

26^{ème} conférence internationale
sur la vie privée et la protection des données personnelles
Wroclaw, 14-16 septembre 2004

Session sur le thème de « La protection de la vie privée de l'employé et les intérêts de l'employeur »

Intervention de M. de Longevialle, Commissaire, Commission Nationale de l'Informatique et des Libertés, France

A l'heure de la révolution numérique et des réseaux l'homme au travail est « tracé » dans les ordinateurs de l'entreprise comme le pilote d'avion ou le conducteur de TGV le sont par les enregistrements de la boîte noire.

Est-ce que les intérêts de l'employeur ne vont pas l'inciter à une exploitation abusive de ces traces alors que les boîtes noires ne sont interrogées que dans des circonstances exceptionnelles et selon des procédures parfaitement définies et comment parer à ce risque, telle est la question mise en débat dans cette session.

Le contrat de travail se caractérisant par l'existence d'un lien de subordination du salarié à l'égard de l'employeur, est-ce que la protection des données personnelles et de la vie privée du cybertravailleur, du salarié à l'ère du numérique et de la société de l'information n'est pas une cause perdue d'avance ?

En prenant le risque d'être taxé de naïveté, ma réponse sera non.

M'appuyant notamment sur l'expérience et les travaux dans ce domaine de l'autorité française de protection, la CNIL, je crois pouvoir avancer que, malgré l'évolution technologique ou peut-être à cause d'elle, la reconnaissance et la garantie de la liberté individuelle et du droit à la vie privée dans la sphère de l'entreprise ont marqué des points dans la période récente. Ce sera mon premier point. Dans un deuxième temps j'illustrerai par des exemples tirés de l'actualité récente la façon dont l'autorité de contrôle que je représente entre en liaison avec les autres autorités et la façon dont les instances européennes tentent concrètement de concilier protection de la vie privée de l'employé et les intérêts de l'employeur.

- 1- Si la protection de la vie privée au travail a, comme je le crois, marqué quelques points, c'est que le cadre et les instruments juridiques d'une régulation des pouvoirs de surveillance de l'employeur se sont progressivement dégagés, clarifiés et mis en place et il ne me paraît pas exagéré d'affirmer ici que les législations informatique et liberté que nous sommes chargés de faire appliquer et que les autorités de contrôle que nous représentons ont joué dans cette évolution un rôle d'éclaireur et d'avant garde.

Quand sont arrivés dans les entreprises les autocommutateurs téléphoniques, les contrôles d'accès par badge électronique, la vidéosurveillance, l'internet, les moyens de géolocalisation (et j'en passe...), la nécessité s'est vite et partout fait sentir, d'un cantonnement par le droit (sans préjudice éventuellement d'autres régulations) des risques d'atteinte à la vie privée des travailleurs.

Mais il est d'abord apparu que le droit du travail pouvait se révéler parfois relativement désarmé devant des problématiques nouvelles. Fallait-il aller vers de nouvelles clauses du contrat de travail ? Fallait-il utiliser ou au contraire bannir la voie du règlement intérieur ? La jurisprudence judiciaire sur la cause réelle et sérieuse du licenciement pouvait limiter les dégâts mais les solutions étaient parfois contradictoires et, de toute façon, l'allocation de dommages et intérêts en cas de licenciement abusif peut-elle être considérée comme constitutive d'une protection suffisante ?

- 2- Pendant que le droit du travail cherchait ainsi ses réponses, les autorités de contrôle (que nous représentons) se sont avancées – je dirais presque sans y prendre garde – sur le terrain des relations entre employeur et salariés simplement en mettant en œuvre les pouvoirs qu'elles tiennent de leurs législations nationales de protection des données personnelles et de la vie privée...

Car, pour nous, qu'est-ce, par exemple, qu'un autocommutateur téléphonique, sinon un équipement mettant en œuvre des traitements automatisés de données nominatives qui devra donc, comme tel, être préalablement déclaré ou autorisé et auquel nous allons appliquer une grille d'analyse bien connue : quelles sont les finalités poursuivies par le traitement, quelles données sont collectées, pour combien de temps, comment les personnes concernées ont-elles été informées, comment s'exerce le droit d'accès, qui est destinataire des données, etc.

Une démarche pour nous tellement habituelle mais qui a pour effet de faire entrer le droit des libertés publiques dans la sphère des relations de travail. Je voudrais citer ici le rapport remis en 1991 par le professeur Gérard Lyon-Caen sur les libertés publiques et l'emploi qui analyse ce qu'il appelait une tendance à la constitutionnalisation du droit du travail et mis en lumière l'existence, sous le travailleur, de la personne bénéficiaire des libertés constitutionnelles et en particulier du droit fondamental au respect de la vie privée.

- 3- « Donnez-moi un point d'appui » réclamait ce savant de l'antiquité. Pour la régulation juridique des pouvoirs de surveillance de l'employeur dans le contexte des NTIC, ce point d'appui, dont tout le reste découle, c'est la reconnaissance d'un droit inaliénable à la vie privée du travailleur. Ce droit, celui de la liberté individuelle, est le principe et l'employeur ne peut lui apporter des restrictions qu'autant qu'elles sont nécessaires pour la bonne marche de l'entreprise et proportionnées au but poursuivi. C'est exactement ce que dit l'article L 120-2 introduit dans le code français du travail à la suite du rapport Lyon-Caen : « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restriction qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ». Finalité et proportionnalité, ces concepts qui se sont révélés opératoires dans le droit informatique se trouvent désormais incorporés dans le droit du travail.

La jurisprudence a consacré cette évolution. Je me réfère ici à deux décisions, d'abord celle rendue en 1992 par la Cour Européenne des droits de l'homme, dans l'affaire Halford contre Royaume-Uni, par laquelle la cour a affirmé que l'article 8 I de la convention, selon lequel toute personne a droit au respect de sa vie privée et familiale, de son domicile et de la correspondance, est applicable pour la protection d'appels téléphoniques lancés de locaux professionnels. La seconde décision, tout à fait dans le même sens, est l'arrêt Nikon du 2 octobre 2001 par lequel la Cour de Cassation française affirme « Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée : celle-ci implique en particulier le secret des correspondances. L'employeur ne peut dès lors, sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail, et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur ».

Grâce à une évolution qui s'est déroulée en parallèle au niveau national, au niveau communautaire et au Conseil de l'Europe et dans le cadre plus large d'institutions internationales, telles que l'OIT, on peut conclure que le pouvoir de surveillance de l'employeur se trouve soumis à un encadrement juridique qui a tiré des législations de protection des données personnelles à la fois son inspiration et ses moyens d'action et qu'il existe aujourd'hui sur cette approche une forte convergence dans plusieurs régions du monde.

* *
*

Dans une communication à un précédent colloque, le professeur Reidenberg avait constaté qu'étaient en réalité en concurrence trois régulations protectrices des données personnelles : une régulation par le droit (l'approche européenne), une régulation par le marché ou autorégulation (l'approche américaine), enfin la régulation par la technologie (la « lex informatica ») à travers certains dispositifs des infrastructures ou des protocoles de fonctionnement des réseaux et il exprimait l'opinion qu'une protection optimale serait celle qui résulterait de l'articulation et la combinaison de ces trois régulations.

Quoi qu'il en soit, pour que ce concert ait lieu, encore fallait-il que la régulation juridique ait trouvé ses instruments... Il me semble que l'objectif n'est pas loin d'être atteint aujourd'hui.

Des instruments régulateurs ayant été trouvés, voyons, par quelques exemples, comment les autorités de régulation et en particulier la CNIL les utilisent.

La recherche permanente du meilleur équilibre entre les prérogatives de l'employeur et le respect de la vie privée au travail

La CNIL a défini une méthode pour atteindre son objectif de protection de la vie privée des employés.

Cette méthode s'appuie largement sur l'étude des problèmes et la concertation avec les organisations professionnelles d'employeurs et d'employés. Elle pourrait se résumer dans le triptyque « identification du risque - recommandation - contrôle ».

La phase d'identification du risque s'appuie d'une part sur les déclarations de traitements de données personnelles, les demandes de conseil et les plaintes reçues, ainsi qu'en complément les résultats de missions d'information menées

sur place dans les entreprises, et d'autre part sur la veille juridique et technique réalisée en par les services de la Commission. Cette phase d'identification des problèmes permet d'évaluer l'impact « informatique et libertés » d'une nouvelle technologie, d'un nouveau procédé ou d'une nouvelle réglementation, et de déterminer si une action particulière de la CNIL est nécessaire ou non en ce domaine.

La phase de recommandation s'appuie le plus possible sur la concertation avec les organisations professionnelles, voire les industriels porteurs de la technologie concernée, puis sur une diffusion des « règles du jeu » souhaitables au moyen du site internet de la CNIL, via ses publications régulières et, le cas échéant, par une opération de communication ciblée. Elle se décline au quotidien par l'information et le conseil des employeurs et des employés. Elle comporte également une dimension européenne avec la participation active de la Commission au « groupe de travail de l'article 29 » qui se saisit régulièrement des questions de vie privée sur le lieu de travail.

Enfin, la phase de contrôle intervient lors du contrôle *a priori* des traitements déclarés à la CNIL, mais elle consiste également à conduire des missions de vérification sur place auprès des employeurs privés et publics. Ces missions, qui sont de plus en plus souvent mises en œuvre par la CNIL, peuvent l'amener à adapter les « règles du jeu » initialement établies.

Sur la base de cette méthodologie en trois temps, la Commission a élaboré au fur et à mesure de l'apparition des nouvelles technologies un corpus de recommandations dont je donnerai trois exemples.

1) Contrôle des communications téléphoniques

La CNIL a rappelé d'une part que l'écoute et l'enregistrement des conversations téléphoniques sur le lieu de travail sont interdits sauf justification particulière (tenant à des circonstances exceptionnelles ou à la spécificité de certaines activités) et peuvent être pénalement sanctionnés.

Au titre des exceptions, elle a pu accepter l'enregistrement de conversations dans un centre d'appels à des fins de formation des personnels, à la condition que cet enregistrement soit réalisé sur une brève période, après information des employés concernés, et soit détruit à l'issue de la formation.

Enfin, la CNIL a d'autre part recommandé que l'employeur n'accède aux relevés individuels d'appels téléphoniques que de façon exceptionnelle, par exemple en cas d'augmentation anormale des appels constatée sur la base de statistiques globales ou par service. De plus, elle demande que les quatre derniers chiffres des numéros appelés ou appelants soient occultés des relevés individuels pour ne pas porter atteinte à la vie privée des employés.

2) Biométrie

Depuis la fin des années quatre-vingt-dix, la CNIL a eu l'occasion d'examiner de nombreux projets informatiques visant à l'introduction de dispositifs biométriques sur les lieux de travail.

Ces dispositifs, reposant essentiellement sur la reconnaissance de l'empreinte digitale, avaient pour objet soit le contrôle des accès à des locaux professionnels, soit le contrôle des temps de travail, soit encore le contrôle des accès au système d'information interne.

Compte tenu des risques de détournement de finalité, la CNIL opère une distinction entre deux types de biométries : celles qui reposent sur la reconnaissance de caractéristiques humaines qui « laissent des traces » (telles que l'empreinte digitale), et celles qui reposent sur des caractéristiques « qui ne laissent pas de traces » (telles que le contour de la main).

En application du principe de proportionnalité, elle considère qu'un employeur ne peut constituer une base de gabarits biométriques « qui laissent des traces » qu'à condition de démontrer l'existence d'un impératif particulier de sécurité (contrôle des accès aux guichets de la Banque de France, à une centrale nucléaire, aux zones réservées d'un aéroport).

A titre d'illustration, elle s'est systématiquement opposée au stockage de gabarits d'empreintes digitales dans une base de données pour des finalités de contrôle du temps de travail.

En revanche, elles estiment que le recours à des techniques « sans trace » ne pose normalement pas de problème de proportionnalité.

Elle n'est toutefois pas opposée au recours à des biométries « qui laissent des traces » pour des finalités autres que sécuritaires, à condition que le gabarit biométrique soit stocké sur support individuel, assurant ainsi à l'employé une maîtrise complète sur les données biométriques qui le concernent.

Il est d'ailleurs intéressant de constater que ce type de stockage sans risque semble être tout à fait adapté pour des traitements à finalité sécuritaire (par exemple pour la sécurisation des aéroports), ce que la CNIL encourage. Cette approche est en ligne avec celle élaborée avec nos homologues au plan européen (document de travail du 1^{er} août 2003).

3) Cybersurveillance

Je reviendrai en terminant sur la question de la cybersurveillance, le contrôle de l'utilisation par les employés de l'Internet et des réseaux, une des questions que l'autorité française a le plus approfondie et sur laquelle, dans le cadre européen, le groupe de l'article 29 a adopté (sous la présidence du Professeur Rodotà) un avis qui fait aujourd'hui autorité, et sur les solutions duquel il existe une réelle convergence.

- L'arrêt Nikon a été rendu à propos d'un employé qui avait pris connaissance du contenu d'un mail dans une entreprise où l'utilisation à des fins personnelles des équipements de messagerie mis à disposition avait été prohibée. Mais la portée exacte de cette décision n'a pas été bien analysée. Il est erroné d'en tirer la conclusion que la cour a entendu dénier le droit pour l'employeur d'interdire un usage non professionnel des outils informatiques. Tout un courant jurisprudentiel s'est développé dans la période récente sur la responsabilité civile du commettant en cas d'utilisation fautive par le préposé du matériel informatique de l'entreprise. Il est non seulement de la compétence mais aussi du devoir de l'employeur de prendre les mesures nécessaires à la sécurité et à l'utilisation régulière du système informatique de l'entreprise. La CNIL dénonce donc comme fausse l'idée que la loi informatique et liberté interdirait tout contrôle individuel de l'activité du salarié.

- La CNIL ne méconnaît donc nullement les prérogatives de l'employeur, mais elle estime, à la lumière de l'expérience, qu'une interdiction absolue d'utilisation à des fins personnelles des équipements mis à disposition des employés est irréaliste, peut être disproportionnée et souvent difficile. Elle plaide donc pour l'admission d'une utilisation personnelle dans des limites raisonnables des équipements mis à disposition par l'entreprise. Aujourd'hui elle constate avec satisfaction que cette position a été reprise à son compte par le groupe de l'article 29 et qu'elle trouve une traduction dans de nombreuses chartes ou codes de bonne conduite que de nombreuses entreprises (et notamment parmi les plus grandes) ont mis en place.

- Autre point, face aux abus de l'utilisation de dispositifs de prise en main à distance permettant de contrôler le poste informatique de tout employé y compris à son insu, la CNIL pense qu'elle devra exposer de nouveau ses recommandations en rappelant que sauf circonstances particulières l'utilisation de telles fonctionnalités n'est conforme au principe de proportionnalité qu'à des fins de télémaintenance informatique assurée par un nombre limité d'informaticiens et non pas à des fins de supervision des personnels par les supérieurs hiérarchiques ou les responsables des ressources humaines.

- je préciserai mon propos en parlant de l'administrateur de réseaux. Ce responsable dispose, dans le cadre de ses attributions, d'un accès à l'ensemble des données enregistrées des employés, y compris celles de nature personnelle. Pour autant, cette habilitation technique ne signifie en aucun cas selon nous que l'administrateur a le droit, par principe, d'accéder à tout moment à ces données et à toutes fins. Cet accès ne peut être justifié qu'en cas de nécessité technique et lorsque le bon fonctionnement des réseaux ne peut être assuré par d'autres moyens moins intrusifs. Je terminerai en soulignant le rôle fondamental de l'administrateur réseau pour une conciliation dans "l'entreprise numérique" du droit des employés à la vie privée et des intérêts légitimes de leur employeur. La question de savoir si l'administrateur de réseau devrait ou non être doté d'un statut ou astreint au secret professionnel est une question qui va se poser de plus en plus...

* *
*

Conclusion

Pour résumer l'état d'esprit de l'autorité que je représente, l'intitulé de cette session – « La protection de la vie privée et les intérêts de l'employeur » - ne doit en aucun cas sonner comme une mise en opposition de deux objectifs qui seraient par nature incompatibles.

En tant qu'autorité de contrôle, il nous appartient au contraire de souligner le caractère indissociable de ces deux objectifs.

Ce faisant, nous contribuons certainement à l'émergence de conditions propices à la mise en œuvre d'un climat de confiance dans les lieux de travail, dans l'intérêt de tous et de chacun.