6.3 : La responsabilité de l’administrateur réseau

Intro : Tout dirigeant d’entreprise ont des intérêts antinomiques mais légitime à gérer au sein de sa structure, en effet l’employeur souhaite protéger les intérêts de son entreprise en protégeant la fuite des informations stratégiques en prévenant l’apparition de virus ou encore en empêchant la circulation des contenus illicite au sein de son réseau. Cela passe donc par la sécurisation de son réseau. A l’inverse nombre de salarié revendique le droit à une vie privée sur le lieu de travail qui se matérialise notamment à travers un connexion internet à des fins personnel. Afin d’encadrer et de limiter un usage excessif d’internet sur le lieu de travail l’employeur dispose au titre de son pouvoir de direction d’un droit de contrôle sur son salarié (arrêt de la chambre social du 14/03/2000, arrêt Dujardin contre la société Instin). Mais ce pouvoir ne doit pas pour autant méconnaitre le respect à la vie privée ainsi que le secret des correspondances. La CNIL a dans plusieurs rapports reconnu un droit à la vie privée pour le salarié tout en soulignant qu’il était irréaliste d’interdire toute utilisation d’intérêt à des fins personnelles.

L’administrateur réseau est au carrefour de ces 2 logiques, en effet il a la fois en charge d’assurer la sécurité du réseau à la demande d’une autorité hiérarchique, il est également en charge de la sécurité des données, aussi bien que professionnelle que personnel des salariés.

1. Le rôle de l’administrateur réseau
2. Les missions de l’administrateur réseau

L’administrateur doit veiller à l’utilisation optimal du réseau et assurer la sécurité des données en entreprise. Il est en charge de la mise en place du système d’information, et il doit prévenir au mieux tout intrusion au sein de système d’information. Les directives communautaires comme la loi informatique et libertés confère une obligation d’assurer la sécurité des traitement informatique, l’article 29 de loi info et libertés dispose qu’il est engagé vis à vis des personnes concerné à « prendre toute précaution utile afin de préserver la sécurité des informations et notamment d’empêcher qu’elle ne soit déformée, endommagée, ou communique à des tiers non autorisés. La loi semble donc un obligation de moyen(une obligation qui oblige à un personne de tout mettre œuvre pour arriver au résultat escompté, on va le juger sur les moyens qui lui ont permis de tout mettre en œuvre) à l’administrateur réseau, cependant la directive communautaire 95/46/CE dans son article 17 semble poser une obligation de moyen renforcé, en effet cette article 17 dispose « que le responsable de la sécurité doit mettre en œuvre les mesures techniques et d’organisation approprié pour protégé les donnés à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l’altération, la diffusions ou l’accès non-autorisé notamment lorsque le traitement comporte des transmission de données dans un réseau ainsi que contre tout autre de traitement illicite. La directive du 12/08/2002 ne solutionne cette question de l’obligation puisse qu’elle invite l’administrateur réseau à « prendre les mesures appropriées pour assure la sécurité de leur service » et d’autre part « à un devoir d’information des risques encourus pour l’utilisateur ».

1. Le statue de l’administrateur réseau

Afin de garantir aux mieux la sécurité du réseau, l’administrateur doit pouvoir accéder à toutes les données contenues dans les messageries ainsi que les fichiers utilisateurs. Autrement dit la Jurice prudence qu’il puisse accéder à l’intégrité des infos mêmes privés afin de pouvoir réaliser au mieux ses obligations. C’est la cour d’appel dans un arrêt du 17/12/2001, l’arrêt ESPCE qui a énoncé :« qu’il est dans les fonction de l’administrateur réseau d’assurer le fonctionnement normal de ceci ainsi que leur sécurité ce qui entraine entre autres, qu’il est accès aux messageries et à leur contenu, ne serait-ce pour débloquer ou éviter des démarché hostile. En conséquence l’administrateur réseau dispose de pouvoirs étendus afin de permettre un bonne utilisation du réseau il peut donc avoir accès aux infos des utilisateurs, à savoir leurs messageries, leurs connexion internet la durée donc le temps de visite de ses sites internet, il peut également contrôlé les débit identifié la durée des connexion, répertorié les sites les plus fréquent, utilisé ou leur tentative de connexion, il peut également contrôlé les pièces jointes ainsi que leurs volumes. Il peur avoir l’ensemble des informations émise, crée et reçu par le salarié. La CNIL notamment dans son rapport du 05/02/2002 confère un statut particulier à l’administrateur réseau et lui permet d’avoir un accès illimité à l’ensemble des infos relatives aux salariés et que statut particulier n’est pas contraire à la loi informatique et liberté du 06/01/78. Toutefois que ce statu atypique est évidement encadré par la loi et par le secret professionnel.

1. Un contrôle encadré et limité
2. L’obligation de confidentialité

Cette obligation de confidentialité est posé par l’arrêt Nikon du 02/10/2001 relative à la vie privée, aux emails, cette arrêt a reconnu expressivement sa vie privée au salarié , il dispose : « que même au temps et lieur de travail, au respect de l’intimité de sa vie privée ; que celle-ci implique en particulier le secret de ses correspondance, que l’employeur ne peut des lors sans violation de cette liberté fondamentale prendre connaissance des messages personnelles émis par le salarié et reçu par lui grâce à un outil informatique mis à sa disposition pour son travail même et ceci où l’employeur aurait interdit un utilisions non-professionnel de l’ordinateur». Ce respect se fonde à travers l’article 8 de la convention européenne de sauvegarde des droits de l’homme et du citoyen, de l’article 9 du code civil, de l’article 1 de la loi informatique et liberté du 06/01/78, ou encore de l’article 226-15 du code pénal. En vertu de la vie privée l‘admin réseau est donc soumis au secret professionnel et qu’il ne peut divulguée les données personnelles auxquels il a accès. Cette obligation de confidentialité couvre aussi bien la messagerie professionnelle ainsi que les fichiers personnels qui relève de la vie privée.

Si la jurice prudence reconnait la possibilité à l’administrateur réseau de lire les messages, il est en revanche pas autorisé à les divulguer à son supérieur hiérarchique. Se pose donc pour admin réseau de savoir comment réagir lorsqu’une situation porte préjudice à l’entreprise. L’arrêt Nikon ou encore l’arrêt ESPCI ne précise à aucun moment comment prendre les dispositions de sécurité qui s’impose lorsque l’administrateur réseau découvre une situation préjudiciable pour l’entreprise. La mission de l’admin réseau est donc très délicate car il devra mettre fin au comportement frauduleux sans pour autant en informer son supérieur hiérarchique qui pourtant tout autorité de décision. A ce titre la cour d’appel a déjà sanctionné un admin réseau pour avoir informé ces supérieurs sur le contenu des messages auxquels il avait accès. Cette arrêt précise que la divulgation d’un message ne se rattache pas aux objectifs de sécurité de l’admin réseau et doit être sanctionner sur le fondement de l’article 432-9 du code pénal. Cependant la cour d’appel d’Aix en Provence du 17/12/2002 est venu tempérer ce principe de non-divulgation.

1. Le contrôle doit être loyale, transparent et proportionné

La loi pose 3 condition dans le cas d’un contrôle d’un admin réseau :

1. Un Contrôle transparent

La démarche de contrôle d’un admin réseau doit se faire dans une logique de transparence vis-à-vis des salariés, en effet les salariés doivent avoir étaient informés de l’employeur de la mise en place d’un dispositif de contrôle soit à travers leur contrat de travail soit à travers une charte informatique (article l121/8/1 du code du travail qui prévoit qu’aucune info peut être collecté à l’insu du salarié). Les comités d’entreprise ou les délègues du personnel doivent être informés de ce contrôle. Lorsque que ce contrôle est automatisé il doit faire l’objet d’une déclaration à la CNIL (la CNIL préconise de plutôt faire des statistiques des sites référencés plutôt que des contrôles nominatifs individualisé)

1. Un contrôle loyal

Le contrôle de l’admin réseau doit se faire de manière impartial et sincère, autrement dit l’admin réseau doit agir dans le cadre de ses fonctions et son action ne peut pas découlés d’une initiative personnelle ou encore d’un ordre hiérarchique mais d’une nécessité justifiée uniquement par des impératifs de sécurité.

1. Un contrôle proportionné

Le contrôle de l’admin réseau doit être proportionné au but recherché. Il appartient à l’admin réseau d’utilisé uniquement les moyens permettant de remplir la sécurisation de réseau sans pour autant aller au-delà, son action doit donc s’inscrire dans une logique cohérente. (ex : il n’as pas à aller que ce qui lui permet si oui et non la réseau sécurisé, si par le contrôle de volumétrie il peut savoir si le réseau est sécurisé il n’a pas aller plus loin)

1. La mise en place d’une charte informatique

La mise en place d’une charte info a un intérêt fondamental dans l’entreprise car elle permet d’informer le salarié des contrôles qu’ils peuvent avoir lieu et des usages ou non pratiqué dans l’entreprise, généralement ces chartes sont annexé au règlement intérieur, et il est demandé au salarié de d’accepter contractuellement cette charte soit par le biais de ce contrat de travail, soit par un avenant contractuel. Pour autant cette charte informatique ne règle pas les questions de rôle de l’admin réseau et à juste titre cette charte devra être aux comités d’entreprise s’il existe ou comité d’hygiène et de sécurité, et elle devra être communiqué à l’inspecteur de travail