Synthèse
La pression réglementaire s'accentue **P 16**

Décryptage
Les lois de 2004 font les chantiers de 2005 **P 20**

Formation
Des cursus mal adaptés aux informaticiens **P 21**

DSI, maîtrisez les risques juridiques

Marc Guillaumot

Garant du fonctionnement du système d'information, le DSI peut également se muer en responsable de ses dysfonctionnements. Une charge susceptible de l'amener devant les tribunaux, surtout si sa direction lui a fait signer une délégation de pouvoir. Mais aussi, plus sûrement, d'entacher sa carrière. Une seule solution pour se protéger : anticiper les risques et savoir alerter sa direction générale à temps.

Synthèse Le DSI placé sous contrainte réglementaire

La mission du DSI, garant du système d'information de son entreprise, peut l'entraîner sur des terrains dangereux, voire le conduire au pénal dans certaines circonstances, si des mesures de précautions ne sont pas engagées. Mais le respect de ces contraintes est aussi affaire de bon sens.

Dans le cadre de sa mission, le directeur des systèmes d'information a pour obligation de veiller à la sécurité des systèmes et réseaux de l'entreprise ainsi qu'au respect des dispositions légales et réglementaires. Une évidence. Mais de cette formulation découle un ensemble de règles à respecter qui doivent non seulement conduire le DSI à adopter un comportement vigilant sur l'existant, mais aussi à se muer en force de proposition sur l'évolution.

Concrètement, sur les aspects de sécurité, plusieurs mesures sont à mettre en place. Lutter contre les atteintes de l'extérieur ou de l'intérieur, tout d'abord, en définissant notamment une politique de sécurité incluant des mesures techniques (pare-feu, contrôle et gestion des accès, mise à niveau des logiciels de sécurité choisis…) pour protéger l'accès au système d'information. Garantir la confidentialité, l'authentification et l'intégrité des échanges et des transactions, notamment pour les cybermarchands, à travers des processus de signature électroniques et, éventuellement, le recours à la cryptographie. "*Il ne faut pas qu'il puisse y avoir contestation des échanges*, explique Christiane Féral-Schuhl, avocate associée au cabinet Salans. *Ce point peut-être traité rapidement, mais il ne faut pas l'évacuer.*" Le DSI doit également assurer la continuité de service et prévoir des solutions de substitution en cas de rupture, en fonction de la sensibilité des applications. Il est en charge de la conservation du patrimoine informationnel de l'entreprise et doit pouvoir le restituer, par une politique d'archivage avec des garanties d'authenticité et de lisibilité.

Sur le volet des dispositions légales et réglementaires, le DSI doit respecter la protection des données à caractère personnel (en passe d'évoluer, *voir page 20*). Et ne pas empiéter sur les libertés des salariés en matière de cybersurveillance, en gardant en mémoire trois principes : la proportionnalité des moyens mis en œuvre par rapport au but recherché, la transparence vis-à-vis des salariés et la transparence vis-à-vis du comité d'entreprise. La législation sur les contrats à distance est aussi un élément à valider, ainsi que l'application des prescriptions fiscales et administratives en vigueur. Enfin le DSI doit se conformer aux droits de la propriété intellectuelle et veiller à ne mettre en œuvre que des instructions de sa hiérarchie conformes au droit.

Marc Guillaumot

S'il a signé une délégation de pouvoir, le DSI peut voir sa responsabilité pénale engagée et se retrouver devant les tribunaux *(ici, le Palais de justice de Paris)*. Mais c'est surtout son avenir dans l'entreprise qui est en jeu.

Attention au risque pénal

On le voit, la liste paraît longue et les tâches semblent ardues. D'autant que le terrain peut se révéler miné. Ainsi, dans le cas de préjudice à un tiers (par exemple, piratage de logiciel) causé par le DSI, c'est le principe de responsabilité de l'employeur qui s'applique, sauf si le directeur informatique a agi sans autorisation, à des fins étrangères à ses attributions, se plaçant ainsi hors de ses fonctions. Attention également aux délégations de responsabilité que peut lui faire signer sa direction générale : dans ce cas, sa responsabilité pénale est engagée en cas d'infraction (par exemple, contrefaçon de logiciels) qu'il commet lui-même ou que commettent des salariés travaillant sur ses instructions. Et ce, même si le DSI agit sur ordre de son employeur. *A contrario*, en l'absence de délégation de pouvoirs, sa responsabilité personnelle n'est pas engagée s'il reste dans le cadre de sa mission.

Isabelle Renard, avocate associée au cabinet August et Debouzy, souligne l'importance de cette délégation de pouvoir *(voir l'encadré ci-dessous)* dans d'autres cas, plus subtils. En effet, la signature de ce document rend le DSI pénalement responsable, à la place de son employeur, par exemple dans des infractions en matière de diffamation ou de contrefaçon commises par des salariés de son entreprise. Même si ceux-ci ont agi seuls, en l'absence de toute instruction d'un supérieur hiérarchique ou en infraction avec les règles en vigueur dans la société. Dans ce cas, c'est la fourniture de moyens informatiques permettant la réalisation de l'infraction qui peut conduire à la mise en cause du DSI. Un danger qui guette notamment dans les cas d'atteinte à un secret de fabrication, qui sanctionne les employés ayant révélé un secret ou un savoir-faire ou ayant effectué un détournement des informations confidentielles de l'entreprise (article L.152-7 du Code du travail) ou d'intrusion non autorisée d'un salarié dans un système d'information autre que celui de son entreprise (application de la loi Godfrain du 5 janvier 1988).

Toujours dans le cadre du pénal, est assimilée à de la contrefaçon l'introduction non autorisée dans l'entreprise d'éléments protégés par un droit de propriété intellectuelle. Selon un livre blanc publié par Staff&Line, les responsables de ces délits peuvent encourir des peines d'emprisonnement allant jusqu'à deux ans, ainsi que des amendes pouvant atteindre 150 000 euros pour des personnes physiques et 750 000 pour des personnes morales. Sans compter qu'en termes d'image, l'entreprise a beaucoup à y perdre. Un point que confirme Patrick Deleau, juriste de formation et président de la société Legal Suite, qui propose une offre logicielle pour la gestion des directions juridiques, pour qui les affaires d'infraction à la propriété intellectuelle font même peser un risque sur la survie de l'entreprise.

DÉLÉGATION DE POUVOIR : UNE ARME DE NÉGOCIATION AUSSI

Fréquemment utilisée pour les services des ressources humaines et les directions financières, la délégation de pouvoir tend à se généraliser aux DSI. Pour un employeur, ce document permet de reporter le risque sur ce salarié : c'est ce dernier qui sera poursuivi en cas d'infraction pénale. Il s'agit d'un acte écrit, différent de l'acte de mission et clairement spécifié. Pour que la délégation de pouvoir soit valable, deux conditions doivent être réunies : il faut que le salarié qui la signe ait les compétences nécessaires pour l'exercer, et que ce salarié dispose des moyens suffisants pour mener à bien sa mission. Il s'agit donc pour le DSI d'un vrai levier de négociation pour bénéficier du budget estimé nécessaire dans le cadre de son action. Lorsque les moyens mis à sa disposition lui semblent insuffisants, le DSI doit penser à préciser par écrit que les ressources allouées rendent impossibles l'accomplissement de sa mission. Un DSI peut reporter sa délégation de pouvoir sur un subordonné… à condition que ce dernier dispose de la compétence, de l'autorité et des moyens nécessaires. **S. H.**

Enfin les infractions sur les données nominatives, notamment la réalisation de traitements automatisés sans que soient prises toutes les précautions utiles pour préserver la sécurité de l'information, peuvent conduire à de lourdes peines selon l'article 226-17 du Code pénal. Isabelle Renard insiste : *"Les données nominatives, c'est-à-dire toutes celles qui permettent d'identifier une personne, doivent être sécurisées. Or aujourd'hui, les DSI ne savent pas toujours où sont situées ces données. Il y a eu l'année dernière des cas de chantage aux données nominatives. C'est un risque à la fois économique et de détérioration de l'image de marque, considérable pour l'entreprise."* Une tendance confirmée par le dernier rapport du Clusif, qui note une "professionnalisation" de la cybercriminalité, avec des pirates qui tentent de plus en plus de monnayer leurs forfaits.

A signaler également deux éléments dans les dispositions du Code du travail souvent négligés ou oubliés. D'une part, l'introduction de toute technologie nouvelle dans l'entreprise doit faire l'objet d'une information spécifique d'organes représentatifs du personnel sous peine de délit d'entrave. On pense notamment à l'introduction des PGI, qui souvent modifient en profondeur les processus internes. Il en va de même pour l'introduction d'un système de traitement automatisé de données nominatives du personnel.

Gestion à la petite semaine

Le DSI endosse également une responsabilité d'ordre disciplinaire. *"Si un responsable informatique n'a pas pris en compte un risque de type pénal, et en cas d'absence de délégation de pouvoir, c'est l'employeur qui sera poursuivi*, remarque Isabelle Renard. *Mais il y a de forte chance pour que cette action se répercute négativement sur la carrière du DSI. Prendre les mesures de base, liées à un état de l'art dans le secteur d'activité concerné* (voir page 18) *est incontournable. On peut reprocher au DSI de l'avoir ignoré ou de ne pas avoir mis son employeur en garde."*

Au-delà des mises en œuvre techniques, qui entrent logiquement dans leur domaine de compétence, les DSI éprouvent plus de difficultés à cerner les risques qui relèvent de la gestion ou de l'organisation. *"Avec les prestataires, notamment dans l'infogérance, la gestion se fait encore parfois à la petite semaine, avec des contrats mal ficelés*, remarque Isabelle Renard. *C'est souvent dû au dialogue qui reste difficile avec les juristes en interne, ces derniers ne proposant pas toujours une approche suffisamment opérationnelle ou manquant de disponibilités. De plus, en France en particulier, il demeure encore une méconnaissance de ce qui est incorporel. C'est une question de culture du management."*

La fonction du RSSI

C'est sans doute cette méconnaissance de la gestion des risques qui a été à l'origine de la naissance, principalement dans les très grandes entreprises, de la fonction de RSSI (responsable de la sécurité des systèmes d'information), avec la volonté de s'ouvrir aux problèmes de sécurité de cette nature. *"L'accumulation des tâches a abouti à une séparation des fonctions : au DSI de faire fonctionner le système d'information, alors que le RSSI est en charge des risques qui y sont liés"*, explique Grégoire Goussu, avocat au cabinet Gide Loyrette Nouel. *"Le RSSI a ainsi un rôle de veille, de conseil et d'alerte et devient en quelque sorte l'audit du DSI. Les secteurs les plus sensibles, tels que les grandes banques ou la Française des Jeux, ont été les premiers à inventer et à exploiter la fonction."* Ils sont aujourd'hui largement suivis par d'autres secteurs d'activité.

Néanmoins la définition du RSSI se

Suite page 18 ➤

ANCIENS SALARIÉS, LA VULNÉRABILITÉ OUBLIÉE

Selon les chiffres donnés par Marc Bernis, directeur technique de HP Sofware France, lors du colloque Risk Management organisé le 1er février par le cabinet IDC, 81 % des failles de sécurité proviennent de comptes d'employés ayant quitté la société. Un chiffre qui prouve l'état d'impréparation des DSI dans la gestion des identités au quotidien. Un véritable casse-tête il est vrai, du fait de la multiplication des applications et des droits qui s'y rapportent. Cette absence de nettoyage des annuaires constitue toutefois une menace pour le DSI, dont la responsabilité serait mise en cause en cas d'intrusion d'un ancien salarié désireux de se venger de son ex-employeur par exemple. Et demeure de toute façon une plaie ouverte dans la politique de sécurité IT de l'entreprise. D'autant que, comme le révélait également Marc Bernis, moins de la moitié des sociétés mènent régulièrement un audit des droits de leurs utilisateurs. Un désintérêt qui ne risque pas d'accélérer la prise de conscience des responsables informatiques sur ce sujet. **R. F.**

ASSURER SON INFORMATIQUE : PAS SI SIMPLE !

Assurer son système d'information, c'est rassurant. Difficile, cependant, de trouver des polices spécifiques clés en main. Cela ne signifie pas pour autant qu'assureurs et courtiers se désintéressent du sujet. *"Toutes les offres d'assurance autour des systèmes d'information sont envisageables"*, assure Valérie Leprovost, directrice de l'unité nouvelles technologies chez l'assureur Aon. Mais chaque cas est particulier et tout se négocie. Une police générale d'entreprise peut suffire à couvrir les principaux risques, notamment ceux liés aux matériels, au titre de la responsabilité civile ou des dommages. *"Si votre système d'information n'est pas critique, n'entreprenez aucune démarche spécifique"*, explique Jean-Laurent Santoni, responsable du pôle Audit et conseil chez Marsh. En revanche, si un sinistre ou un incident peut avoir de graves conséquences, mieux vaut prendre les devants. *"En mettant un accent particulier sur les risques dont la fréquence est faible, mais l'impact élevé"*, conseille-t-il. Le point le plus délicat concerne les pertes d'informations, tantôt protégées par des droits de propriété intellectuelle (logiciel, œuvre numérique, base de données...), tantôt non-objets de droits particuliers (fichier clients, descriptif de processus...). Avec, au-delà de l'indisponibilité du "patrimoine informationnel", des impacts en termes d'atteinte à l'image de marque, d'arrêt d'activité, d'efforts de gestion de crise, etc. **T. P.**

Marc Guillaumot

Jean-Laurent Santoni, responsable du pôle Audit et Conseil chez Marsh : ***"Sans système d'information critique, pas de démarche spécifique."***

ILS ONT DIT


MARC GUILLAUMOT

Christiane Féral-Schuhl, avocate associée au cabinet Salans : ***"Au-delà des contraintes imposées, le DSI doit avoir un rôle de veille technico-juridico-économique et savoir se muer en force de proposition".***


MARC GUILLAUMOT

Isabelle Renard, avocate associée chez August et Debouzy : ***"Le dialogue entre DSI et juristes reste difficile. Ces derniers ne proposant pas toujours une approche suffisamment opérationnelle."***

Patrick Deleau, président de la société Legal Suite : ***"Les affaires d'infraction à la propriété intellectuelle endommagent profondément l'image de marque d'une entreprise, faisant même peser un risque sur la survie de celle-ci."***


DR

cherche encore, au niveau tant de ses missions que de sa place dans l'organisation. D'autant qu'un nouvel intervenant devait prochainement apparaître, le CIL (correspondant "informatique et libertés"), prévu par la nouvelle loi Informatique et libertés dont les décrets d'application doivent sortir en mars. *"La nomination, non obligatoire, d'un CIL permettra de réduire la paperasse concernant la protection des données à caractère personnel en remplaçant les déclarations obligatoires auprès de la Cnil par une simple demande d'autorisation. Le CIL sera ainsi le garant, pour l'entreprise, des obligations liées à la Cnil"*, explique Grégoire Goussu. Qui remarque toutefois que *"la mission du CIL, de même que sa fonction, restent encore mal définies"*

SOPHIE HUET, AVEC REYNALD FLÉCHAUX

LES PRINCIPALES ACTIONS PRÉVENTIVES

▷ Ne pas négliger le devoir d'alerte

Le DSI doit avertir par écrit sa direction générale ou sa direction financière des risques que fait peser telle ou telle pratique (exposition aux virus, manque de "traçabilité" financière au regard des exigences légales de la Loi sur la sécurité financière ou de Sarbanes-Oxley...) et suggérer les investissements nécessaires. Faute de quoi, cette négligence lui sera reprochée et pourra entraîner son licenciement pour faute grave ou lourde.

▷ Penser à l'archivage des données

Une contrainte lourde qui touche tous les documents administratifs et fiscaux dématérialisés. Les durées de conservation légales sont très longues : dix ans pour les éléments de facturation et les pièces justificatives de TVA, trente ans pour les contrats commerciaux, cinq ans pour les bulletins de paie...

▷ Eviter le délit de marchandage

Ce délit est constitué dès que le recours à la sous-traitance est justifié par la volonté de l'employeur de ne pas attribuer aux employés du sous-traitant tous les avantages sociaux dont bénéficient les autres salariés. Il faut donc acheter une prestation, et non du temps de travail, et éviter tout lien hiérarchique direct entre le chef de projet de l'entreprise et les ingénieurs de la SSII.

▷ Garder un œil sur les fichiers nominatifs

Même si la réforme de la loi Informatique et libertés va alléger les contraintes, la constitution et la manipulation de fichiers nominatifs restent soumises à autorisation de la Cnil. Et les interdictions pesant sur certains types d'informations (origine ethnique, religion...) sont maintenues. Au DSI de mettre en garde les directions opérationnelles susceptibles de franchir la ligne jaune.

▷ Respecter la propriété intellectuelle

Le DSI doit veiller à ce que tous les logiciels utilisés dans l'entreprise disposent d'une licence valide. Mais attention à quelques autres subtilités, comme l'utilisation illicite sur un site Web de textes et d'images protégés par le droit d'auteur. Faute d'accord particulier, les développements spécifiques réalisés par une SSII demeurent sa propriété.

▷ Rédiger une charte informatique

Usage de logiciels piratés, téléchargement en pair-à-pair de musique ou de films, ressources de l'entreprise détournées à des fins personnelles, consultation de sites pornographiques ou incitant au piratage : par leurs pratiques, les utilisateurs mettent en danger la sécurité du SI. Le DSI est pénalement responsable s'il a signé une délégation de pouvoirs. Les avocats recommandent la rédaction d'une charte informatique : un code de bonne conduite des salariés vis-à-vis des outils mis à leur disposition. Une formation régulière des utilisateurs permet aussi de rappeler ces consignes de base.

▷ Recourir aux juristes pour les contrats

Le recours à l'infogérance rend certains contrats de service critiques pour l'entreprise. Le DSI doit impliquer des juristes, de son entreprise ou d'un cabinet, le plus tôt possible dans la mise en œuvre des projets. Un bon contrat de services doit prévoir toutes les hypothèses, y compris un dérapage important du projet.

▷ Anticiper les contraintes métier

Certains métiers sont soumis à des contraintes réglementaires fortes, en particulier la finance (Bâle II), la pharmacie ou l'agroalimentaire (règlement européen sur la traçabilité). Le respect de ces réglementations exige des investissements que doit consentir la direction générale.

▷ Réfréner les ardeurs en matière de cybersurveillance

L'informatique facilite grandement la surveillance des salariés. Mais ceux-ci doivent être informés de tout moyen mis en œuvre pour décortiquer leur activité. Et ces moyens doivent rester "proportionnels aux objectifs".

Décryptage Les lois de 2004 font les chantiers de 2005

Loi pour la confiance dans l'économie numérique, réforme de la loi informatique et libertés, dématérialisation des achats publics... Si 2004 a été riche en réformes impliquant l'informatique, 2005 va voir leur mise en pratique.

Depuis le 1er janvier, les textes de lois remettant en cause les pratiques professionnelles des responsables informatiques se sont multipliés. Ainsi, d'après la loi pour la confiance dans l'économie numérique (LCEN), la diffusion de pourriel est punie de deux ans de prison et 37 500 euros d'amende. Parallèlement, depuis la promulgation de la réforme de la loi informatique et libertés, le 6 août dernier, la Cnil (Commission nationale de l'informatique et des libertés) a la possibilité d'infliger des amendes administratives (jusqu'à 300 000 euros). L'empêcher d'enquêter ou tenter de limiter ses investigations est, de plus, puni de 15 000 euros d'amende.

A l'inverse, les nouvelles réglementations ouvrent la voie à des simplifications qui devraient se concrétiser en 2005. Exemple avec la Cnil : la nouvelle loi permet *"de dispenser de déclaration certains traitements qui ne sont pas susceptibles, dans le cadre de leur utilisation régulière, de porter atteinte à la vie privée ou aux libertés des personnes"*, explique le site de la commission. Sont concernés par cette dispense les fichiers de paie et la gestion informatisée des déclarations obligatoires (DADS, emploi de travailleurs handicapés...) et des registres obligatoires (tels que le registre unique du personnel).

Très attendue par les responsables informatiques, la suppression de l'obligation de déclaration à la Cnil de tout traitement comportant des informations nominatives, pourvu que l'entreprise dispose d'un *"correspondant aux données personnelles"*. Mais le statut de celui-ci est encore en suspens.

Une autre réforme concerne le secteur public et ses fournisseurs : la dématérialisation des marchés publics. Depuis le 1er janvier, aucun acheteur public ne peut refuser une offre sous prétexte qu'elle est parvenue par voie électronique. Malgré la création d'une plate-forme mutualisée sous les auspices de l'Adaé (Agence pour le développement de l'administration électronique) et de l'Ugap (Union des groupements d'achats publics), des contentieux pourraient apparaître dans le courant de l'année.

BERTRAND LEMAIRE

POUR EN SAVOIR PLUS

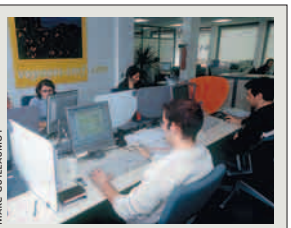
- L'ensemble des textes de référence concernant l'économie numérique :

Pour la confiance en l'économie numérique, collectif, Editions des Journaux officiels, collection "Aux sources de la loi", 756 pages, 18,20 €.

- Textes régissant les médias, Internet, le commerce électronique, la conservation et le traitement des données nominatives, l'archivage, etc. (accompagnés de commentaires) : **Code de la communication**, édition 2005, Editions Dalloz, 1 337 pages, 65 €.

MISE EN ŒUVRE

Voyages-sncf.com gagne à donner confiance



MARC GUILLAUMOT

Fruit d'un rapprochement de l'Américain Expedia et de la SNCF, le portail Voyages-sncf.com agrège les offres commerciales de ses deux géniteurs. La promulgation de la LCEN (loi pour la confiance dans l'économie numérique) lui a particulièrement donné du fil à retordre. *"La LCEN a été un catalyseur pour nos actions,* explique Chrystel Raharijaona, directrice du marketing relationnel. *Le taux de clics sur les liens dans la lettre d'information a augmenté et le taux d'ouverture a crû de 10 %. Elle était déjà conforme à la loi, car la simple création d'un compte ne suffisait pas à la recevoir, il fallait manifester sa volonté de l'obtenir. Mais notre structure particulière nous a obligés à qualifier chaque client comme étant client du train uniquement, client des autres prestations uniquement ou client mixte."* Les informations reçues par le client devant correspondre à sa classification.

"La logique du site repose sur la possibilité de se renseigner, voire d'acheter avant de s'identifier ou de s'inscrire. Le tout en un minimum de clics, ajoute Chrystel Raharijaona. *Or la LCEN nous a contraints à prévoir une relecture de la commande avant validation. De plus, comme la création d'un compte client n'est pas obligatoire, la relation client recommence chaque fois à zéro."* Ces contraintes n'ont pas pesé sur le chiffre d'affaires : en un an, Voyages-sncf.com a vu celui-ci croître de 71 %. B. L.

VOYAGE-SNCF.COM EN FAITS ET EN CHIFFRES

Voyages-sncf.com rassemble les offres de deux sociétés : une filiale à 100 % SNCF et une coentreprise SNCF-Expedia.
Chiffre d'affaires 2004 : 784 millions d'euros (dont 648 millions sur la vente de billets de train, soit 12,2 % des ventes de la SNCF) pour 11,1 millions de transactions.
Bénéfice net 2004 : 9,5 millions d'euros.

Formation Peu de cursus destinés aux DSI

Cycles longs destinés à une population de juristes, cycles courts trop segmentés. Le parcours est épineux pour les informaticiens.

QUELQUES FORMATIONS AU DROIT DE L'INFORMATIQUE

Organisme	Intitulé	Contenu	Prix	Durée
Afai	Management de la sécurité informatique	Cadre juridique de la sécurité informatique (Cnil, loi Godfrain, propriété intellectuelle, économie numérique, droit des contrats, surveillance des salariés, élaboration des chartes)	1 600 € pour les non-adhérents	4 jours
Cegos	Les achats de prestation	Maîtrise des risques juridiques et rédaction de contrats solides, droit intellectuelle de la propriété intellectuelle et artistique, obligations contractuelles, clauses de confidentialité et de responsabilité	1 390 €	3 jours
Comundi	Maîtrisez le régime juridique des fichiers et traitements informatiques	L'enjeu informatique et libertés, la gestion des nouvelles procédures de déclaration à la Cnil, libertés individuelles et gestion du personnel, gestion des clients et des prospects	1 595 €	2 jours
INPI	Les outils de la propriété intellectuelle	Aspects juridiques et procéduraux de la protection des créations artistiques du design, du brevet et des marques, ainsi que les autres droits applicables	200 € par jour	De 1 à 3 jours
Université Paris-2	DESS droit du multimédia et de l'informatique	Associer les connaissances élémentaires (droit des contrats, propriété intellectuelle) et spécifiques (contrats informatiques, protection des données)	Prise en charge	325 heures
Université Paris-Sud	DESS du numérique et des nouvelles techniques	Droit des propriétés intellectuelles et protection des créations informatiques, nouvelles techniques, droit des obligations, etc.	Prise en charge	Cycle long

Source : LMI

Peu d'informaticiens sont sensibilisés aux subtilités juridiques de l'informatique. La faute à une formation encore mal adaptée et qui n'aborde pas l'ensemble des problématiques du droit de l'informatique. "*Les grandes écoles d'ingénieurs, comme Supélec ou Centrale, intègrent bien une dimension juridique à leur offre*, explique Antoine Latreille, codirecteur du master en droit, innovation, communication et culture (DI2C) à l'université de Paris-11. *Mais les contenus ne balaient pas l'ensemble des problématiques et ne délivrent qu'un vernis du droit informatique.*"

La solution passe donc plutôt par des cursus courts, en formation continue. En théorie. Car, ainsi que le note Isabelle Renard, ingénieur et avocate associée du cabinet August et Debouzy, "*les formations techniques de quelques jours sont en général trop ciblées et ne permettent pas d'obtenir une vision globale qui permettrait de limiter la responsabilité du DSI et celle de l'entreprise*". A l'inverse, les cycles longs, de type DESS de l'enseignement supérieur, exigent un solide bagage juridique et concernent plutôt les juristes.

Les formations de l'INPI (Institut national de la propriété industrielle) figurent dans la première catégorie. C'est la bonne filière pour des ingénieurs intéressés par les aspects juridiques de la propriété industrielle, mais elle ne couvre qu'un des aspects du droit informatique. Côté cursus longs, le DESS de l'université de Paris-Sud porte sur le droit du numérique et des nouvelles technologies. Mais il s'adresse aux titulaires d'une maîtrise de droit privé. "*Ce type de diplôme peut néanmoins s'ouvrir aux informaticiens qui souhaiteraient se reconvertir dans le juridique*", précise Antoine Latreille. Reste que les formations longues représentent un investissement lourd pour les entreprises.

Pour Isabelle Renard, seul le stage mis sur pied par l'Afai, auquel elle participe en tant qu'intervenante, permet de répondre aux attentes de la profession. Dans un programme de quatre jours intitulé "Management de la sécurité informatique" figure un module de droit taillé sur mesure pour les RSSI. Et l'association planche sur la mise en place d'une formation plus axée sur les contrats et sur les besoins des DSI.

VÉRONIQUE ARÈNE