REVUE LAMY

droit des affaires

OCTOBRE 2011

Les pouvoirs du directeur général délégué de SAS
Par Christine LEBEL

Créances non déclarées et droits de la caution
Par Jean-Luc VALLENS

Gestion d'actifs : les principales modifications apportées par l'ordonnance n° 2011-915 du 1er août 2011 et ses décrets d'application
Par Isabelle RIASSETTO

Ventes liées, ventes avec prime, loteries commerciales : le protectionnisme français à l'épreuve du libéralisme communautaire
Par Thierry TITONE et Matthieu DARY

Forfait-jours : sanction du non-respect par l'employeur des stipulations de la convention collective
Par Florence CANUT

ÉTUDES

Le juge du lieu de livraison
Par Christoph Martin RADTKE

La force du secret professionnel face aux perquisitions chez l'avocat
Par Vincent NIORÉ

DOSSIER SPÉCIAL

Le risque pénal de l'entreprise : approche pratique des évolutions actuelles
Par Émilie BAILLY, Pierre-Philippe BOUTRON-MARMION, Julien CHEVAL, Emmanuel DAOUD, Marie DESPLANQUES, Catherine GAMBETTE, César GHRENASSIA, Julie FERRARI et l'équipe d'APCO Worldwide Paris : Nicolas BOUVIER, Elvire KORMANN-ESMEL et Anne KUENTZ-LAFOURCADE

Collection LAMY DROIT DES AFFAIRES

64

Lamy
une marque Wolters Kluwer

LE RISQUE PÉNAL DE L'ENTREPRISE : APPROCHE PRATIQUE DES ÉVOLUTIONS ACTUELLES

INTRODUCTION
Emmanuel DAOUD, Avocat à la Cour, VIGO Cabinet d'avocats

LE CHARME DISCRET DE LA GARDE À VUE : ERREMENTS ET AMBIGUÏTÉS DE LA LOI DU 14 AVRIL 2011
César GHRÉNASSIA, Avocat à la Cour, VIGO Cabinet d'avocats, Ancien secrétaire de la Conférence

INFORMATIONS ET OUTILS PRATIQUES RELATIFS AUX DIFFÉRENTES ÉTAPES DE LA PROCÉDURE PÉNALE
Julie FERRARI, Avocat associé, VIGO Cabinet d'avocats

LA DÉGÉNÉRESCENCE DE L'ARTICLE 121-2 DU CODE PÉNAL
Emmanuel MERCINIER, Avocat associé, VIGO Cabinet d'avocats, Ancien secrétaire de la Conférence

LES DÉLÉGATIONS DE POUVOIRS : PRINCIPES ET ACTUALITÉS
Marie DESPLANQUES, Avocat à la Cour, VIGO Cabinet d'avocats

HARCÈLEMENT MORAL ET JUGE PÉNAL : UN JUGE DE PLUS EN PLUS COURTISÉ
Catherine GAMBETTE, Avocat, VIGO Cabinet d'avocats

LES RISQUES LIÉS À LA CORRUPTION
Pierre-Philippe BOUTRON-MARMION, Avocat à la Cour, VIGO Cabinet d'avocats

L'ENTREPRISE FACE AUX RISQUES INFORMATIQUES : LES RÉPONSES DU DROIT PÉNAL
Émilie BAILLY, Avocat à la Cour, VIGO Cabinet d'avocats

RESPONSABILITÉ PÉNALE DES DIRIGEANTS DE L'ENTREPRISE EN DIFFICULTÉ : UN REGRETTABLE *STATU QUO*
Julien CHEVAL, Avocat Associé, VIGO Cabinet d'avocats

RESPONSABILITÉ PÉNALE EN ENTREPRISE ET DOMMAGE DE RÉPUTATION
Par l'équipe d'APCO Worldwide Paris, Cabinet de conseil en affaires publiques et communication stratégique : Nicolas BOUVIER, Directeur général, Anne-Elvire KORMANN-ESMEL, Directrice Conseil, Anne KUENTZ-LAFOURCADE, Consultante

Par Émilie BAILLY
Avocat à la Cour
VIGO Cabinet d'avocats

L'entreprise face aux risques informatiques : les réponses du droit pénal

La généralisation de l'utilisation de l'outil informatique et de l'Internet a entraîné ces dernières années l'émergence d'une criminalité bien spécifique de nature à inquiéter les pouvoirs publics, mais aussi les entreprises. De plus en plus informatisées, les entreprises sont aussi de plus en plus vulnérables aux attaques numériques. Espionnage industriel, vol de données ou simple campagne de dénigrement sur le net, l'entreprise doit faire face à de nouvelles menaces. Alors que le droit du numérique est toujours en construction, quelles réponses le droit pénal peut-il apporter aux entreprises victimes de cybercriminalité ?

En juin dernier, un rapport de l'OCDE classait la cybercriminalité comme l'une des cinq plus grandes menaces planant sur l'économie mondiale (le rapport intitulé « *Les futurs chocs mondiaux* », publié le 27 juin 2011, analyse cinq risques majeurs potentiels pour les années à venir : une pandémie, une cyber-attaque visant une infrastructure critique, une crise financière, un conflit socio-économique et une tempête géomagnétique).

Le rapport annuel de Symantec (société spécialisée dans la protection des systèmes informatiques qui a présenté la 15e édition de son rapport annuel sur l'analyse de l'activité cybercriminelle) souligne, quant à lui, que les cybercriminels se tournent de plus en plus vers les entreprises pour commettre des agissements répréhensibles.

Ainsi, selon un article de *La Tribune*, les pertes de données liées pour la plupart à des actes de piratage ont coûté en moyenne 2,2 millions d'euros aux entreprises visées par ces attaques en 2010 (La Tribune, La cybercriminalité, un business à 1.000 milliards, 28 juin 2011). Un chiffre en augmentation de 16 % par rapport à 2009. Le risque informatique est donc pris très au sérieux par les entreprises.

La cybercriminalité englobe trois catégories d'activités criminelles. La première comprend les formes « *traditionnelles* » de criminalité (vol, escroquerie, pédopornographie). La deuxième concerne la publication de contenus illicites par voie électronique. La troisième vise les infractions propres aux réseaux électroniques, c'est-à-dire les attaques visant les systèmes informatiques, le déni de service et le piratage.

Les menaces qui pèsent sur les entreprises sont principalement liées aux deux dernières catégories de comportement délictueux. Le législateur, toujours soucieux de protéger les entreprises et leurs intérêts économiques, a vu dans le droit pénal une arme de premier choix pour dissuader et réprimer les cyber-attaques. Le droit pénal est, en effet, une réponse efficace mise à la disposition des entreprises pour faire respecter ce qu'il est désormais convenu d'appeler leur « *e-réputation* » (I) ; c'est également une arme de choix pour faire sanctionner toute atteinte à leur systèmes informatiques (II).

*

I.– LA PROTECTION DE L'E-RÉPUTATION

Pour Jean-Pierre Piotet, Président de l'Observatoire de la Réputation, « *la réputation apporte une indiscutable valeur ajoutée à l'entreprise. La réputation est d'abord un actif patrimonial qui suppose du talent et du temps...* » (<www.obs-reputation.org/ip=2011>).

L'e-réputation est composée des informations que l'on trouvera sur une entreprise dans les moteurs de recherche. C'est-à-dire :

– la qualité et la variété des informations disponibles ;

– le contenu des conversations, blogs, sites et avis disponibles en ligne et notamment sur les réseaux sociaux ;

– la cohérence de l'image, etc...

Si Internet est un outil fantastique pour les entreprises, notamment en terme de marketing, son utilisation peut s'avérer risquée. En effet, sur la toile, l'information circule à toute vitesse et touche un nombre toujours plus important de personnes. Une communication mal contrôlée peut donc s'avérer désastreuse. La récente déconfiture boursière de la Société Générale à la suite d'une rumeur infondée relayée par Internet en atteste ; en quelques heures, ces rumeurs alimentées par les marchés financiers sur Twitter ont fait dégringoler le cours de Bourse de la banque. Et son image. Des Médias sérieux ont même pris le relais, toujours sur Internet : le *Wall Street Journal* s'est fendu d'un article sur son édition en ligne, et le *Guardian*, sur son compte twitter, redoutait même un scénario à la Lehman Brothers...

Comment alors protéger sa réputation sur Internet ?

Dans le cas de la Société Générale, son PDG, Fréderic Oudéa, a fait le tour des médias pour tenter de rassurer clients et actionnaires, plusieurs articles ont été retirés de la toile, etc... Pour les entreprises qui ne bénéficient pas d'un tel droit d'entrée dans les médias, le droit pénal de la presse peut offrir une alternative efficace.

En effet, sous le couvert d'un certain anonymat, une grande liberté de parole s'est développée sur Internet, pouvant aller jusqu'à la publication de propos diffamants ou injurieux qui sont ensuite repris par la blogosphère et, de plus en plus, sur les réseaux sociaux. Cependant, il ne faut pas se tromper, Internet n'est pas une zone de non droit. Il a depuis longtemps été jugé que la diffamation ou l'injure par la voie de l'Internet constitue une publication « *par voie de presse* », et peut, à ce titre, faire l'objet de poursuite sur le fondement de la loi du 29 juillet 1881 sur la liberté de la presse.

L'article 29 de la loi définit la diffamation comme l'allégation ou l'imputation d'un fait précis, portant atteinte à l'honneur et à la considération d'une personne déterminée ou déterminable, et ce publiquement et de mauvaise foi. En revanche, toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait est une injure. Les personnes morales peuvent être victimes d'une diffamation ou d'une injure (Cass. crim., 12 oct. 1976, n° 75-90.239, Bull. crim., n° 287) et l'appréciation de la situation financière d'une entreprise peut porter atteinte à l'honneur et à la considération

de la personne morale visée, dès lors qu'il y a imputation de faits précis. Ainsi, prétendre qu'une société serait menacée dans sa continuité et sur le point de licencier plus de la moitié de son personnel a été jugé diffamatoire (CA Paris, 11e ch., 3 avr. 2008, n° 05/02837). On n'est pas loin de ce qu'il est convenu d'appeler les « *rumeurs* » concernant la Société Générale.
Deux difficultés sont apparues dans l'application de la loi du 29 juillet 1881 sur la liberté de la presse aux délits perpétrés sur Internet : celle liée à la courte prescription et celle liée à l'identification de l'auteur de l'infraction.
En effet, le délai légal pour réagir est extrêmement court. Qu'il s'agisse de faire valoir un droit de réponse (Loi de confiance en l'économie numérique : L. n° 2004-575, 21 juin 2004, art. 6-IV) dont dispose chaque personne nommée dans un contenu mis en ligne, ou qu'il s'agisse d'engager une action en justice pour diffamation ou injure, le délai de prescription est de trois mois. Au-delà, il n'est pas possible de faire juridiquement retirer un contenu publié sur Internet.
Afin de pouvoir réagir rapidement, il est donc recommandé de mettre en place une surveillance automatisée. Des outils gratuits et simples à mettre en œuvre permettent d'automatiser ce travail de surveillance, tels que le service « *Google Alert* » (<www.google.fr/alerts>) qui permet de définir des alertes à partir de mot clés. Ainsi, dès qu'un nouveau contenu publié contient les mots clés définis, un e-mail d'alerte (ou un flux RSS) avec un lien vers la source, est envoyé.

*

Une autre difficulté peut résulter de l'impossibilité d'identifier l'éditeur ou l'auteur des propos illicites publié sur Internet.
En matière de presse et d'édition, sont responsables des faits de diffamation, dans l'ordre le directeur de la publication, le codirecteur ou l'éditeur. Puis, à défaut, les responsables subsidiaires sont l'auteur, l'imprimeur et les diffuseurs (articles 42 et suivants de la loi de 1881).
Pour Internet, le directeur de la publication ou l'éditeur du site Internet sera l'auteur principal du délit de diffamation, puis à défaut, l'auteur du texte. Toutefois, cette responsabilité dite « *en cascade* » s'applique à la condition que le message incriminé ait fait l'objet d'une fixation préalable à sa communication au public... ce qui n'est pas toujours le cas. En effet, s'agissant de propos diffusés « *en direct* » sur des blogs ou des réseaux sociaux, cette condition de fixation préalable ne semble pas formellement remplie et seul l'auteur des propos pourra être poursuivi comme auteur principal.
En outre, la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique n'impose pas les mêmes obligations aux « *éditeurs professionnels* » et aux « *éditeurs non professionnels* » en matière d'identification. En effet, l'article 6-III de la loi du 21 juin 2004 impose aux éditeurs professionnels de mettre à disposition du public des éléments précis permettant de les identifier. En revanche, le même article permet aux éditeurs non professionnels de préserver leur anonymat en se limitant à tenir à la disposition du public les éléments d'identification de l'hébergeur à qui ils doivent, bien entendu, transmettre leurs coordonnées personnelles.
Dans de telles circonstances, l'entreprise victime de propos diffamatoires ou injurieux peut solliciter auprès de l'hébergeur le retrait de propos manifestement illicites. Pour qu'une telle demande soit valide, elle doit comporter les coordonnées du notifiant, la description des faits et leur localisation, les motifs de retrait du contenu avec mention des dispositions légales l'imposant, et soit la copie de la lettre adressée à l'éditeur ou à l'auteur du contenu, soit la justification des raisons pour lesquelles celui-ci n'a pu être contacté (L. n° 2004-575, 21 juin 2004, art. 6).
La loi prévoit que la responsabilité, civile ou pénale, des hébergeurs à raison des contenus illicites publiés sur leur réseau, peut être engagée si, après en avoir eu connaissance (notamment par une notification adressée par la victime), ils n'ont pas alors « *agi promptement pour retirer ces informations ou en rendre l'accès impossible* ».
L'entreprise victime peut également, après avoir notifié à l'hébergeur l'existence de propos manifestement illicites et lui en avoir demandé le retrait, solliciter l'identification de l'éditeur ou de l'auteur du contenu auprès de l'hébergeur, afin d'engager à son encontre des poursuites pénale sur le fondement de la diffamation ou de l'injure. Les données personnelles relatives à l'éditeur ou à l'auteur des propos illicites sont, en principe, couvertes par le secret professionnel de l'hébergeur. En pratique, il faut donc demander au président du tribunal de grande instance, par voie de requête ou en référé, d'enjoindre l'hébergeur d'identifier le responsable du site.
L'hébergeur n'est donc saisi que parallèlement à l'éditeur ou l'auteur des propos illicites.
En tout état de cause, les entreprises victimes de propos diffamatoires ou injurieux publiés sur Internet ne sont pas démunies. Les hébergeurs, soucieux – eux-aussi ! – de leur bonne réputation, répondent en général rapidement aux notifications qui leurs sont faites, en retirant de la toile les contenus manifestement illicites, dès lors que ceux-ci sont démontrés.
Par ailleurs, une fois l'éditeur ou l'auteur de propos diffamatoires identifié (au besoin, grâce à une ordonnance judicaire obtenue sur requête ou en référé), celui-ci ne peut s'exonérer de sa responsabilité qu'en apportant la preuve des imputations alléguées ou en démontrant sa « *bonne foi* » (l'intention coupable de l'auteur des imputations diffamatoires étant toujours présumée – *cf.*, par exemple, Cass. crim., 29 nov. 1994, n° 92-85.281, Bull. crim., n° 382).

Deux difficultés sont apparues dans l'application de la loi du 29 juillet 1881 sur la liberté de la presse aux délits perpétrés sur Internet : celle liée à la courte prescription et celle liée à l'identification de l'auteur de l'infraction.

*

Outre les atteintes à leur e-réputation, les entreprises peuvent également être victimes d'autres infractions liées aux nouvelles technologies. Il s'agit des attaques contre leurs systèmes d'information (ou systèmes de traitement automatisé de données).

II.– LA PROTECTION DES SYSTÈMES INFORMATIQUES

Depuis quelques années, la fraude informatique n'est plus seulement le fait de quelques passionnés pas toujours conscients de la gravité de leurs actes, elle est aussi le fait de groupements criminels organisés.
Les tentatives d'intrusion des systèmes d'information des entreprises ne cessent d'augmenter. Ces attaques sont multiples : tour à tour ultra automatisées et prolifiques, ou lentes et ciblées, organisées en interne, au sein même des entreprises, ou perpétrées à l'échelle des réseaux nationaux de systèmes piratés, >

ou encore au moyen de techniques d'ingénierie sociale,

Les infiltrations sur des réseaux protégés et la compromission de données qui en résulte, constituent un véritable fléau pour les entreprises du monde entier.

En droit interne, le législateur a instauré, depuis plusieurs années, un dispositif répressif destiné à lutter contre cette nouvelle forme de criminalité. En effet, les articles 323-1 et suivants du Code pénal qui traitent de la fraude informatique, ont été introduits par la loi n° 88-19 du 5 janvier 1988 sur la fraude informatique (dite loi *Godfrain*) et ont été modifiés par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Ils ont pour but de réprimer un certain nombre d'infractions en matière informatique.

L'article 323-1 du Code pénal sanctionne la pratique du *hacking*. Il rend les intrusions dans un système de traitement automatisé de données passibles de trois ans d'emprisonnement et de 30 000 euros d'amende. L'alinéa 2 du même article prévoit une aggravation de peine lorsque l'accès frauduleux au système a entraîné la suppression ou la modification des données ou l'altération du fonctionnement du système.

L'accès frauduleux est constitué dès lors qu'une personne non habilitée pénètre dans un système de traitement automatisé de données tout en sachant qu'elle est dépourvue d'autorisation. C'est ainsi qu'un groupe de hackers a été condamné pour s'être introduit sur le site Internet de la Mission interministérielle de lutte contre la drogue et la toxicomanie (MILDT ; CA Paris, 28 janv. 2010, n° 09/00927, D. 2002, p. 940).

L'article 323-2 du Code pénal quant à lui, incrimine le fait de fausser ou d'entraver le fonctionnement du système informatique qui est passible de cinq ans d'emprisonnement et de 75 000 euros d'amende. Peut importe qu'il y ait eu accès – autorisé ou non – au système informatique de la victime, il s'agit ici de réprimer des dégâts causés volontairement aux données et au système, notamment, par exemple, par l'introduction d'un virus. L'envoi massif de courriels non sollicités (ou spamming) est un autre exemple d'entrave au système (CA Paris, 18 déc. 2001, D. 2002, p. 940). En revanche, pour que l'infraction soit constituée, il faut que le fonctionnement du système soit faussé ou entravé, c'est-à-dire qu'il soit affecté de manière préjudiciable.

L'article 323-3 du Code pénal vise la modification frauduleuse de données. Il sanctionne l'introduction, la suppression ou la modification frauduleuse de données de cinq ans d'emprisonnement et de 75 000 euros d'amende. À titre d'exemple, le groupe de hackers qui avait profité d'une faille pour s'introduire sur le site Internet de la MILDT a également été condamné pour modification frauduleuse de données ; ils avaient, en effet, remplacé un texte qui figurait sur le site, par des propos incitant à la consommation de cannabis (CA Paris, 28 janv. 2010, préc.).

En revanche, la simple copie des données ne tombe pas sous le coup de l'article 323-3 du Code pénal. Il faudra donc se reporter à d'autres textes pénaux comme ceux relatifs à la protection des logiciels (C. propr. intell., art. L. 112-2, 13°) ou ceux relatifs aux traitements de données à caractère personnel (C. pén., art. 226-16).

L'article 323-3-1 du Code pénal vise quant à lui les moyens qui permettent ces attaques et punit des mêmes peines l'importation, la détention, l'offre, la cession et la mise à disposition de ces moyens techniques, matériels ou logiciels. Sont ainsi directement visés les créateurs de virus.

La tentative de commission de tous ces délits est punie des mêmes peines (C. pén., art. 323-7).

L'article 323-4 du Code pénal permet de réprimer les associations de malfaiteurs, dès leurs premiers efforts accomplis en vue de l'intrusion.

Enfin, le recel d'informations obtenues à la suite d'une intrusion frauduleuse dans un système de traitement automatisé de données est puni par l'article 321-1 du Code pénal de cinq ans d'emprisonnement et de 375 000 euros d'amende.

L'arsenal répressif en matière de lutte contre la fraude informatique semble ainsi complet. Toutefois, il comporte plusieurs failles, imputables à l'évolution de la taille et du nombre d'infractions (cyberattaques). En effet, la législation française ne concerne qu'un nombre limité d'infractions (les grandes absentes étant la copie d'information, l'interception illégale de données, etc..) et ne permet pas de faire face à la menace potentielle que les attaques à grande échelle représentent pour les sociétés. Elle ne tient pas non plus suffisamment compte de la gravité des infractions et ne prévoit pas de sanctions à leur mesure (rappelons que les attaques à grande échelle contre les systèmes d'information sont passibles de sanctions allant jusqu'à dix années d'emprisonnement au Royaume-Uni : Avis du Comité économique et social européen sur la « Proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil »).

En outre, la répression de telles infractions se heurte au principe de territorialité de la loi pénale. Le développement de cette nouvelle forme de délinquance transnationale que constitue la cybercriminalité impose donc un effort international concerté.

Le Conseil de l'Europe a été la première organisation internationale à avoir élaboré une convention à vocation universelle s'efforçant d'appréhender la problématique des réseaux dans sa dimension pénale globale. Une convention relative à la cybercriminalité a, ainsi, été adoptée à Budapest le 23 novembre 2001 et signée le même jour par la France. Cependant, seuls 31 des 47 États membres du Conseil de l'Europe ont jusqu'à ce jour ratifié la Convention sur la cybercriminalité. La France l'a fait, le 19 mai 2005.

La Convention vise à définir les contours de la cybercriminalité, en fixant, par le biais d'une harmonisation au niveau international des principales incriminations, un droit commun en matière d'infractions.

L'inconvénient majeur de cet instrument est qu'il est rédigé dans « *des formules très souples* » (*cf.* Projet de loi AN n° 905, 20 juin 2003, autorisant l'approbation de la convention sur la cybercriminalité), dans le but de concilier les approches juridiques fondamentalement différentes et les spécificités de chaque ordre juridique national des États membres du Conseil de l'Europe.

Le Conseil de l'Union européenne a également adopté le 24 février 2005 une décision cadre relative aux attaques visant les systèmes d'information, dans le but de rapprocher les législations européennes et de renforcer la coopération internationale dans le domaine de la lutte contre la cybercriminalité.

Une proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre du Conseil est actuellement à l'étude (Proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil). Ce projet de directive vise essentiellement à définir les cybercrimes et établir les peines afférentes, mais aussi à aider les autorités à poursuivre les actes de cybercriminalité qui tentent d'exploiter l'interconnectivité internationale des réseaux, de même que les personnes qui essaient de se cacher derrière l'anonymat susceptible d'être offert par les outils sophistiqués inhérents à ce type de criminalité.

La directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information devrait, lorsqu'elle sera adoptée, faire évoluer le droit interne afin d'apporter une réponse plus efficace au fléau qu'est la cybercriminalité.

*
* *

Le droit interne, comme le droit international et européen, s'adapte régulièrement à l'évolution de la criminalité informatique, elle-même fruit de l'évolution technique. Encore récemment, la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (dite *LOPPSI 2*) a créé un nouveau délit d'utilisation frauduleuse de l'identité ou de données à caractère personnel d'un tiers sur un réseau de communications électroniques, comblant ainsi un vide juridique. Ce nouveau délit s'applique à l'usurpation de l'identité des personnes morales (lors des travaux parlementaires, il a été expressément indiqué que « *dans le silence de la loi les dispositions* (...) *s'appliquent aussi bien aux personnes morales qu'aux personnes physiques* », *séance du 11 février 2010*), qui sont très souvent victimes de ce type de comportement délictueux.

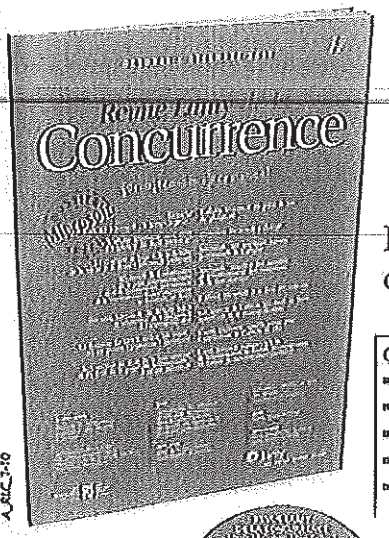
En outre, pour améliorer l'efficacité des poursuites engagées par les autorités contre les actes de cybercriminalité, de nouveau moyens sont régulièrement mis en œuvre. La LOPPSI 2 représente, à ce titre, une avancée considérable dans la mesure où elle permet aux forces de l'ordre de recourir à la captation à distance de données informatiques dans les affaires de criminalité organisée. Cette nouvelle procédure particulièrement intrusive est fort heureusement très encadrée et limitée au champ spécifique de la criminalité organisée.

Toutes ces évolutions vont dans le « *bon sens* » et devraient permettre aux entreprises – comme aux personnes physiques d'ailleurs – d'être de mieux en mieux protégées contre la cybercriminalité. ◈

Abonnez-vous vite !

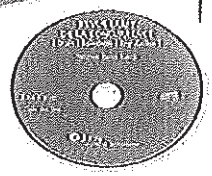
Revue Lamy de la Concurrence

Pour 2 ans
833 € HT seulement
au lieu de 952 € HT
soit 3 mois de lecture gratuite
Pour 1 an : 462 € HT



La Revue trimestrielle de la concurrence

Compris dans votre abonnement annuel
- 4 numéros de la *Revue Lamy de la Concurrence*
- 1 cédérom archives actualisé, accès @revue en ligne
- Le texte intégral des sources commentées et citées
- Le service d'actualités en ligne « Dernière minute Concurrence »
- Un partenariat privilégié avec les *Matinées-débats Concurrence* de la *Lettre des Juristes d'Affaires*



Wolters Kluwer France

Conditions de vente, informations et commandes :
www.wkf.fr

BULLETIN D'ABONNEMENT
À retourner à l'adresse suivante :
Wolters Kluwer France - Service Clients - Case Postale 402
1, rue Eugène et Armand Peugeot - 92856 Rueil-Malmaison cede
Fax : 01 76 73 48 09 - N° Indigo 0 825 08 08 00 - www.wkf.fr

☐ Oui, je m'abonne à la *Revue Lamy de la Concurrence* (réf. 00158) et je choisis :
☐ L'abonnement 2 ans au prix de 833 € HT (850,49 € TTC) ; je bénéficie alors de 3 mois de lecture gratuite.
☐ L'abonnement 1 an au prix de 462 € HT (471,70 € TTC)

☐ Vous trouverez ci-joint mon règlement de _____ € TTC par chèque à l'ordre de Wolters Kluwer France SAS, je recevrai une facture acquittée.
☐ Je réglerai à réception de la facture.

☐ Mme ☐ Mlle ☐ M. 002579 007
Nom : _____
Prénom : _____
Fonction : _____
Établissement : _____
Adresse : _____
Code postal : |_|_|_|_|_|
Ville : _____
Téléphone : |_|_| |_|_| |_|_| |_|_| |_|_|
Télécopie : |_|_| |_|_| |_|_| |_|_| |_|_|
E-mail : _____
N° Siret : |_|_|_|_|_|_|_|_|_|_|_|_|_|_|
Code NAF : |_|_|_|_|_| ☐ Siège ☐ Établissement
Nombre de salariés à mon adresse : _____

Date et Signature :