Utilisation de l'outil informatique au travail : sécurité, contrôle et sanctions

Quelques généralités

Tout salarié à qui on met à sa disposition un ordinateur et une connexion internet peut utiliser cette dernière à des fins professionnelles. Mais même dans ce cas, il doit en faire une utilisation responsable qui ne mette pas en péril l'outil informatique. Plus discutée est la question de l'utilisation d'une connexion internet à des fins privées. Le premier principe veut que le salarié ait droit au respect de sa privée même sur son lieu de travail. Un arrêt de la CEDH nous rappelle que «Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et de développer des relations avec ses semblables de sorte qu'il n'y a aucune raison de principe de considérer cette manière de comprendre la notion de vie privée comme excluant les activités professionnelles» *(Cour EDH, Niemietz contre Allemagne, 23 novembre 1992).*

Le deuxième principe de taille qui vient limiter le premier est l'intérêt de l'entreprise. Il ne faut pas que l'utilisation d'internet à des fins privées mette en péril les intérêts de l'entreprise. Tout est ici une question de mesure et d'appréciation sur la fréquence et la durée d'utilisation personnelle de la connexion. Le privé ne doit pas prendre le pas sur le professionnel en aucune circonstance. Le salarié est ainsi autorisé à utiliser internet à des fins privées dès lors que l'usage qu'il en fait n'est pas exagéré. Cette limitation est guidée par le devoir de loyauté que le salarié doit à son employeur. Mais dans la mesure où il s'agit d'une question d'appréciation, l'employeur sera toujours bienvenu d'établir une charte ou un règlement interne sur l'utilisation d'internet au travail afin de mieux préciser son utilisation. Ainsi aucune partie ne sera prise par surprise en cas d'abus.

Compte tenu de ce qui vient d'être dit, il est difficilement acceptable qu'un employeur interdise toute utilisation de l'outil informatique à des fins privées. Notons enfin que bien souvent l'employeur interdit déjà l'accès à certains sites ou limite les échanges de fichiers à un certain volume, ce qui est parfaitement conforme au droit.

Etendue du contrôle exercé par l'employeur et sanctions

S'agissant du contrôle exercé par l'employeur, il ne faut pas perdre de vue que le matériel mis à disposition lui appartient et que par conséquent ce dernier peut contrôler sans limitation les données de contenu professionnel (en prenant garde de ne pas violer le principe de correspondance privée qui peut être sanctionné pénalement).

S'agissant plus globalement de l'utilisation d'internet comme outil de connexion à des sites, Il est prohibé de mettre sous surveillance constante un employé sur l'utilisation qu'il fait d'internet sauf si l'on a pu déceler chez lui une activité particulièrement intense et particulièrement grave pour les intérêts de l'entreprise. A défaut de soupçons bien définis sur la personne d'un salarié et d'un usage prohibé qu'il ferait de la connexion internet, l'employeur n'a pas le droit de procéder à un contrôle nominatif. Il peut par contre contrôler collectivement les connexions en amont afin justement de prévenir tout usage abusif et/ou prohibé.

Les sanctions qui découleraient d'un usage prohibé et/ou abusif d'une connexion internet est une affaire d'appréciation. Comme il a été précisé, l'employeur a un intérêt évident à mettre en place une charte ou un règlement intérieur sur l'usage d'internet sur le lieu de travail. Cela lui permettra de prendre des sanctions adéquates et proportionnées en cas de faute du salarié qui peuvent aller du simple avertissement au licenciement pour faute grave. Néanmoins et compte tenu des développements qui ont été faits, l'employeur est bien conseillé de consulter un professionnel du droit avant de s'engager dans une surveillance nominative d'un salarié et de lui rédiger une lettre de licenciement. Les motifs devront en effet être particulièrement circonstanciés et préciser par exemple l'historique de navigation. Surtout l'employeur devra préciser en quoi l'utilisation d'une connexion internet qui a été faite a été préjudiciable aux intérêts de l'entreprise. L'employeur est conseillé de préciser dans les motifs de licenciement le caractère excessif et/ou prohibé des connexions afin de permettre aux juges, en cas de recours pour licenciement abusif, d'apprécier leur bien-fondé.

S'agissant des e-mails, le salarié est conseillé de bien définir par leur objet les e-mails qu'il envoie et d'encourager son interlocuteur à en faire de même en mentionnant clairement la confidentialité des échanges. Par conséquent, l'employeur peut avoir un droit d'accès aux e-mails personnels dès lors que ces derniers prêtent à confusion sur leur objet personnel ou professionnel.

Le salarié est conseillé de conserver les e-mails privés dans un dossier bien séparé du reste de ses correspondances professionnelles. Cela évitera tout risque de violation de correspondance et par conséquent tout risque d'erreur d'interprétation sur le caractère privé des échanges dans le chef des employeurs. Un salarié ne peut se retrancher derrière le caractère confidentiel d'un e-mail pour violer allègrement le principe de loyauté qu'il doit à son employeur (violation du secret des affaires, préparation d'une activité concurrente à celle de son employeur etc…). C'est en effet à cette occasion de l'utilisation de l'outil informatique que le salarié va commettre le vol de données informatiques. Les moyens pour y parvenir sont nombreux: téléchargements sur clef usb, envoi de données sur un cloud ou sur son adresse personnelle. La réponse à ce genre de pratique doit être adaptée.

C'est pourquoi la jurisprudence luxembourgeoise est à ce propos unanime pour dire que si les intérêts de l'entreprise l'exigent et que certaines conditions sont remplies, il doit être permis à l'employeur de porter atteinte à la vie privée de son salarié. De plus, l'inviolabilité absolue des correspondances risquerait d'inciter des salariés indélicats à y loger des dossiers plus ou moins illégaux (C.S.J. 15.03.2012, n°36395 du rôle). L'une des premières sanctions mise à la disposition de l'employeur en cas d'usage prohibé de l'outil informatique est le licenciement. Il n'est pas rare que ce licenciement soit doublé d'une plainte pénale (surtout en cas de recours pour licenciement abusif). En cas par exemple de détournements de données informatiques, l'employeur peut être amené à porter plainte avec constitution de partie civile pour vol de données sinon pour accès et maintien frauduleux dans un système informatique au sens de l'article 509-1 du Code pénal.

La question de l'infraction de vol suscite cependant bien des controverses. Pour qu'il y ait vol, il faut une soustraction frauduleuse et une chose appartenant à autrui. Mais peut-il y avoir vol s'agissant de données immatérielles ?

Dans un arrêt de 200[1], la Cour précise que «la chose» visée à l'article 461 du Code pénal doit s'entendre comme d'un meuble corporel excluant de par là même tout objet incorporel puisqu'il n'y a pas d'appréhension directe de la chose. Dans le cas cependant où le support physique de données électroniques, par exemple l'ordinateur a été soustrait, il s'agit d'un vol, même si le support n'a été emprunté que momentanément pour copier ensuite les données sur un autre support.

Plus loin, elle reprend la définition selon laquelle les données électroniques sont des données immatérielles: informations traitées qui peuvent prendre plusieurs formes telles que des ondes électromagnétiques et les impulsions magnétiques. Dans cette optique, elles ne sont pas considérées comme une chose intellectuelle telle que les droits ou les idées, mais comme une chose qui a, dans le monde réel, une présence matérielle, les données pouvant être enregistrées sous la forme d'impulsions dans des circuits électroniques ou sur des bandes magnétiques,- clé USB par exemple. Ainsi, dans la mesure où les données immatérielles, électroniques ou informatiques, sont susceptibles d'avoir un support, elles peuvent valablement faire l'objet d'une soustraction frauduleuse. La chose semblait entendue alors même que la Cour de cassation avalisait cette analyse[2], les données électroniques enregistrées sur un serveur constituant des biens incorporels pouvant faire l'objet d'une appréhension par voie de téléchargement. Dès lors que les données sont mises sur support en vue de leur soustraction, il y a vol. L'affaire «Medicoleak» a cependant freiné cette analyse. Pour le tribunal, qui va clairement à l'encontre de la tendance jurisprudentielle dégagée ces dernières années et de la position suprême, il ne fait pas de doute que le législateur a entendu la notion de «chose» comme ne visant que les biens matériels[3].

Partant d'une méthode de raisonnement grammatical, le tribunal nous enseigne que pour qu'une chose soit soustraite, cette dernière doit encore «appartenir» à quelqu'un. Or, l'appartenance doit pour le moins être un rapport de droit qui établit «un doit d'exclusivité univoque d'une personne sur cette chose, donc un monopole permettant d 'exclure autrui de la jouissance de cette chose». Ensuite, il faut encore que la chose soit susceptible de soustraction, notion qui suppose un appauvrissement (lat. subtrahere ; sous-tirer, enlever par le bas). Le tribunal précise que même en cas de «soustraction» d'un code d'accès, ce dernier reste à la disposition de son utilisateur autorisé. Retenir le contraire, ce serait entériner la situation incongrue dans laquelle une chose serait volée plusieurs fois à un même propriétaire sans que celui-ci n'en soit dépossédé.

Finalement, le tribunal a choisi de faire prévaloir l'interprétation restrictive de la loi pénale. On ne peut que rejoindre ce raisonnement alors que l'infraction de recel mentionne expressément «les biens incorporels» et que la loi du 18 juillet 2014 sur la cybercriminalité n'a étendu le champ d'application de l'infraction de vol qu'aux seules clefs électroniques. A l'heure actuelle, le débat semble ouvert mais de portée plus limitée alors qu'il existe un arsenal législatif propre aux infractions cybercriminelles prévoyant des sanctions autrement plus sévères, tel que l'accès et le maintien frauduleux dans un système informatique au sens de l'article 509-1 du Code pénal.

In fine, précisons aussi que tous les vols de données informatiques ne sont pas des infractions alors que la jurisprudence reconnait qu'un salarié qui vole dans l'esprit de se constituer des pièces utiles à sa défense en justice ne commet pas de délit. Les droits de la défense sont un principe autrement plus important que les intérêts de l'entreprise.

David GIABBANI
Etude David Giabbani
www.etudegiabbani.lu

1) CSJ corr 29 janvier 2008, n°57/08 V
2) C.Cass. 3 avril 2014, n°3304 du registre
3) Trib. Arr, 16/10/2014, 2628/2014, jugement rendu sous l'empire de l'ancien article 461 du Code pénal

Le Luxembourg lance un projet de supercalculateur

Le Commissaire Européen Günther H. Oettinger et le Vice-Premier Ministre luxembourgeois, et Ministre de l'Economie, Etienne Schneider viennent de cosigner un article sur le blog de la Commission Européenne. Ils y donnent les grandes lignes de la suite du projet ICPEI ("Important Project of Common European Interest") sur la mise en place en Europe d'un supercalculateur (HPC) et d'applications "Big Data" compatibles.

L'Europe ne compte à ce jour qu'un seul supercalculateur classé dans le top 10 mondial dominé par la Chine, et où les USA comptent 5 installations. "Nous devons unir nos forces en groupant des financements régionaux, nationaux et européens pour couvrir l'investissement nécessaire pour développer cette technologie HPC", soulignent les deux auteurs.

Comme annoncé à Luxembourg par le Commissaire Oettinger lors de la récente conférence "European Data Forum" (EDF 2014), le Gouvernement luxembourgeois a déjà lancé avec la France, l'Italie et l'Espagne un projet ICPEI sur la mise en place d'un nouveau supercalculateur.

Début 2016, la Commission Européenne va à son tour lancer une initiative majeure pour le déploiement en Europe d'une infrastructure informatique de classe mondiale : the European Cloud Initiative. Dans le cadre de celle-ci, Le Luxembourg, la France, l'Italie et l'Espagne, en étroite collaboration avec les autres états membres, vont fournir en septembre 2016 au Conseil Européen et à la Commission Européenne une feuille de route pour l'implémentation du supercalculateur (HPC) et de ses applications "Big Data" compatibles.

Les acteurs luxembourgeois qui coordonnent ce projet HPC d'envergure, soit le Ministère de l'Economie, Luxinnovation et le LIST, ont donc jusqu'à septembre pour rendre leur copie.

Pour lire l'article complet sur le blog de la Commission, rendez-vous sur: https://ec.europa.eu/commission/2014-2019/oettinger/blog/luxembourg-launches-supercomputing-project_en

Numen Europe et Labgroup combinent leurs savoir-faire

Optimiser la gestion, la protection et la conservation des documents, tant physiques qu'électroniques, dans une optique "Paperless Office", telle est la préoccupation des responsables d'entreprise à la recherche d'agilité et d'efficience.

Numen Europe, expert en traitement externalisé de données et documents sensibles, et Labgroup, tiers-archiveur de métier depuis 38 ans, deux acteurs majeurs au Luxembourg, s'associent pour leur apporter une solution clé en main, sous la forme d'une offre logiciels + services à la demande.

Il est en effet insuffisant de proposer la prise en charge de certaines opérations ponctuelles, comme la numérisation des documents papier ou l'archivage à long terme, quand les entreprises expriment un besoin d'externalisation complète de processus de traitement d'information, afin de concentrer leurs ressources sur leur cœur de métier.

C'est donc toute la "Supply Chain" de l'information qui est couverte par l'offre DaaS (Document as a Service): depuis la collecte physique ou la capture automatique, jusqu'à la destruction certifiée, en passant par la classification, la dématérialisation, l'indexation, l'extraction de données, l'analyse de données (Data Analytics), la gestion électronique des flux (Enterprise Content Management, Workflow Management, and Collaboration Tools), l'archivage physique ou électronique (Records Management), la sauvegarde, l'éditique (Desktop Publishing), la composition et le routage. L'offre DaaS est commercialisée par Numen Europe et Labgroup, qui restent indépendantes l'une de l'autre, en service bureau (SaaS Mode), en mode licence ou en mode intégration de services.

Un partenariat comme une évidence

"Nous allier était juste évident" affirme David Gray, Deputy General Manager Numen Europe. "Nos sociétés ont l'ambition de couvrir tout le cycle de vie des documents, chacune en s'appuyant sur ses points forts. Chacune est certifiée ISO 9001 et ISO 27001, a le statut de PSF de support, et a investi lourdement pour devenir prochainement Prestataire de Services de Dématérialisation ET de Conservation (PSDC-DC). Bernard Moreau, CEO de Labgroup confirme la logique: "Nous exploitons aussi les mêmes technologies, par exemple la solution de gestion documentaire Easyfolder éditée par Numen. Ensemble, nous proposons à nos clients le meilleur de nos entreprises, en ajoutant un avantage compétitif exclusif: la continuité d'activité garantie par la redondance de nos infrastructures et de nos équipes. Un point clé pour satisfaire les fortes exigences du marché et du statut PSDC! Labgroup et Numen Europe apportent plus ensemble à leurs clients que séparément."

Partenaire de long terme et acteur de poids à l'échelle européenne

Et Bernard Moreau de poursuivre la démonstration des avantages de l'alliance: "Dans notre métier de tiers-archiveur, le client vérifie avant tout la pérennité du service, car il sait nous confier la conservation intègre d'informations sensibles pour des dizaines d'années. Depuis près de 40 ans d'activité, Labgroup a franchi des paliers dans son développement. L'alliance commerciale avec Numen Europe élargit les perspectives de croissance de Labgroup, et conforte donc sa pérennité…"

David Gray conclut en disant: "La combinaison des compétences de nos deux sociétés va s'avérer fructueuse localement, mais également au-delà des frontières. Ensemble, Numen Europe et Labgroup ont la capacité de remporter des marchés d'envergure au niveau européen et pour de grands groupes internationaux. Nous comptons ainsi contribuer largement à l'ambition du Luxembourg de devenir le coffre-fort électronique de l'Europe."