions technologiques donnent accès aux employeurs à de nouveaux outils de surveillance et de contrôle des salariés, la réglementation et la jurisprudence ont évolué pour préserver un cadre juridique protecteur des droits et des libertés. Parallèlement, la Cnil joue un rôle indispensable de régulation sur ces questions.

La surveillance numérique des salariés : un pouvoir limité de l'employeur

De manière générale, l'employeur peut surveiller et contrôler l'activité de ses salariés. Sous certaines conditions, les comportements du salarié considérés comme fautifs peuvent même faire l'objet d'une sanction disciplinaire. Mais, si ces prérogatives de l'employeur sont reconnues en vertu du lien de subordination, leur mise en œuvre reste très encadrée, notamment pour protéger les libertés individuelles des salariés. Ce cadre juridique, prévu initialement pour des techniques « classiques » de surveillance, trouve à s'appliquer

également en matière de surveillance numérique, y compris avec les outils les plus récents. Le système de surveillance que l'employeur envisage de mettre en place doit être justifié par la nature de la tâche à accomplir et proportionné au but recherché par l'employeur. Il s'agit d'un principe général gouvernant les relations individuelles de travail : « *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.* » *(Cf. Article L. 1121-1 du Code du travail).* Par exemple, le salarié a le droit au respect de sa vie privée. Ce droit fondamental, d'abord affirmé par la Déclaration universelle des droits de l'homme, adoptée par l'Organisation des Nations unies le 10 décembre 1948 (article 12), a été consacré au niveau européen par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales de 1950, qui prévoit que « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* » *(article 8, §1).* En 1970, le législateur français a modifié l'article 9 du Code civil, qui prévoit depuis que « *chacun a droit au respect de sa vie privée* », et précise quels sont les pouvoirs du juge pour faire cesser toute atteinte. La jurisprudence, en particulier l'arrêt Nikon de 2001[15], est venue préciser que le droit au respect de l'intimité de la vie privée du salarié s'applique même au temps et au lieu du travail.

Récemment, le recours massif au télétravail, qu'il soit contraint (isolement lié à la pandémie) ou choisi (organisation mise en place dans l'entreprise), a pu soulever de nouvelles questions en matière de surveillance numérique. En effet, beaucoup d'entreprises n'ont pas adapté leurs méthodes d'encadrement des salariés et d'évaluation de leur travail à ce mode d'organisation, mais les règles préexistantes permettent de sanctionner les abus. Par exemple, si les caméras sont utilisées depuis longtemps pour des questions de sécurité et pour contrôler, dans la mesure du raisonnable, l'activité des salariés, des situations relativement nouvelles de surveillance permanente des salariés en télétravail au moyen de webcams ont pu être constatées. La Cnil rappelle notamment qu'il est excessif de la part de l'employeur d'exiger que le salarié soit connecté en visioconférence pendant toute la durée du travail, afin de s'assurer qu'il est bien à son poste de travail, car il s'agit d'un dispositif de surveillance permanente qui ne peut être mis en œuvre. Cette position est équivalente à celle adoptée pour les caméras utilisées sur site[16]. De même, le partage d'écran en permanence et/ou l'utilisation de logiciels permettant d'enregistrer toutes les frappes effectuées sur le clavier de l'ordinateur, appelés « *keyloggers* », sont considérés comme des procédés invasifs de surveillance permanente et disproportionnés au regard du but recherché. Enfin, le fait d'obliger un télétravailleur à effectuer très régulièrement des actions (clics sur une application, photos, etc.) pour prouver qu'il est bien derrière son écran ne semble pas non plus compatible avec les principes applicables en matière de surveillance des salariés[17].

Non seulement le pouvoir de contrôle de l'employeur est limité, mais il doit également être exercé en respectant son obligation de loyauté.

Les obligations de l'employeur qui met en place un dispositif de surveillance numérique des salariés

L'employeur est tenu d'informer les salariés du projet de mise en œuvre de dispositifs de surveillance de leur activité : « *Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance* » *(Cf. Article L. 1222-4 du Code du travail).*

Le cadre juridique français est fixé par deux textes : la loi dite Informatique et Libertés[18] venue réglementer le traitement des données personnelles en 1978, et le Règlement général sur la protection des données (RGPD) entré en application en 2018[19]. Si, auparavant, les dispositifs de traitement de surveillance de l'activité des salariés devaient faire l'objet de formalités préalables auprès de la Cnil, aujourd'hui l'employeur doit les porter au registre des traitements, et effectuer une analyse d'impact à la protection des données (AIPD) en cas de risque élevé pour les droits et libertés des personnes concernées par la collecte des données. Concrètement, les traitements ayant pour finalité de surveiller de manière constante l'activité des salariés sont prohibés, sauf s'ils sont justifiés et proportionnés, auquel cas ils doivent faire l'objet d'une AIPD.

En tant que responsable du traitement des données personnelles, l'employeur se voit imposer par la réglementation européenne une obligation de transparence qui implique notamment de fournir un certain nombre d'informations au salarié concerné *(Cf. Articles 12 à 14 du RGPD).*

De même, il doit informer et consulter le CSE sur la mise en œuvre des moyens de contrôle de l'activité des salariés (*Cf. Article L. 2312-37 du Code du travail).*

Comme toute personne concernée par la collecte de ses données personnelles, le salarié bénéficie d'un droit d'accès aux données qui le concernent[20], c'est-à-dire qu'il peut demander à son employeur si de telles données sont traitées et en obtenir la communication, afin de vérifier leur exactitude et de pouvoir, si nécessaire, les faire rectifier, voire supprimer dans certains cas *(articles 15 à 17 du RGPD).*

→

Ce « droit à l'oubli » peut par exemple être exercé lorsque les données personnelles ont fait l'objet d'un traitement illicite ou si la personne concernée met en œuvre son droit d'opposition. Celui-ci permet au salarié de s'opposer, à tout moment, à ce que ses données personnelles apparaissant dans un fichier non obligatoire soient utilisées pour un objet précis, pour des raisons tenant à sa situation particulière. L'employeur ne traitera plus les données concernées, sauf s'il « *démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice* » *(Cf. Article 21 du RGPD*[21]*).*

Les évolutions juridiques liées aux usages de l'IA

En 2021, une proposition de règlement dite « *AI Act* » a été présentée par la Commission européenne ; elle vise à établir des règles harmonisées concernant les usages de l'IA[22]. Il s'agit de la première tentative, au niveau mondial, d'encadrement de l'IA par une institution politique. Dans l'exposé des motifs, la Commission souligne que « *l'intelligence artificielle recouvre un large champ de technologies en évolution rapide et peut procurer de nombreux avantages économiques et sociétaux dans l'ensemble des secteurs économiques et des activités sociales. […] Cela étant, les éléments et techniques qui rendent possibles les bénéfices socio-économiques de l'IA peuvent aussi être à l'origine de nouveaux risques ou de conséquences négatives pour les personnes ou la société. Au vu de la rapidité des évolutions technologiques et des éventuels défis à relever à cet égard, l'UE est déterminée à faire tout son possible pour adopter une approche équilibrée. Il est dans l'intérêt de l'UE de préserver son avance technologique et de faire en sorte que les Européens puissent bénéficier de nouvelles technologies dont le développement et le fonctionnement respectent les valeurs de l'Union et les droits et principes fondamentaux.* » La Commission a choisi une approche par niveau de risque : minimal, faible, haut, inacceptable, avec une réponse adaptée en fonction de chaque niveau. La proposition est encore en cours d'examen par les instances européennes. Le 14 juin 2023, le Parlement européen a validé l'*AI Act* avec quelques amendements, notamment en faveur d'une plus grande prise en compte des personnes concernées par les systèmes d'intelligence artificielle (SIA).

Risques professionnels et axes de prévention

Parmi les conséquences d'une surveillance excessive ou manquant de transparence sur sa finalité, l'étude canadienne de la *Cybersecure Policy Exchange* relève les possibles risques suivants : « *Au nombre des impacts négatifs d'une surveillance excessive en milieu de travail, c'est-à-dire lorsqu'elle dépasse ce qui est raisonnable ou nécessaire, mentionnons des effets psychologiques comme la faible estime de soi, l'anxiété et la dépression. Lorsqu'un employé vit un stress attribuable à une surveillance excessive, on peut observer l'apparition de symptômes, dont des lésions dues aux mouvements répétitifs ou des malaises musculosquelettiques […]. Les outils de surveillance perçus comme étant excessifs sont aussi associés à des taux élevés de roulement et d'absentéisme, à un moral bas, à une faible confiance en la direction, ainsi qu'à la détérioration des relations entre les employés et les employeurs.* »

Un autre risque de ce développement de la surveillance pèse plus directement sur la prévention des risques elle-même, car il pourrait amener à favoriser une approche individualisée de la prévention, au détriment d'une approche collective, plus efficace. Dans le cadre de ses travaux de prospective sur les usages de l'IA au service de la santé et sécurité au travail[11], l'INRS avait ainsi souligné que ces nouvelles fonctionnalités peuvent « *conduire à développer des outils de surveillance des travailleurs et d'alerte lorsque les conditions d'un travail en sécurité ne sont pas remplies (consignes non respectées, état de santé du travailleur hors norme, etc.). Cette surveillance permanente peut générer des risques psychosociaux et également conduire à une individualisation de la santé et sécurité au travail et à une responsabilisation exclusive du travailleur au détriment de la mise en place par l'employeur de mesures de prévention collectives* ».

Afin d'éviter le développement d'usages excessifs et potentiellement néfastes pour la santé des travailleurs, plusieurs mesures de prévention ont d'ores et déjà été proposées par l'INRS dans de précédentes publications. La recommandation de la Cnam (R 470), définissant les bonnes pratiques dans les centres d'appels, précise également que « *les modalités de suivi de la performance mises en place par le chef d'établissement devront être appropriées pour prévenir le sentiment de pression continue et de surveillance permanente* ».

L'INRS recommande ainsi de :

- vérifier que la collecte de données personnelles effectuées par ces équipements respecte le RGPD ;
- veiller à faire respecter le droit à la déconnexion ;
- favoriser la négociation d'accords d'entreprise instaurant une acception plus large du droit à la déconnexion en reconnaissant la possibilité de s'en prévaloir également durant le temps de travail (mise en place de périodes blanches sans connexion pour favoriser la concentration, les échanges interpersonnels entre collègues…) ;
- informer, consulter et impliquer les salariés dans le déploiement des outils de surveillance

numérique et conserver la possibilité de revenir en arrière s'ils s'avèrent plus nocifs que vertueux.

Les institutions européennes, telles que la Fondation européenne pour l'amélioration des conditions de vie et de travail (Eurofound) ou l'Agence européenne pour la santé et la sécurité au travail (EU-OSHA), appellent pour leur part à poursuivre le développement de la réglementation et de la négociation collective sur le sujet. Un rapport d'Eurofound paru en 2020[23] souligne ainsi que l'utilisation des technologies numériques a renforcé le potentiel de contrôle et de surveillance des travailleurs à distance et que les comités sociaux et économiques d'entreprise, ou d'autres formes de représentation des travailleurs, ont un rôle important à jouer pour fixer des limites à l'utilisation de technologies de surveillance intrusive des travailleurs.

De la même façon, un rapport de l'EU-OSHA sur la gestion des travailleurs par des systèmes d'IA[24] alerte sur le fait que ces systèmes peuvent renforcer le pouvoir de la hiérarchie et introduire de nouvelles formes de contrôle potentiellement oppressives sur les lieux de travail et de surveillance en dehors des lieux et des heures de travail. La loi sur le droit à la déconnexion instaurée en France constitue, selon cette institution, une étape importante dans la lutte contre ces pratiques. Outre son objectif premier de garantir aux travailleurs le droit de se déconnecter en dehors des heures de travail, il pourrait aussi servir de moyen pour garantir la protection de la vie privée et des données personnelles, en particulier lorsqu'il s'agit d'un contrôle et d'une surveillance disproportionnés et non strictement nécessaires. L'EU-OSHA propose, pour aller plus loin, l'instauration de mécanismes de signalement robustes qui pourraient inclure le signalement aux autorités publiques, ou encore le renforcement des capacités des inspecteurs du travail en collaboration avec les autorités nationales chargées de la protection des données.

Conclusion et perspectives

Comme l'expliquent Aloisi et De Stefano dans leur ouvrage cité précédemment, le recours au droit est le principal moyen d'éviter une progression d'évolutions potentiellement néfastes de ces pratiques pour les travailleurs. C'est une des raisons pour lesquelles les travaux en cours au niveau de l'Union européenne, en particulier ceux portant sur l'encadrement des usages de l'intelligence artificielle (*IA Act*), sont scrutés avec grande attention. ●

1. Si la surveillance numérique n'est pas systématique, la surveillance du travail de manière générale existe lorsqu'il y a subordination : il s'agit de la surveillance de la réalisation du travail et de l'évaluation de sa qualité.

2. Voir : https://www.cairn.info/revue-hermes-la-revue-2009-1-page-85.htm

3. Le caractère prédictif auquel il est fait ici référence peut prendre plusieurs formes : prédictif de la performance, de la productivité, de divers risques…

4. Voir : https://business.lesechos.fr/entrepreneurs/juridique/0702564137298-surveiller-ses-salaries-quand-la-tentation-est-trop-grande-349798.php

5. Voir : « La surveillance en milieu de travail et le travail à distance. En explorer les impacts et les répercussions en pleine pandémie de COVID-19 au Canada », *Cybersecure Policy Exchange, Ryerson University, août 2021.*

6. Voir : https://dares.travail-emploi.gouv.fr/enquete-source/conditions-de-travail-2019

7. Voir : https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_-_42e_rapport_annuel_-_2021.pdf

8. Voir : https://www.cairn.info/revue-economique-2017-5-page-843.htm

9. Au sens de : réduction des efforts du salarié.

10. Voir : https://cnnumerique.fr/files/uploads/2023/CNNum_Travailler_a_l_heure_du_numerique_corps_et_machines_2022_version_web.pdf ; p 129 : « La surveillance technologique entre dans le bureau ».

11. Voir : https://www.inrs.fr/media.html?refINRS=PV%2020

12. Voir : https://www.inrs.fr/media.html?refINRS=TF%20191

13. Voir : https://www.puf.com/content/UberUs%C3%A9s

14. Voir : https://www.bloomsbury.com/uk/your-boss-is-an-algorithm-9781509953189/

15. Voir : Cour de cassation (chambre sociale), 2 octobre 2001, pourvoi n°99-42942.

16. Voir : https://www.cnil.fr/fr/la-videosurveillance-videoprotection-au-travail, notamment pour un exemple de sanction de la Cnil prononcée contre un employeur ayant installé une caméra au-dessus du poste de travail d'un salarié.

17. Ces éléments font partie des points abordés dans les questions-réponses de la Cnil sur le télétravail, accessibles sur : https://www.cnil.fr/fr/les-questions-reponses-de-la-cnil-sur-le-teletravail

18. Voir : Loi n°78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés.

19. Règlement (UE) 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).

20. Sur le droit d'accès des salariés à leurs données personnelles, voir également : https://www.cnil.fr/fr/le-droit-dacces-des-salaries-leurs-donnees-et-aux-courriels-professionnels

21. Sur le droit d'opposition de la personne concernée par la collecte de ses données personnelles, voir également : https://www.cnil.fr/fr/le-droit-dopposition-refuser-lutilisation-de-vos-donnees.

22. Proposition de règlement du Parlement européen et du Conseil du 21 avril 2021 établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union. Voir : https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0020.02/DOC_1&format=PDF

23. Voir : Employee monitoring and surveillance: The challenges of digitalization. Accessible sur : *https://www.eurofound.europa.eu/en/publications/2020/employee-monitoring-and-surveillance-challenges-digitalisation*

24. Voir : https://osha.europa.eu/sites/default/files/artificial-inteligence-worker-management_en.pdf