Les synthèses du CLUSIF

Divulgation 2.0 : la divulgation compulsive d'informations par l'internaute, quelles solutions pour l'entreprise ?

Synthèse de la conférence thématique du CLUSIF du 20 octobre 2011 à Paris

Le web 2.0 ne pose pas de problèmes électroniques mais un problème de société. Il génère des modifications de comportement, principalement l'addiction et la compulsivité. Ces deux phénomènes amènent les utilisateurs à diffuser des informations confidentielles.

Pierre-Luc Refalo, Hapsis

Pierre-Luc Refalo dresse le schéma d'une société où les sphères privées, publiques et professionnelles sont de plus en plus imbriquées. La mode du travail à la maison (télétravail) laisse la place à l'intrusion de la maison au travail. Le BYOD (Bring Your Own Device), qui consiste à utiliser son propre équipement nomade au bureau (smartphone, ordinateur) est une tendance qui se développe. Les outils de réseaux sociaux comme Twitter ou Facebook sont eux aussi utilisés au travail.

Un autre constat est la cohabitation de plusieurs générations pour qui internet, la confidentialité ou l'information au sens large, n'ont pas la même signification.

Le contexte de la divulgation compulsive :

- Pourquoi ? pour avoir le sentiment d'exister, l'individu doit communiquer quelque chose chaque jour, sur son blog par exemple. Il doit aussi faire connaître, avant tout le monde, les informations dont il pourrait disposer. Ce besoin d'utiliser les outils de communication est une sorte d'emprisonnement pour certains.

- De quoi et sur quoi ? Bien souvent, la réponse est « sur tout et n'importe qui ». Cette question effleure la morale : ce qu'il est bien de dire ou ne pas dire. Le support texte est de plus en plus souvent enrichi ou remplacé par des images et du son. Pour lutter contre l'enregistrement opportuniste, certaines sociétés interdisent même les téléphones dans les salles de réunion.

- Comment ? le web permet de diffuser une information à tout le monde, à tout instant et en tout lieu.

Les quatre exemples qui suivent se distinguent des dossiers habituellement traités par les responsables sécurité : ce ne sont pas des intrusions, des piratages ou des actes de malveillance destinés à être conservés pour en tirer un avantage. Ces informations sont divulguées volontairement au plus grand nombre grâce à la caisse de résonance que constitue internet.

1) Wikileaks : ce site qui milite pour un journalisme libre de tout censure, a divulgué des rapports confidentiels de l'armée américaine sur l'Afghanistan.

2) Les photos privées de stars piratées dans leur boîte à lettres et diffusées sur des forums ou des blogs.

3) Une photo du dernier prototype de téléphone prise pendant la réunion d'une société de télécom et diffusée le soir même sur internet.

4) « Ma plus belle attaque » : un américain qui préparait un système d'attaque informatique sur un hôpital de Dallas a commencé à filmer ses préparatifs. Il a été arrêté avant de commettre son forfait.

Dans ces exemples, l'objectif principal de l'individu est de faire savoir qu'il a l'information et de la partager en avant première. Le dernier exemple est à la frontière entre l'acte de malveillance et la volonté de diffuser l'information au plus grand nombre de personnes.

Ces quatre autres exemples illustrent la volonté de faire « une bonne action » et de se rendre célèbre de cette manière.

1) Un individu prend la photo des sujets du bac, la donne à un ami et le sujet se retrouve sur internet.

2) Un informaticien de la banque HSBC en Suisse fournit à la France une liste de fraudeurs fiscaux. La diffusion est plus restreinte que celle du sujet de bac mais elle est très médiatisée.

3) Un Norvégien diffuse depuis plusieurs années un manifeste sur internet dans lequel il exprime sa haine des immigrés. Il explique comment préparer une attaque meurtrière avant de passer à l'acte lui-même.

4) Le candidat d'un jeu télévisé diffusé en différé révèle le nom des finalistes sur internet avant la diffusion.

Les conséquences de ces divulgations sont :

- une gloire médiatique, éphémère,
- une traduction en justice,
- des débats sociétaux sur les questions de secret et de confidentialité,
- des impacts économiques (obligation de refaire passer un examen par exemple).

Bloquer, freiner, restreindre ou empêcher la divulgation compulsive sont des tentatives vouées à l'échec. Il demeure essentiel en revanche de réglementer, éduquer et définir une éthique sur la gestion de l'information. Le contrôle et la surveillance sont, quant à eux, obligatoires. L'organisme (y compris les parents) a le devoir de contrôler l'usage des media sociaux. Mais ces restrictions restent insuffisantes et ne sont pas satisfaisantes en démocratie.

L'anticipation pourrait se faire par l'analyse des zones de risque et des personnels à risque. La question reste « comment ? ».

Diane Baudry, Harmonie Technologie

Diane Baudry explique l'approche comportementale de la divulgation compulsive 2.0, dans le but d'identifier les dispositifs permettant d'anticiper et de gérer les risques associés.

Introduction et points d'attention :

- Une démarche compulsive n'est pas de facto synonyme d'addiction ou de pathologie. Lorsque les participants d'une réunion consultent leur Smartphone toutes les minutes, l'on parle de besoin compulsif, non de pathologie.

- La divulgation 2.0 ne signifie pas diffamation ou acte de malveillance. Il s'agit plutôt dans notre contexte d'une diffusion d'informations liées aux activités de l'entreprise sur des medias sociaux, informations qui auraient dû rester dans la sphère professionnelle.

I. La divulgation compulsive en entreprise : définition et enjeux

Une démarche compulsive est une force intérieure qui pousse l'individu à agir même s'il sait que cette action est interdite, ou qu'il s'est lui-même interdit de réaliser. Il ne peut maîtriser cette force qui lui est irrésistible. L'appel de l'émotion prend le pas sur le fondement de la raison. Car aux sources de la compulsion, on retrouve l'angoisse ou l'anxiété. C'est cette angoisse qui devient alors insupportable, et céder à la divulgation devient source de soulagement et de réconfort. Cette compulsion prend forme à travers une démarche de compensation : l'individu cherche à compenser un manque ou un besoin sous-jacent non satisfait.

Exemple : Le « Fear of missing out » ou FOMO, représente la peur de manquer quelque chose ou de passer à côté de quelque chose. Certaines personnes se sentent socialement isolées, voire perdues, si elles n'ont pas leur Smartphone ou ne sont pas connectées sur leurs médias sociaux, 24h/24, 7j/7 et 365 jours/an.

Ces besoins de compensation peuvent engendrer des comportements à risque au sein de l'entreprise. Aujourd'hui, 94 % des entreprises font part d'incidents liés aux réseaux sociaux. Comment l'expliquer ?

La divulgation 2.0 est :

- **rapide** : l'information diffusée sur un media social est à la fois instantanée et globale (à grande échelle). On ne peut pas en circonscrire la fuite, à partir du moment où elle pénètre dans le cyberespace
- **rémanente** : une information diffusée sur le Web reste dans le Web. Elle peut resurgir à n'importe quel moment, et en particulier à l'occasion d'une période critique ou stratégique pour l'entreprise (contexte de conflit social, procès, développement d'activités stratégiques, etc.…).

- **anonyme** : la divulgation 2.0 est réalisée à partir d'un pseudonyme ou d'un avatar : l'origine de la diffusion est difficilement identifiable. De plus, l'anonymat facilite la divulgation compulsive dans la mesure où l'individu se sent protégé derrière son identité numérique.

En effet, l'individu aujourd'hui est un collaborateur, un parent, un ami mais également un être numérique. Au même titre que son identité civique ou physique, il s'est créé une identité numérique propre, au nom de laquelle il publie et partage sur les médias sociaux. Or, son comportement en tant qu'individu numérique peut être différent de son attitude habituelle dans sa vie personnelle ou professionnelle. On peut donc observer dans certains cas **un gap comportemental entre son comportement sur les médias sociaux, et dans le cyberespace en général, et celui qu'il adopte dans les contextes personnel et professionnel**. De surcroît, l'internaute développe son identité numérique et la duplique sous différentes formes pour exploiter plusieurs identités numériques : chacune d'entre elles s'adapte aux opportunités d'interactions et de partage offertes par les médias sociaux, ainsi qu'aux communautés virtuelles avec lesquelles il échange.

Car les médias sociaux ne se limitent pas aux réseaux sociaux comme Facebook. Ils incluent entre autres les sites de publication (plateformes de blog…), de partage (vidéos comme Youtube…), de discussion (plateforme de forums…), de Livecast (web TV où l'auteur se filme 24/24 h), de jeux MMO (massivement multi joueurs), etc. La diversité des médias sociaux offre à chaque individu la possibilité de s'y retrouver et de choisir celui qui lui correspond le mieux. Les options de partage de publications et d'informations, véritables passerelles entre les différents sites, favorisent les interconnexions entre acteur numérique et divulgation. Si elle représente alors un vaste champ des possibles, **la diversité de cet écosystème favorise également l'adoption de comportements à risque**.

Dès lors, comment peut-on expliquer cette diffusion compulsive d'informations professionnelles, liées aux activités de l'entreprise du collaborateur ?
Deux explications principales sont avancées :

- **L'information est banalisée**. **Dans un contexte d'infobésité, nous n'avons plus la capacité d'analyser la masse d'informations que nous recevons quotidiennement**. Cette surabondance nuit à notre vigilance et à notre réflexion sur la sensibilité ou l'importance à accorder à telle ou telle donnée. Par conséquent, **notre capacité à identifier les risques liés à leur diffusion est altérée.** A l'heure du nomadisme, les outils mobiles (Smartphones, tablettes, etc.) permettent non seulement d'accéder à l'information partout et tout le temps, mais surtout de la partager et de la diffuser instantanément dans les mêmes conditions. **Les applications intégrées dans la plupart de ces outils autorisent la rediffusion en « un seul clic »**, créant ainsi une automatisation de nouveaux usages et réflexes qui s'introduisent dans la sphère professionnelle.

- **Les individus se détachent de l'entreprise. L'entreprise est devenue un moyen de développement personnel** comme un autre. Le collaborateur s'épanouit à travers la réalisation d'un projet collectif dont le succès est plus valorisant que le sentiment d'appartenance à l'entreprise. Les principes de loyauté et d'autorité qui étaient l'usage sont aujourd'hui remis en cause, au profit d'une **logique « fratriarcale » dans laquelle chaque collaborateur peut s'exprimer et intervenir en tant qu'expert.** De ce fait, la circulation verticale de l'information, respectant l'ancienne logique pyramidale, laisse la place à une diffusion plus horizontale au sein d'une équipe, dans le cadre d'un projet : le besoin d'en connaître prend le pas sur le droit d'en connaître

La banalisation de l'information et le détachement vis-à-vis de l'entreprise constituent des sources d'explication quant à la diffusion d'informations professionnelles sur les médias sociaux. C'est ainsi que 14 % des entreprises mondiales ont signalé des menaces de poursuites judiciaires résultant de divulgations par le personnel d'informations confidentielles.

Deux autres paramètres sont à prendre en compte :

- **La vie personnelle s'immisce dans l'entreprise.** Tout comme la vie professionnelle s'est introduite dans la sphère personnelle (démocratisation des ordinateurs portables et PDA, télétravail, Smartphones, etc.), nous assistons aujourd'hui à la logique inverse. **Le collaborateur qui partage des informations personnelles sur son blog étendra le périmètre de diffusion à ses activités professionnelles.** Certains d'entre eux sont de véritables « stars » sur les médias sociaux : reconnus à travers leur pseudonyme ou avatar au sein de leur communauté virtuelle, **leur reconnaissance numérique est synonyme de divulgation**

d'informations importantes, stratégiques et de valeur.

- **L'entreprise peut devenir un sujet de diffusion**. Les médias sociaux accueillent la parole qui n'est pas entendue ou reçue au sein de l'organisation. **Diffuser des commentaires sur ses activités, publier des informations liées à l'entreprise permettent à la fois de compenser un besoin de reconnaissance professionnelle, un besoin de s'exprimer sur l'entreprise et parfois de réparer des injustices ressenties comme telles par le collaborateur**. C'est le cas du « journalisme citoyen » : le collaborateur donne l'alerte sur un événement lié à la vie de l'entreprise, qu'il considère comme injuste ou immoral. Par exemple, un salarié d'un grand groupe industriel destinataire d'une note interne annonçant l'externalisation de la production, publie cette information sur un forum : pour lui, le chiffre d'affaires du groupe ne justifie pas cette décision. Il considère alors qu'il est de son devoir de signaler cette injustice au plus grand nombre dans l'espoir de la réparer.

II. Pistes de réflexion face aux risques de divulgation 2.0

- **Redonner de la valeur à l'information.** Il s'agit de remettre de la réflexion là où l'émotion engage une démarche compulsive. Il s'agit de **valoriser l'information, en élaborant une Politique d'usage des Médias sociaux spécifique à l'entreprise**. Elle présente les enjeux et les objectifs, explique les rôles et les responsabilités des collaborateurs et de l'entreprise, tout en indiquant un certain nombre de principes de sécurité propres à l'utilisation de ce type de média au sein de l'organisation. Ces principes de sécurité peuvent ainsi se décliner dans un guide de bonnes pratiques spécifiques. **Sensibiliser les utilisateurs** sur les risques et les responsabilités liés à l'usage des médias sociaux au sein de l'entreprise est nécessaire, en rappelant les bons réflexes à adopter. Cette action permettra également de responsabiliser le collaborateur dans son usage personnel des sites web 2.0, et de différencier information privée et information professionnelle. **Les professionnels des Ressources Humaines doivent être impliqués** à partir du moment où la problématique de divulgation compulsive d'informations sur les médias sociaux relève d'une gestion du risque humain dans l'entreprise : **en intégrant la protection de l'information dans leurs processus opérationnels**. Il s'agit par exemple d'évaluer le niveau de sensibilité du collaborateur à cette problématique lors de l'entretien d'embauche ou au cours des entretiens annuels. Ce suivi s'inscrit tout au long de la gestion de carrière, en prenant en compte le changement de poste, les promotions et les nouvelles responsabilités dues à la gestion d'informations de plus en plus sensibles. A travers la prise en compte de la protection de l'information comme un objectif à part entière, ou dans la fiche de poste / mission, les RH participent à faire du collaborateur un acteur responsable en termes de protection de l'information.

- **Comprendre la divulgation 2.0 dans l'entreprise.** Il s'agit d'abord d'**identifier et d'anticiper les comportements à risque (*a priori*)** par la mise en place d'une cellule de gestion des risques humains au sein de l'entreprise (rattachée à la Direction Générale), ou par l'intégration de cette problématique au sein d'une cellule des risques psychosociaux (rattachée à la DRH). Ce dispositif permet d'anticiper les comportements à risque, notamment lors d'événements anxiogènes que peut rencontrer l'entreprise. Ensuite, il est possible de **mettre en place des outils de monitoring et de surveillance (*a posteriori*)** : l'entreprise est alertée dès la diffusion d'informations professionnelles sur un média social, et a ainsi les moyens de réagir en conséquence (suppression de références sur le Web, communication positive, etc.)

- **Réduire les opportunités de diffusion de l'information**. L'objectif est de multiplier les étapes entre la volonté de diffuser une information et la possibilité de le réaliser. Ajouter des barrières rend la démarche de divulgation moins aisée, moins intuitive et spontanée : l'impossibilité de diffuser « en un seul clic » casse le caractère compulsif de la démarche initiale du collaborateur. **Le déploiement d'une politique de classification outillée** participe à cette stratégie, en sollicitant le collaborateur dès qu'il souhaite diffuser un document, une information par mail, sur Internet, etc. via des étapes intermédiaires de validation ou de confirmation.

64 % des entreprises françaises bloquent l'accès aux réseaux sociaux : cette solution radicale n'est pas forcément pertinente pour toutes les entreprises. Il existe aujourd'hui des **solutions techniques qui donnent la possibilité aux entreprises d'affiner**

leur stratégie de sécurité en fonction de leur besoins et de leurs activités. Parmi ces solutions, citons les règles de filtrage URL : on peut par exemple autoriser l'accès à Facebook, mais interdire l'utilisation du module « chat ». Autre action possible, les règles de contenus : l'accès à Twitter est autorisé avec la publication de tweets ; toutefois, ceux d'entre eux contenant un mot ou une expression faisant référence à tel ou tel projet peuvent être bloqués. Ces outils permettent, non plus de mettre en place une solution générique ne prenant pas en compte le contexte de l'entreprise, mais bien d'adapter les principes de sécurité aux besoins des métiers.

Aujourd'hui, trois quarts des entreprises mondiales ont intégré les médias sociaux dans leurs activités. En quoi cette stratégie constitue-t-elle un élément de réponse à la divulgation compulsive ?

- **Intégrer le 2.0 dans la stratégie de l'entreprise** consiste à intégrer les médias sociaux dans sa stratégie business. Elle peut faire le choix soit d'autoriser l'usage des médias sociaux existants, soit de déployer en interne des blogs, des RSE (Réseaux Sociaux d'Entreprise), ou encore des plates-formes wiki, au sein d'une équipe ou dans le cadre d'un projet. L'entreprise met alors à disposition de ses collaborateurs des rituels qui annihilent le besoin de compenser et rendent ainsi obsolète toute démarche compulsive.

Davantage encore, par cette stratégie digitale, l'entreprise a l'opportunité de développer son image de marque sur le Web, à travers les médias sociaux. Cette démarche peut s'organiser autour d'un Community Manager qui a deux fonctions principales :

- un rôle de médiateur : il anime les médias sociaux, veille aux contenus publiés et au respect des bonnes conduites, élargit la communauté, etc.
- un rôle d'interface avec le client sur le Web : il développe la visibilité de l'entreprise, son image de marque, recherche des partenariats ou fait de la prospection (tests d'offres 2.0 par exemple)

L'élaboration de cette stratégie digitale engage l'ensemble des collaborateurs et les responsabilise : ils deviennent des acteurs numériques dans le cadre de leurs activités professionnelles. L'entreprise peut officialiser cette implication via la signature d'un engagement digital, au même titre que la signature du règlement intérieur ou de la charte informatique. Au-delà de cet engagement, elle anticipe l'arrivée des « digital natives » (Générations Y et Z) et leurs méthodes de travail multitâches et fondamentalement numériques.

Conclusion : trouver le juste équilibre

- Le risque zéro de divulgation compulsive n'existe pas, mais c'est une réalité qu'il est nécessaire d'intégrer dans l'analyse de risque globale de l'entreprise.

- Car le challenge réside bien dans la recherche du juste équilibre entre rendre la diffusion « en un clic » moins facile, via des solutions organisationnelles et techniques, et construire l'entreprise 3.0 en intégrant dès aujourd'hui les médias sociaux au sein d'une stratégie digitale.

Diane Mullenex, Avocate, Ichay & Mullenex

Diane Mullenex aborde la divulgation d'informations sous l'angle juridique et expose les possibilités d'agir en justice

Il n'y a pas d'alternative, l'entreprise doit travailler avec les media sociaux. C'est notamment une façon pour elle de gagner de nouveaux clients. Pour exemple, la page Facebook de La Redoute est une des plus importantes avec plus d'un demi-million de *followers*. Les contrôles divers, dont on a parlé dans les autres présentations, se heurtent au principe de liberté d'expression, auquel les Français sont très attachés. Les entreprises doivent à la fois suivre le mouvement vers le « tout digital », le triple A (anywhere, any device, anytime[1]) et mettre en place des moyens qui sont conformes à la protection des données personnelles et à la liberté d'expression du salarié.

<u>L'information confidentielle</u> :

La confidentialité des informations d'une entreprise s'apprécie selon divers critères. Elle peut résulter:

- d'une obligation contractuelle : accord de non divulgation, obligation de loyauté des salariés,
- d'une obligation légale : secret professionnel (des avocats, des médecins, des notaires) mais aussi secret bancaire et traitement de données personnelles,
- du régime de la responsabilité civile : toute divulgation susceptible de causer un préjudice à la personne qui en est l'objet.

[1] N'importe où, par n'importe quel dispositif, à tout moment

Les informations protégées sont :

- les informations confidentielles,
- les informations protégées par le secret professionnel,
- les données personnelles. Divulguer des données personnelles sur un réseau social relève du pénal. La CNIL oblige les responsables des traitements des données personnelles à sécuriser ces données.

I. Fondements de l'obligation de confidentialité

L'obligation de confidentialité et de protection des informations reçues peut avoir :

- **Un fondement pénal tenant** :
  - à l'activité de l'auteur (secret professionnel, traitement de données personnelles, exécution d'un contrat de travail),
  - à l'intention de l'auteur (abus de confiance, dénigrement, recel etc.).
- **Un fondement civil** (violation d'une obligation contractuelle, clause de confidentialité, accord de non-concurrence).

Pour être sanctionnée, l'appropriation d'une information doit être faite par des moyens illicites. C'est toute la problématique posée par Wikileaks, organisation qui diffuse des informations confidentielles mais qui n'est pas nécessairement à l'origine de l'appropriation de ces informations.

La divulgation d'information est parfois autorisée, voire imposée par la loi. Certains professionnels sont obligés de faire des signalements et de les divulguer. L'obligation de signaler une maltraitance par exemple l'emporte sur le secret médical.

La difficile notion du « droit du public à l'information » a donné lieu à de nombreuses jurisprudences. Par exemple, la jurisprudence et la loi disent clairement que les informations divulguées dans les conseils d'administration ou dans les conseils de surveillance sont supposées confidentielles. Il est néanmoins essentiel de réitérer ce caractère confidentiel au début du conseil et de rappeler également que les comités d'entreprise sont sujets à un devoir de réserve et de confidentialité.

L'entreprise peut mettre en œuvre une politique de confidentialité pour déterminer quelles informations sont strictement confidentielles. Dès lors, lorsque l'entreprise encadre l'accès et la divulgation de ses informations, un tiers non autorisé commet une faute s'il cherche à se procurer des informations protégées de façon illégitime.

La notion de proportionnalité en droit impose qu'il y ait adéquation entre un moyen employé et le but qui lui est assigné. Dans le cas de la divulgation d'informations, l'exigence de proportionnalité se fait entre :

- l'atteinte aux droits fondamentaux des salariés (liberté de communication, liberté d'expression des salariés) et,
- la légitimité de la protection d'informations confidentielles (intérêts légitimes de l'entreprise, légitimité du secret des affaires).

Les risques pour les entreprises en cas de divulgation :

- atteinte à la « e-réputation » de l'entreprise (par exemple lorsque le personnel navigant de Virgin Atlantic dénonce la vétusté des appareils),
- atteinte aux droits de propriété intellectuelle de l'entreprise (récentes affaires Renault et Michelin),
- perte de compétitivité,
- risque de favoriser les entreprises concurrentes,
- perte de clientèle,
- échec d'une négociation avec une entreprise partenaire.

Notons que le risque est plus souvent humain que numérique : plus de 700 ordinateurs portables seraient abandonnés chaque semaine dans les aéroports parisiens dont à peine 10 % sont réclamés.

Ne pas confondre :

- **la divulgation d'informations confidentielles :** un commercial, qui sans aucune intention de nuire fait part sur Facebook de chacun de ses déplacements dans telle ou telle ville. Son employeur ne comprend pas pourquoi son concurrent démarche systématiquement les mêmes clients que lui quelques jours après son passage.

- **avec le dénigrement de son employeur** : des salariés de la société Alten échangent des propos critiques envers leur employeur sur Facebook . Ils sont licenciés pour faute grave et cette décision entérine le fait qu'Internet est un espace public. C'est la première fois que des salariés sont condamnés pour avoir tenu des propos diffamants sur leur employeur, depuis leur domicile.

II. Comment l'entreprise peut-elle agir en justice en cas de divulgation d'informations ?

I. Les sanctions pénales :

- L'abus de confiance est l'infraction la plus fréquente. C'est le fait d'être en possession d'une information qui a été remise dans le cadre professionnel et qui est « détournée ». C'est la sanction retenue dans l'affaire Michelin où un salarié avait tenté de vendre des informations confidentielles à une entreprise concurrente.

Jusqu'au 26 septembre dernier la plupart des tribunaux se refusaient à caractériser un vol de données informatiques sans support matériel. Il fallait selon la jurisprudence antérieure démontrer la soustraction d'un bien matériel pour caractériser l'infraction pénale. Pour la première fois un tribunal correctionnel a condamné une salariée pour soustraction frauduleuse de données informatiques confidentielles. Elle avait subtilisé les fichiers de clientèle sur une clé USB pour les revendre.

- La contrefaçon d'œuvres,
- La divulgation de secret de fabrication,
- Le recel,
- Le vol,
- Le délit d'initié,
- L'atteinte au secret des correspondances,
- La violation du secret professionnel,
- La divulgation de données à caractère personnel.

Une proposition de loi de Bernard Carayon déposée le 12 janvier 2011 visant à créer un délit d'atteinte aux informations économiques protégées a été reprise par Eric Besson. Elle pourrait passer avant la fin de l'année.

II. Les sanctions civiles :

Article 1382 du Code civil :
L'auteur d'un acte de divulgation devra payer des dommages-intérêts à la personne victime de cette divulgation si sont prouvés : un préjudice, une faute ou un lien de causalité entre le préjudice et la faute.

Article 1383 : Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence.

Sanctions en cas de violation de l'obligation contractuelle de confidentialité :
- résiliation du contrat
- paiement de dommages-intérêts

III. Les sanctions en droit social

Elles concernent la violation d'engagements contractuels :
- violation par le salarié de son obligation contractuelle de confidentialité,
- manquement du salarié à son obligation contractuelle de loyauté.

Le salarié est tenu à une obligation de loyauté à l'égard de son employeur. De nombreuses jurisprudences sur ce sujet concernent l'utilisation des outils professionnels mis à la disposition du salarié. Dans le cadre de la loi Hadopi (sur la diffusion des œuvres et la protection de droits sur internet) par exemple, c'est l'adresse IP qui est relevée. Il appartient donc à l'entreprise de dénoncer à l'Hadopi l'auteur du téléchargement illégal. Sinon c'est leur responsabilité qui est engagée.

Les sanctions possibles en droit social sont :
- des sanctions pénales (pour vol, abus de confiance, etc.),
- des sanctions disciplinaires,
- le licenciement.

La jurisprudence du 5 mars 2008 (affaire TNS Secodip/Fédération CGT) a entériné le fait que « le droit d'expression d'un syndicat sur son site Internet était limité aux profits des intérêts légitimes de l'entreprise ».

L'administration de la preuve de divulgations :

En droit pénal, l'administration de la preuve est gouvernée par les principes de :
- présomption d'innocence,
- liberté de la preuve : tous les moyens de preuve sont recevables devant le juge (mais sont tout de même encadrés),
- loyauté.

En droit civil :

- Les actes juridiques sont soumis au **système de preuve légale** (acte authentique, acte sous seing privé, aveu ou le serment décisoire). Certains modes de preuve imparfaits sont laissés à la libre appréciation du juge (présomption, témoignage, enregistrements…).
- Les faits juridiques sont soumis **au principe de liberté de la preuve**.

En droit commercial, la preuve est libre.

La vigilance s'impose. Trop d'entreprises commettent des délits pénaux en voulant collecter des preuves.

III. Les mesures utiles aux entreprises afin d'éviter toute divulgation d'information :

Les mesures internes :

- rédiger une charte d'éthique ou un code de conduite des affaires,
- rédiger une charte informatique (seules 50% des entreprises en ont),
- organiser des formations à la communication sur internet,
- sensibiliser le personnel à la confidentialité, aux risques encourus par l'entreprise en cas de divulgation d'informations sensibles et au devoir de loyauté des salariés,
- restreindre l'accès au secret et imposer des mesures de surveillance pour ceux qui y ont accès,
- prévoir dans les contrats de travail des clauses de confidentialité, de non-concurrence et relatives au devoir de réserve.

Les mesures externes :

- signer des contrats comprenant une clause de confidentialité,
- négocier l'étendue de la confidentialité sur l'objet du contrat signé avec un prestataire, négocier aussi le contrat en lui-même, le projet dans son ensemble, sans oublier la durée de confidentialité des informations concernées.

La nouvelle génération ne conçoit pas de vivre sans Internet et les outils de mobilité. Les entreprises devront s'adapter, d'autant plus que les décisions européennes vont dans le sens d'un droit fondamental à l'accès à Internet.

Questions et Réponses avec l'assistance.

Cette conférence comportait également un débat avec la salle, non retranscrit dans ce document mais disponible en vidéo à l'adresse suivante : http://www.clusif.asso.fr/fr/production/videos/#video111020.

Retrouvez les vidéos de cette conférence et les supports des interventions sur le web CLUSIF http://www.clusif.asso.fr/fr/infos/event/#conf111020.