informatique et entreprises

Par **nonomayor**, le **27/01/2005** à **23:50**

Je souhaiterais connaître les limites du contrôle de l'administrateur d'un réseau informatique (d'entreprise ou d'administration), en matière de logiciels et de fichiers illégaux présent sur les ordinateurs.

Plus concrètement:

- Lors d'un contrôle par les autorités judiciaires si des logiciels non utiles à l'exécution du travail, ou des fichiers de type MP3 ou Divx illégaux, sont découverts sur un ordinateur, qui sera responsable? l'employé-utilisateur de l'ordinateur ou l'employeur selon l'article 1384 c.civ.?
- Si c'est l'employeur, celui-ci peut-il, pour se prémunir de ce risque, demander à son administrateur réseau de vérifier (sur place ou à distance) les logiciels et documents présents sur l'ordinateur sans violer la vie privée de l'employer?
- L'ordinateur est-il un outil de travail de l'entreprise? ou l'employé est il considéré comme le gardien de l'ordinateur?
- Les conditions sont-elles les mêmes pour une entreprise et une administration?

Je vous remercie par anticipation de bien vouloir m'éclairer sur ces points !

Par **jeeecy**, le **28/01/2005** à **09:30**

je déplace le sujet end roit social car c'est la qu'il a sa place

en effet il s'agit d'exposer les moyens de controle du dirigeant d'entreprise sur ses employes...

je ne sais plus le fondement mais je crois que le dirigeant a le droit de controler les disques durs des employes s'il les a prevenu avant

toutefois ce controle ne peut etre que ponctuel et pour des raisons precises

En effet il s'agit du respect de la vie privée. L'ordinateur peut contenir des données personnelles et donc l'employeur ne peut pas demander a son administrateur de rechercher des fichiers illégaux entre autres...

Il faudrait demander à un spécialiste de droit social mais si mes souvenirs sont bons ca doit etre ca...

Par **nonomayor**, le **29/01/2005** à **20:18**

Alors voila j'ai trouver quelques informations pour repondre à mes questions, j'aime les monologues... donc si ca vous interesse (ca m'etonnerait) j'ai compilé une petite réponse:

[size=150:18wmxutq][b:18wmxutq]Le rôle légal de l'administrateur réseaux[/b:18wmxutq][/size:18wmxutq]

L'aspect légal de la fonction d'administrateur réseau met celui-ci dans une position délicate. En effet d'une part il est soumis à son employeur qui est le commettant des utilisateurs du réseau et le propriétaire du matériel informatique, et d'autre part il doit veiller au respect de la vie privée des employés puisqu'il a accès de par son rôle à des informations personnelles. Ainsi il doit veiller à une utilisation et à fonctionnement du matériel informatique en concordance avec le droit positif sous peine d'exposer son employeur et lui-même à des poursuites judiciaires en vertu du principe de responsabilité des commettants pour leurs préposés. Après avoir étudié les justifications de la nécessité d'un contrôle par l'employeur (I), nous verrons les modalités et les limites de ce contrôle (II)
[color=red:18wmxutq]I) Les justifications du contrôle par l'employeur et l'administrateur réseaux[/color:18wmxutq]
L'article 1384 du code civil dispose « On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde.». Cet article est le fondement principal de la justification du contrôle par les employeurs. En l'espèce ceux-ci justifient le contrôle du matériel informatique, d'une part car il en sont propriétaire et gardien donc responsables (A) et d'autre part car toute responsabilité d'une infraction commise par un préposé, et notamment par le bief d'un outil informatique, leur incombe (B).

[color=green:18wmxutq]A) Le droit de propriété[/color:18wmxutq]
« Là où est la propriété, là est le pouvoir ». Cette phrase de François Mitterrand pourrait parfaitement illustrer l'un des fondements mis en avant à l'appui du pouvoir de contrôle de l'employeur. Le pouvoir de contrôle exercé sur l'utilisation de la chose, c'est avant tout le pouvoir du propriétaire sur son bien. De plus le droit de propriété est défini par l'article 544 du code civil qui dispose « la propriété est le droit le de jouir et de disposer des choses de la manière la plus absolue, pourvu qu'on en fasse pas un usage prohibé par les lois ou par les règlements ». Cette définition attribue trois prérogatives au propriétaire d'un bien : l'usus, l'abusus et le fructus. On comprend dès lors que cette disposition soit légitime à fonder un contrôle de l'employeur sur l'usage des biens professionnels. D'ailleurs contrairement à l'idée reçue, sauf clause contraire dans le contrat de travail, un ordinateur mis à la disposition d'un salarié ou d'un agent public dans le cadre de la relation de travail est la propriété de l'entreprise ou de l'administration et ne peut comporter que subsidiairement des informations relevant de l'intimité de la vie privée. Il peut être protégé par un mot de passe et un login, mais cette mesure de sécurité est destinée à éviter les utilisations malveillantes ou abusives par un tiers; elle n'a pas pour objet de transformer l'ordinateur de l'entreprise en un ordinateur à usage privé. Par ailleurs l'employé dispose du droit d'accès au matériel mais l'entreprise reste gardienne de la chose mise à la disposition de son salarié pour exécuter le travail, or la jurisprudence affirme que« être gardien c'est détenir le pouvoir d'usage, de contrôle et de direction de la chose »
C'est ainsi que la responsabilité de l'employeur se fonde non seulement sur l'autorité qu'il détient sur ses préposés, mais aussi sur celle qu'il possède sur les choses. Le risque

d’engagement de la responsabilité de l’employeur peut être illustré par une décision du TGI de Marseille datée du 11 juin 2003 qui retient la responsabilité d’un employeur au visa de l’article 1384, alinéa 5 du Code civil en raison de la fourniture par l’entreprise d’un accès Internet. En effet, un salarié avait pendant son temps de travail et à l’aide de son ordinateur à usage professionnel, construit un site critiquant, voire insultant la politique menée par une société exploitant des autoroutes. Le juge a retenu la responsabilité de l’employeur de ce salarié au motif que la direction avait émis une note autorisant la libre consultation des sites Internet mais n’imposant "aucune interdiction spécifique […] quant à l’éventuelle réalisation de sites Internet ou de fourniture d’informations sur des pages personnelles". En conséquence, le juge en déduit que la faute du salarié "a été commise dans le cadre des fonctions auxquelles il était employé". Cette décision qui peut être qualifiée de sévère est un exemple des risques de responsabilité encourus par les employeurs en fournissant un accès Internet et du matériel informatique à leurs salariés. Ce mouvement d’élargissement de leur responsabilité rend légitime la préoccupation des employeurs. Nous pouvons tout de même ajouter que selon la ligne jurisprudentielle adoptée à l’heure actuelle par la Cour de cassation, l’employeur conserve la possibilité de voir sa responsabilité partagée avec celle de son salarié dans le cas où la faute ne présente qu’un lien ténu avec les fonctions assignées au travailleur.

[color=green:18wmxutq]B) La responsabilité du commettant[/color:18wmxutq]
La mise en avant de leur responsabilité par les employeurs pour justifier leur pouvoir de contrôle s’explique également par les conséquences d’éventuelles infractions pénales commises par leurs subordonnés. L’arrêt de l’Assemblée plénière du 19 mai 1988 précise que « le fait que le préposé ait commis une infraction pénale, quelle qu’en soit la gravité, n’exclut pas en soi le rattachement de la faute à l’exercice des fonctions et donc à la responsabilité civile du commettant ». Cette formulation accroît encore le risque pour l’employeur de devoir répondre des agissements de son salarié. Cependant, certaines infractions pénales n’entraînent pas le déclenchement de ce mécanisme de responsabilité prévu à l’article 1384, alinéa 5 du Code civil. C’est ainsi que suite à l’arrêt Cousin du 14 décembre 2001, on peut avancer avec certitude que les infractions supposant chez l’auteur l’intention de causer un dommage à autrui caractérisent nécessairement une faute dissociable des fonctions, entraînant la seule responsabilité personnelle du salarié. Il faut bien sûr exclure de cette analyse les délits où l’intention ne résulte que d‘une conception abstraite. Dans ce contexte, les risques pour un employeur de voir sa responsabilité engagée suite à des infractions fréquemment citées en exemple dans les débats concernant l’usage d’Internet telles que les consultations de sites pédophiles ou encore la fraude informatique, semblent relativement limités. Le droit positif semble préserver le commettant du risque d’engager sa responsabilité dans ces hypothèses.
Une autre inquiétude présente est celle d’une éventuelle condamnation pénale de l’employeur (article 121-2 c.pén.). En effet la Cour de cassation a posé dans son arrêt Costedoat du 25 février 2000 le principe selon lequel « n’engage pas sa responsabilité à l’égard des tiers le préposé qui agit sans excéder les limites de la mission qui lui a été impartie par son commettant ». Ce régime de responsabilité inspiré directement de celui prévu en cas de faute de service de l’agent public, prévoit que l’employeur sera comptable des fautes de son préposé si cette faute entre dans le cadre de sa mission ou, quoique détachable de cette dernière, la faute n’est pas dépourvue de tout lien avec les fonctions du préposé. Dans ce dernier cas, les responsabilités de l’employeur et de son salarié seront cumulativement engagées. Cette clarification, intervenant après une opposition persistante entre la chambre civile et la chambre criminelle, accorde pour certains une véritable immunité du préposé ayant agi dans le cadre de ses fonctions. Le salarié voit sa protection vis à vis des tiers fortement renforcée. Concernant la faute détachable, un arrêt de l’Assemblée plénière de la Cour de

cassation du 19 mai 1988 a retenu que « le commettant ne s'exonère de sa responsabilité que si le préposé a agi hors des fonctions auxquelles il était employé, sans autorisation et à des fins étrangères à ses attributions ». La chambre civile précisera a contrario qu'il suffit, pour que la responsabilité du commettant soit engagée, que le préposé ait trouvé dans ses fonctions « l'occasion et les moyens de sa faute ». Cette solution s'avère intéressante dans notre domaine d'étude, l'employeur fournissant au salarié la matériel nécessaire à la réalisation du comportement sanctionnable. On peut donc considérer que la mise à disposition de l'outil informatique pourrait être considéré comme la fourniture des moyens et de l'occasion nécessaires à la commission d'une faute. Le salarié peut tout d'abord commettre un acte incriminé par la loi Godfrain du 5 janvier 1988. Cette initiative législative sanctionne la fraude informatique en interdisant l'accès et le maintien dans un système de traitement automatisé de données (article 323-1 c.pén.), ainsi que les atteintes ayant pour finalité de toucher le système (article 323-2 et 3 c.pén.). Les travailleurs peuvent également se rendre coupables d'atteintes à la personne humaine telles que la diffusion d'images pédophiles (article 227-23 c.pén.) ou encore de délits plus traditionnels comme le vol ou le recel de données sans tire de licence. L'employeur encourt-il une responsabilité d'ordre pénal pour de tels agissements de la part de son subordonné ? L'article 121-7 du Code pénal pose qu'« est complice d'un crime ou d'un délit la personne qui sciemment, par aide ou assistance, en a facilité la préparation ou la consommation ».La rédaction de cette disposition révèle rapidement que la recherche du caractère intentionnel de l'acte ou tout du moins de la connaissance des agissements de l'auteur principal de l'infraction, est requise pour retenir la responsabilité pénale d'une personne physique ou morale au titre de la complicité. Dès lors, il devient difficile de retenir la responsabilité pénale d'une entreprise par la simple fourniture de moyens informatiques. Cette difficulté d'application du système de responsabilité créé par l'émergence des nouvelles technologies et de leurs organisations induit de véritables difficultés. L'identification du supérieur hiérarchique ou de l'employeur responsable a toujours constitué une difficulté notable pour le droit. Pour tenter de se prémunir contre ce risque les employeurs les employeurs adoptent de plus en plus des chartes, qui ne sont cependant pas des protections absolues puisque ce sont des règles interne et donc de valeur inférieur aux lois.

Ces arguments plaident en faveur d'un accès et d'un contrôle total des postes de travail lorsque des adminicules laissent penser à l'employeur que son préposé utilise le matériel à des fins illégales. Cependant la vérification peut porter atteinte à la vie privée, c'est pourquoi ces contrôles sont très réglementés.

[color=red:18wmxutq]II) Les moyens et les limites du contrôle [/color:18wmxutq]
Depuis la fin des années 60 où le modèle de l'autorité a été contesté, le recul du pouvoir discrétionnaire de l'employeur a été l'une des caractéristiques majeures de la métamorphose juridique des formes d'exercice du pouvoir. L'employeur se voit donc contrôlé a priori avec une exigence sans cesse croissante de motivation de ses actes, et contrôlé a posteriori avec un rôle accru du juge. Cette exigence procédurale ne vise en fait qu'à limiter l'arbitraire du pouvoir. Ainsi le contrôle se fait de manière très encadrée (B) et le plus souvent par une personne ad hoc (A).

[color=green:18wmxutq]A) Le rôle de l'administrateur réseaux : protection de l'entreprise et protection de l'individu[/color:18wmxutq]
L'installation d'un système de surveillance et son fonctionnement se fait sous l'autorité de l'administrateur réseau ou du directeur des systèmes informatiques. Ces supérieurs

hiérarchiques intermédiaires bénéficient d'ailleurs la plupart du temps de délégations de pouvoir. Ces derniers seront donc considérés comme les auteurs des éventuelles infractions pénales commise à l'occasion de l'utilisation de tels procédés de contrôle; on pense notamment aux sanctions pénales de la violation du secret des correspondances (articles 226-15 c.pén., et article 432-9 c.pén. pour les agents publics). Les mécanismes de droit pénal n'acceptent pas l'ordre donné par une autorité comme une contrainte absolue de nature à faire disparaître la responsabilité de l'auteur. Ainsi, même si l'employeur pourra être reconnu complice, le directeur informatique restera l'auteur principal de l'infraction. Le conflit de logique du droit pénal avec celle du droit du travail invite donc à réfléchir sur l'inadaptation des règles actuelles de responsabilité appliquées aux nouvelles technologies.
En effet les administrateurs qui doivent veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes sont conduits par leurs fonctions même à avoir accès à l'ensemble des informations relatives aux utilisateurs (messagerie, connexions aux sites internet, fichiers "logs" ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail. Un tel accès n'est contraire à aucune disposition de la loi du 6 janvier 1978 concernant l'informatique et les libertés. L'utilisation encadrée de logiciels de télémaintenance qui permettent de détecter et réparer les pannes à distance ou à prendre le contrôle, à distance, du poste de travail d'un salarié ne soulève aucune difficulté particulière au regard de la loi du 6 janvier 1978 à condition que les mesures de sécurité nécessaires à la protection des données soient mises en œuvre. D'ailleurs un arrêt de la Cour d'appel de Paris du 17 décembre 200156 a estimé que « la préoccupation de la sécurité du réseau justifiait que les administrateurs de systèmes et de réseaux fassent l'usage de leurs positions et des possibilités techniques dont ils disposaient pour mener les investigations et prendre les mesures que cette sécurité imposait ». Cet exemple pourrait être un premier pas des tribunaux vers la reconnaissance de l'impératif de sécurité informatique dans les entreprises. Certains auteurs appuient d'ailleurs cette démarche en proposant aux juges d'adopter le critère de « légitime surveillance »
Par contre aucune exploitation à des fins autres que celles liées au bon fonctionnement et à la sécurité des applications des informations dont les administrateurs de réseaux et systèmes peuvent avoir connaissance dans l'exercice de leurs fonctions ne saurait être opérée, d'initiative ou sur ordre hiérarchique. Tenus au secret professionnel, les administrateurs de réseaux et systèmes ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'entreprise. Ils ne sauraient non plus être contraints de le faire, sauf disposition législative particulière en ce sens.

[color=green:18wmxutq]B) Les limites du contrôle : un encadrement rigoureux[/color:18wmxutq]
La question des limites du pouvoir d'acces aux differents postes de travail, et du contrôle de l'employeur dans l'entreprise est essentielle. Tout d'abord, l'outil informatique et les logiciels d'exploitation fournissent aux employeurs des moyens sans commune mesure de surveillance des postes de travails des salariés et plus ou moins directement des salariés eux même. Les nouvelles technologies sont, sous cet angle, vecteur de la multiplication des atteintes possibles à la vie privée et plus largement de violation des limites du pouvoir de contrôle de l'employeur. L'article 9 du Code civil, issu de sa rédaction remodelée par la loi du 17 juillet

1970 affirme avec force que « chacun a droit au respect de la sa vie privée ». Cette règle va peu à peu s'enraciner dans les différentes branches du droit et devenir un droit fondamental attaché à la personne.La vie privée fait également l'objet d'une protection au niveau européen. Elle est tout d'abord reconnue par l'article 8 de la Convention Européenne des Droits de l'Homme, intitulé « droit au respect de la vie privée et familiale », qui énonce que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance »et de plus la Cour Européenne des Droits de l'Homme en fait une interprétation extensive. La consécration de cette nouvelle notion de vie personnelle interviendra avec l'arrêt Nikon à l'occasion d'une question touchant l'utilisation d'Internet au sein de l'entreprise. Les juges affirment sans détour que « même au temps et au lieu de travail, le salarié a droit au respect de l'intimité de sa vie privée, qui inclut en particulier le secret des correspondances ».
D'autre part le contrat de travail suppose l'existence d'un lien de confiance entre l'employeur et le salarié. La relation de subordination, si inégalitaire soit-elle, réclame l'adoption de certains comportements par les parties. L'entreprise est une communauté qui ne peut durer si elle est fondée sur la déloyauté. Le pouvoir de contrôle de l'employeur est donc invité à la transparence dans son exercice.La loyauté « imprègne le droit tout entier au travers du principe de bonne foi ». Le droit du travail n'échappe pas à ce rayonnement puisque le contrat de travail a toujours été soumis en vertu de l'article L.121-1 du Code du travail aux règles de droit commun et donc à l'alinéa 3 de l'article 1134 du Code civil. Cependant, la loi de modernisation sociale du 17 janvier 2002 a consacré l'exigence de loyauté en insérant l'article L.120-4 en vertu duquel « le contrat de travail est exécuté de bonne foi ». La chambre sociale a en effet trouvé dans cette exigence de comportement un moyen de faire primer la relation contractuelle sur le pouvoir. On permet au salarié par cette démarche d'être informé de sa situation, c'est-à-dire de prendre la mesure de l'exercice du pouvoir de contrôle de l'employeur, et surtout d'avoir l'opportunité de défendre ses droits et libertés et d'exercer son propre contrôle.
Cependant de nombreuses entreprises imaginent qu'une information préalable des salariés suffirait à se prémunir de tout problème et à autoriser l'emploi de tous les modes de surveillance et de contrôle. Dans le souci de se garantir contre tout aléa, elles peuvent quelque fois être tentées de déclarer à la CNIL leur schéma de sécurité d'ensemble. Une telle manière de procéder n'est pas suffisante dès lors que les finalités seraient mal définies ou mal comprises. Elle peut nourrir, à tort, le sentiment des utilisateurs qu'ils se trouveraient sous un contrôle constant de l'organisation alors que les mesures prises, dans bien des cas, se bornent à assurer la sécurité du système ou celles des applications et non pas un contrôle individuel ou nominatif de leur activité. Elle peut conforter l'entreprise ou l'administration dans l'idée qu'une déclaration à la CNIL de l'ensemble de son système de sécurité l'autoriserait à porter des atteintes à ce que commande le respect de l'intimité de la vie privée et de la liberté personnelle résiduelle du salarié sur son lieu de travail, alors qu'il appartient, en dernière instance, aux juridictions administratives ou judiciaires d'en apprécier la régularité et, compte tenu des circonstances de fait ou de droit de l'espèce, la proportionnalité.
La surveillance des salariés par l'employeur est soumise au contrôle de la CNIL. En effet, le chef d'entreprise, pour contrôler ses installations informatiques et indirectement ou directement l'exécution du travail, doit mettre en place un traitement automatisé (art.5 de la loi du 6 janvier 1978). Est visé « tout ensemble d'opérations réalisées par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives, ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou base de données… » . Ainsi tout système visant la récolte et l'exploitation de données individuelles du salarié doit donner lieu à une déclaration préalable à la CNIL selon les dispositions des articles 15, 16 et 17. Cette déclaration nécessite la fourniture d'un nombre important d'informations sur le

système mis en place : sa finalité, les personnes concernées, la nature et le temps de conservation des données collectées, les personnes ayant accès au système, les mesures de sécurité prises,…(article 19).[/color][/color]

Bon voila c'est pas de la grande litterature mais bon...[/color][/color][/color][/color]