GUIDE DE CONFORMITÉ
À L'ATTENTION DES ENTREPRISES

Organiser dès aujourd'hui la gestion des données électroniques

&

Anticiper les obligations légales de demain

Par Cynthia L. Jackson

BAKER & McKENZIE





Cynthia L. Jackson

Partner, Baker & McKenzie LLP

Installée à Palo Alto en Californie, Cynthia L. Jackson travaille en tant qu'associée au sein du cabinet Baker & McKenzie, le plus grand cabinet d'avocats au monde, avec des bureaux répartis sur 38 pays. Cynthia L. Jackson est l'auteur d'un guide de conformité à l'attention des entreprises (Business Guide to Compliance) qui vise à informer les chefs d'entreprise sur les questions de conformité au sens large, les obligations administratives et les exigences en termes de conservation des données électroniques. Elle exprime sa gratitude envers John Raudabaugh, un associé du cabinet de Chicago, pour sa contribution à certaines sections relatives à la surveillance des ressources, tirées de ses conclusions en tant qu'amicus curiae, publiées dans *The Guard Publishing Company et Eugene Newspaper Guild,* et présentées devant le NLRB (National Labor Relations Board, organisme national de protection des travailleurs américains) le 9 février 2007.

Cynthia L. Jackson représente les sociétés en cas de litiges et les conseille dans tous les domaines ayant trait à l'emploi, tant au niveau national qu'international. Ces domaines couvrent notamment les plaintes pour discrimination et harcèlement, les règles applicables au personnel et leur mise en œuvre, les contrats d'embauche et les indemnités de licenciement, les plans de licenciement, les codes de conduite, la confidentialité, la responsabilité sociale des entreprises, la protection des informations confidentielles et le secret commercial, ainsi que les incidences des fusions et acquisitions sur l'emploi.

Maître Jackson a été désignée comme l'une des « Meilleures avocates des États-Unis » et on la surnomme couramment la « Super avocate de Californie du Nord ». Maître Jackson est diplômée, avec mention, de l'université de Stanford et de l'école de droit de l'université du Texas.

Cynthia L. Jackson, Avocate
Baker & McKenzie LLP
660 Hansen Way, Palo Alto, Californie 94304, États-Unis
Téléphone : +1 650-856-5572
Télécopie : +1 650-856-9299
cynthia.l.jackson@bakernet.com





Table des matières





De quoi s'agit-il ?

L'archivage, la conservation, le suivi, le filtrage et le cryptage ne font plus partie des tâches facultatives, elles sont indispensables.

Dans un monde où l'utilisation des données électroniques ne cesse de croître, les entreprises doivent élaborer dès à présent des stratégies de gestion permettant de prévenir les risques juridiques. La prolifération des données électroniques est phénoménale et accablante. Compte tenu du volume d'informations que les ordinateurs moyens sont aujourd'hui en mesure de stocker, toutes les entreprises, aussi petites soient elles, disposent d'une capacité de stockage électronique équivalente à 2 000 armoires de rangement à quatre tiroirs.[1] La gestion de ces données est d'autant plus complexe qu'il ne s'agit plus de feuilles de papier réelles, mais d'octets virtuels qui représentent des informations constamment modifiées, déplacées et mises à jour par des personnes et des sources diverses. L'archivage, la conservation, le suivi, le filtrage et le cryptage ne font plus partie des tâches facultatives, elles sont indispensables.

Les systèmes de données électroniques contrôlent et dirigent des machines, traitent des données financières, gèrent des stocks, passent des commandes et transmettent des images et des documents. Ils accélèrent les communications verbales et non verbales de façon significative. L'e-mail est la forme la plus courante de communication électronique, mais il existe d'autres vecteurs tels que les bulletins en ligne (journaux Web ou blogs), la messagerie instantanée (les internautes « chattent » en temps réel), les conférences par webcams interposées, les transferts de documents et de vidéos, ainsi que les

[1] Jason Krause, *E-Discovery Gets Real,* ABA JOURNAL, février 2007 ; note de George L. Paul & Bruce H. Nearon, *The Discovery Revolution: A Guide to the E-Discovery Amendments to the Federal Rules of Civil Procedure,* ABA SECTION OF SCI & TECH. LAW.

En 2005, 24% des entreprises ont été citées à comparaître par présentation de courriers électroniques et 15% ont été attaquées en justice du fait de courriers électroniques rédigés par des employés.

services de voix à large bande. Toutefois, ces systèmes peuvent être utilisés à mauvais escient et nuire aux entreprises. Les messageries peuvent servir à harceler et à intimider des employés, des responsables et des tiers. Le personnel peut télécharger (« voler ») des éléments relevant de la propriété intellectuelle d'autres sociétés ou tiers, dénigrer l'entreprise, ses produits et services, ses clients et concurrents. Il peut également transférer des données volées vers des emplacements à distance ou les dissimuler sur le matériel de l'entreprise. Les utilisateurs peuvent consulter ou diffuser des documents jugés importuns et illégaux par décision de justice, créer et publier sur Internet des éléments à caractère diffamatoire, préméditer ou même perpétrer des crimes, tout cela à partir de leur lieu de travail, sous couvert des installations de l'entreprise.[2]

Rien d'étonnant donc à ce que, selon une étude réalisée par l'association des conseillers juridiques d'entreprise (Association of Corporate Counsel, ACC), 86% des conseillers interrogés aient classé au premier rang de leurs préoccupations, « le suivi des activités de la société pouvant avoir une incidence juridique ».[3] En 2005, 24% des entreprises ont été citées à comparaître par présentation de courriers électroniques et 15% ont été attaquées en justice du fait de courriers électroniques rédigés par des employés. Selon cette même étude, 10% des e-mails comprennent des éléments à caractère sexuel, romantique ou pornographique.[4] Même avant l'entrée en vigueur des preuves électroniques dans le code fédéral de procédure civile (Federal Rules of Civil

[2] *Electronic Workplace : Is Your Company's Work Blogging Down?* FEDERAL EMPLOYMENT LAW INSIDER, septembre 2006 (2) ; Michael R. Phillips, *Inappropriate Use of Email by Employees and System Configuration Management Weaknesses Are Creating Security Risks,* Treasury Inspector General for Tax Administration, 31 juillet 2006.
[3] ACC & SERENGETI, MANAGING OUTSIDE COUNSEL SURVEY REPORT, 23 octobre 2006.
[4] *Enquête de 2006 sur l'e-mail, la messagerie instantanée et les blogs (2006 Workplace E-mail, Instant Messaging & Blog Survey : Bosses Battle Risk by Firing E-mail, IM & Blog Violators),* par l'AMA, 11 juillet 2006, http://www.amanet.org/press/amanews/2006/blogs_2006.htm.

Procedure, FRCP) le 1er décembre 2006, plus d'une société sur cinq avait dû produire des communications électroniques dans le cadre de litiges ou d'enquêtes administratives au cours de l'année 2004.[5] Entre 2001 et 2004, ce pourcentage a plus que doublé.[6] En réalité, les entreprises américaines ont dépensé 1,2 milliard de dollars dans des services de recherche de preuves électroniques en 2005,[7] contre 1,9 milliard de dollars en 2006.[8] Avec l'application des nouvelles règles du FRCP sur les preuves électroniques, on aurait pu s'attendre à une croissance fulgurante de ces chiffres. Toutefois, contre toute attente, une étude publiée seulement deux mois avant l'entrée en vigueur de l'amendement au FRCP, montre que seuls 7% des conseillers juridiques d'entreprise indiquaient que leur société était préparée à l'application du nouvel amendement et 54% ne savaient même pas que cette modification législative s'appliquerait en décembre 2006.[9]

Les entreprises américaines ont dépensé 1,2 milliard de dollars dans des services de recherche de preuves électroniques en 2005. Ce chiffre a été estimé à 1,9 milliard de dollars pour l'année 2006.

Les sociétés doivent en outre se conformer à un nombre croissant d'autres lois réglementant les communications électroniques et les propositions de loi se multiplient.[10] La plupart des réglementations concernent la protection des données personnelles sensibles, *par exemple :* la loi de 1986 sur la confidentialité des communications électroniques (Electronic Communications Privacy Act)[11] ; la loi de 1996 sur la transférabilité et la responsabilité dans le cadre de l'assurance-maladie (Health Insurance Portability and Accountability Act)[12] ; la loi de 1998 sur la protection de la vie privée des enfants en ligne

[5] Enquête réalisée en 2004 par AMA/ePolicy Institute Research sur l'e-mail et la messagerie instantanée au travail, *(2004 Workplace E-mail and Instant Messaging Survey Summary,* (1)).
[6] *Idem*
[7] Sacha Consulting, Ramon Nunez, Metal INCS, Gregory McCurdy, Microsoft Corp, ABA Digital Evidence Project, The National Law Journal/www. NLJ.com, 19 septembre 2005.
[8] *Idem*
[9] Lexis Nexis® Applied Discovery® enquête réalisée lors de la conférence annuelle ACC 2006 au mois d'octobre 2006.
[10] *Data Security : Federal and State Laws,* rapport du CONGRESSIONAL RESEARCH SERVICE devant le Congrès des États-Unis d'Amérique, 3 février 2006 ; *Data Security : Federal Legislative Approaches,* rapport du CONGRESSIONAL RESEARCH SERVICE devant le Congrès des États-Unis d'Amérique, 9 février 2006 ; *Obscenity and Indecency : Constitutional Principles and Federal Statutes,* rapport du CONGRESSIONAL RESEARCH SERVICE devant le Congrès des États-Unis d'Amérique, 25 juin 2003.
[11] Titre 18 du Code fédéral des États-Unis d'Amérique § 101 *et suivants.*
[12] Titre 42 du Code fédéral des États-Unis d'Amérique § 201 *et suivants.*

Les courriers non sollicités représentent 93% des e-mails entrants.

(Children's Online Privacy Protection Act)[13] ; la loi Gramm-Leach-Bliley de 1999[14] ; la loi de 2003 sur le contrôle des attaques marketing et à caractère pornographique non sollicitées (Controlling the Assault of Non-Solicited Pornography and Marketing Act)[15] ; la loi de 2002 sur la signification des infractions liées à la sécurité en Californie (California Security Breach Notification Act)[16] ; la loi de 2004 sur la sécurité des informations d'ordre personnel en Californie (California Security Personal Information Act)[17] ; et de nombreuses autres législations nationales et internationales.[18]

Les sociétés doivent non seulement respecter les lois régissant la destruction et la conservation des documents, mais également se prémunir contre les pirates informatiques et les vols de contenus électroniques importants qui relèvent de leur propriété intellectuelle.[19] Internet ouvre en effet aux tiers un accès aux ressources les plus précieuses de l'entreprise. En 2004, la part des courriers indésirables sur l'ensemble des e-mails entrants s'élevait à 73% et elle atteint 93% en 2006.[20] Mis à part le désagrément et la perte de temps qu'ils entraînent, les courriers indésirables sont en grande majorité inoffensifs. En revanche, les pratiques et les logiciels malveillants, tels que virus, vers, programmes de téléchargement, chevaux de Troie, spam, référencement abusif, phishing et pharming mettent en péril le réseau, les informations professionnelles et la propriété intellectuelle de l'entreprise.[21] Des tiers peuvent

[13] Titre 15 du Code fédéral des États-Unis d'Amérique § 6501 *et suivants*.
[14] Titre 15 du Code fédéral des États-Unis d'Amérique §§ 6801 à 6809.
[15] Titre 15 du Code fédéral des États-Unis d'Amérique §§ 7701 à 7713.
[16] Cal. S.B. 1386 (2002) (Cal. Civ. Code §§ 1798.82 and portions of 1798.29).
[17] Code civil de Californie § 1798.81.5 (Cal. A.B. 1950 (2004)).
[18] Allan Holmes, *The Global State of Information Security 2006,* CIO MAGAZINE, 15 septembre 2006.
[19] *Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth,* rapport du CONGRESSIONAL RESEARCH SERVICE devant le Congrès des États-Unis d'Amérique, 13 avril 2005.
[20] AMA/ePolicy Institute Research, *2004 Workplace E-mail and Instant Messaging Survey* (2004) ; W*ireless Privacy and Spam: Issues for Congress,* rapport du CONGRESSIONAL RESEARCH SERVICE devant le Congrès des États-Unis d'Amérique, 22 décembre 2004 ; *« Junk E-mail » : An Overview of Issues and Legislation Concerning Unsolicited Commercial Electronic Mail (« Spam »),* rapport du CONGRESSIONAL RESEARCH SERVICE devant le Congrès des États-Unis d'Amérique, 15 avril 2003 ; *Cybercrooks Deliver Trouble,* WASHINGTON POST, 27 décembre 2006, D1.

pirater de l'extérieur les secrets commerciaux et les informations confidentielles de la société, subtiliser des mots de passe et rediriger les utilisateurs vers des sites de téléchargement. Sur l'ensemble de ces attaques, 33% sont initiées par des utilisateurs en interne.[22]

Lors d'un récent sondage réalisé par le centre national pour les applications des super-ordinateurs (National Center for Supercomputing Applications, NCSA) 40% des personnes interrogées ont déclaré qu'elles utilisaient des sites communautaires sur leur lieu de travail, exposant ainsi aux pirates le réseau de leur employeur[23] (68% des sociétés consultées ont indiqué avoir été victimes de crimes électroniques en 2004. Parmi ces dernières, 43% ont relevé des accès non autorisés à leurs informations, systèmes ou réseaux et 14% ont signalé un vol d'adresse IP).[24] Les tribunaux ont dernièrement dévoilé dans leurs comptes-rendus, l'affaire d'un scientifique senior employé par la société Dupont qui avait téléchargé 22 000 documents sensibles en moins de cinq mois. Celui-ci avait transféré 180 documents de Dupont vers un ordinateur portable pour les transmettre à son nouvel employeur. Ces documents, qui présentaient « les principales technologies et gammes de produits, ainsi que des technologies nouvelles en phase de recherche et de développement », ont été évalués à 400 millions de dollars américains.[25]

Les activités légales et « sans conséquences » peuvent également générer des coûts élevés et les tentations sont extrêmement nombreuses. Lors d'une enquête menée

[21] *Pharming*, WEBSENSE, INC. (2006) ; *The Economic Impact of Cyber-Attacks,* rapport du CONGRESSIONAL RESEARCH SERVICE devant le Congrès des États-Unis d'Amérique, 1er avril 2004.
[22] Scott Berinato, *The Global State of Information Security 2005,* PRICE WATERHOUSECOOPERS AND CIO, 15 septembre 2005
[23] *Rapport sur les réseaux sociaux, CA/NCSA Social Networking Study Report,* RUSSELLRESEARCH.COM (4), http://staysafeonline.org/features/SocialNetworkingReport.ppt.
[24] *Enquête sur les crimes électroniques : 2005 E-Crime Watch Survey – Survey Results,* CSO MAGAZINE, U.S. SECRET SERVICE, CERT COORDINATION CENTER., http://www.csoonline.com/info/ecrimesurvey05.pdf.
[25] David Kauffman, *How Safe Is Your Data?,* HR HERO LINE, 9 mars 2007.

en 2004 auprès de 840 sociétés américaines, 66% des entreprises interrogées ont indiqué que leurs employés utilisaient le réseau de la société à titre personnel au maximum deux heures par jour, deux à trois heures pour 24% d'entre elles, et plus de quatre heures pour les 10% restant.[26] Selon cette même enquête, 75% des employés envoient quotidiennement moins de 10 messages électroniques d'ordre personnel.[27] 90% des employés conversent à titre personnel jusqu'à 90 minutes par jour sur leur messagerie instantanée, 19% d'entre eux joignent des fichiers à leurs messages texte, 16% transmettent des blagues, des rumeurs ou des remarques désobligeantes, 9% envoient des informations confidentielles et 6% des messages comportant du texte à caractère sexuel, romantique ou pornographique.[28]

Face à leurs obligations légales et par mesure de protection, les entreprises doivent organiser et mettre en œuvre des pratiques d'utilisation saines, et former leur personnel avant que des problèmes d'ordre juridique ne surviennent. Peu de sociétés auront le loisir d'étudier ce genre de difficultés avant d'avoir à y répondre, en particulier si la loi concernée est déjà en vigueur, si des éléments de leur propriété intellectuelle ou des informations confidentielles ont été divulguées, ou une fois que l'ambiance de travail est devenue hostile. Toutes les organisations doivent s'y préparer. Tout d'abord, les entreprises doivent planifier la conservation, l'archivage et le suivi des communications. Elles doivent ensuite mettre en place des processus de chiffrement et des restrictions d'accès. Enfin, elles doivent instaurer des formations et des contrôles permanents de leurs méthodes et de leur politique.

[26] Enquête réalisée en 2004 par AMA/ePolicy Institute Research sur l'e-mail et la messagerie instantanée au travail, *(2004 Workplace E-mail and Instant Messaging Survey)*.
[27] *Idem.*
[28] *Idem.*

Qui est concerné ?

Dans le cadre d'une entreprise, la gestion des données électroniques concerne tout le monde : le département juridique, les agents de la mise en conformité, les agents comptables, le service financier, les responsables de l'informatique, les employés des ressources humaines, le personnel en charge des brevets et de la propriété intellectuelle, les responsables des achats, le service de contrôle des exportations et les commerciaux.

Par exemple, les sociétés américaines cotées en bourse ont des obligations de rapports, d'audit et de transparence dans le cadre de la loi Sarbanes-Oxley (SOX), ainsi que des obligations comptables et de conservation des archives selon la loi sur les pratiques de corruption à l'étranger (Foreign Corrupt Practices Act). Les sociétés en procès devant le tribunal fédéral, ou qui sont menacées de procès, doivent se tenir prêtes à agir pour conserver les données électroniques pertinentes qu'elles stockent. Dans le cas du secteur bancaire, financier ou de la santé, le stockage, l'utilisation, l'accessibilité et la diffusion des informations sont réglementés de manière extrêmement stricte. Ces organisations, qui opèrent à l'international ou exportent du matériel ou des logiciels, se trouvent dans l'obligation d'appliquer à leurs données, notamment pour le cryptage, des méthodes de gestion fort complexes et parfois contradictoires.

Pour toutes les autres entreprises, confrontées à des procès ou à des menaces de procès dans des secteurs hautement réglementés ou sur des marchés

Les sociétés en procès devant le tribunal fédéral, ou qui sont menacées de procès, doivent se tenir prêtes à agir pour conserver les données électroniques pertinentes qu'elles stockent.

Toutes les entreprises sont concernées. Les PME doivent elles aussi anticiper et déployer leurs systèmes dès aujourd'hui.

internationaux, l'ère des données électroniques génère également de nouveaux défis. Des études ont démontré qu'un tiers des vols de données sont commis par des employés actuels et que la grande majorité des allégations de dénigrement, de discrimination et de harcèlement sont formulées par des membres autorisés du personnel.[29] Toutes les entreprises sont concernées. Les PME doivent elles aussi anticiper et déployer des systèmes permettant de protéger leur propriété intellectuelle contre les vols, de prévenir les plaintes d'employés relatives à une ambiance de travail hostile ou de se préparer à interrompre la suppression des documents dans la perspective d'un procès.

Paradoxalement, ce sont ces mêmes technologies à l'origine de la prolifération des données et de nos maux de tête qui apportent des solutions de gestion dans des systèmes évolutifs, conçus pour garantir le respect des obligations légales imposées par les lois et juridictions compétentes. Ces systèmes électroniques doivent inclure des logiciels permettant la conservation des documents et leur archivage, le remplacement des procédures de destruction des documents, les restrictions d'accès par cryptage, le cas échéant, ainsi que le suivi et le filtrage Web lorsque cela est autorisé. Outre l'installation d'un système adéquat, il est impératif d'identifier les conditions légales à respecter et de former le personnel à une gestion appropriée des données au quotidien. Dans le cas d'une crise juridique, les données électroniques pourront ainsi être retrouvées et restituées rapidement et facilement.

[29] Scott Berinato, *The Global State of Information Security 2005*, PRICE WATERHOUSECOOPERS AND CIO, 15 septembre 2005.

La sélection et la mise en œuvre d'un système de gestion des données électroniques, l'élaboration et l'application de règles, la formation permanente du personnel et les contrôles assurant le bon fonctionnement du système avant l'apparition d'un problème juridique sont des tâches qui requièrent la collaboration de l'ensemble du personnel, des conseillers juridiques aux ressources humaines et de tous les autres services.

La sélection et la mise en œuvre d'un système de gestion des données électroniques, l'élaboration et l'application de règles, la formation permanente du personnel et les contrôles assurant le bon fonctionnement du système *avant l'apparition d'un problème juridique* sont des tâches qui requièrent la collaboration attentive de l'ensemble du personnel.





Obligations légales liées à l'archivage électronique

Ignorer les nouveaux amendements au code fédéral de procédure civile peut coûter cher.

En dehors des situations litigieuses, il n'existe aucune obligation universelle de conserver les données électroniques stockées (ou d'autres enregistrements), bien que la consignation de certains types de documents (déclarations d'impôts, dossiers d'emploi et statuts de l'entreprise) soit obligatoire selon les lois fédérales et nationales. En cas de litige, toutefois, l'obligation de conserver les documents ressurgit et impose aux entreprises de modifier leurs procédures de suppression des documents. Les nouveaux amendements au FRCP préconisent un « stockage à titre conservatoire » des documents que la société estime pouvoir utiliser comme preuves. Le « stockage à titre conservatoire » peut intervenir bien avant qu'un procès soit intenté (lorsque la société reçoit une plainte en interne concernant un responsable, lorsqu'elle reçoit une lettre d'un tiers ou d'un avocat exigeant la conservation de certaines données en vue d'une éventuelle action en justice, lorsqu'elle doit retrouver les échanges de correspondances avant un procès, lorsqu'elle reçoit une notification d'enquête par un organisme gouvernemental, une citation à comparaître ou une demande d'information d'un tel organisme, ou encore l'enregistrement d'une plainte administrative). Lorsqu'une situation de litige se présente, la société est tenue, selon ces amendements, de prendre toutes les mesures nécessaires à l'interruption immédiate des

L'entreprise a été condamnée à payer les frais de justice et d'avocat du plaignant en raison de son incapacité à suspendre la suppression des données et courriers électroniques, et à conserver les documents utiles après réception de la réclamation interne pour harcèlement sexuel.

procédures habituelles de destruction des données et de conserver tous documents utiles, notamment les données électroniques et méta-données associées dont elle sait ou devrait raisonnablement savoir qu'elles pourront servir dans le cadre d'une action en justice ou constituer des preuves admissibles.

Avant ces amendements récents au FRCP, les tribunaux montraient déjà peu de clémence envers les sociétés qui, plus ou moins sciemment, ne conservaient pas les données sensibles dans le cadre d'une instruction. Dans l'affaire *Broccoli contre Echostar Communications Corp.,* 229 F.R.D. 506 (D.C. Md. 2005), la Cour a retenu que l'employeur devait conserver les documents électroniques durant les 11 mois précédant la démission du plaignant/de l'employé. Cette obligation est née du fait des plaintes adressées par courrier électronique et verbalement par le futur plaignant à son employeur et signalant une situation de harcèlement sexuel. L'entreprise a été condamnée à payer les frais de justice et d'avocat du plaignant en raison de son incapacité à suspendre la suppression des données et courriers électroniques, et à conserver les documents utiles après réception de la *réclamation* pour harcèlement sexuel.

Dans une série d'affaires, *Zubulake contre UBS Warburg LLS,* 220 FRD 212 (S.D. N.Y. 2004), 229 F.R.D. 422 (S.D. N.Y. 20 juillet 004 Zubulake II) et 231 FRD 159 (S.D.N.Y. 3 février 2005 Zubulake III), la Cour a considéré que la société aurait dû conserver les documents électroniques durant les

quatre mois précédant l'enregistrement de la plainte pour discrimination (dix mois dans le cas d'une action devant le tribunal fédéral), car elle savait ou aurait dû savoir que ses procédures de suppression des documents aboutiraient à la destruction de preuves importantes. Dans l'affaire *Zubulake,* la Cour a établi que les cassettes de sauvegarde utilisées sur le réseau du défendeur constituaient bien une source d'indices appropriée, mais que des employés extérieurs au service juridique prenaient en charge la suppression de documents pertinents que le défendeur devait ensuite extraire à grands frais de récupération de méta-données.

Dans l'affaire *Wiginton contre CB Richard Ellis,* 229 F.R.D. 568 (N.D. Ill. 2003), la Cour a estimé que la société avait été informée de l'« action collective » intentée, uniquement par une notification envoyée par l'avocat du plaignant, dans laquelle des documents et plusieurs harceleurs présumés étaient identifiés. Cette notification avait été reçue plusieurs jours après l'enregistrement de la plainte. Par ailleurs, la Cour a considéré que la société avait pour obligation de conserver les disques durs, comptes de messagerie et historiques Web de toutes les personnes accusées de harcèlement sexuel ou impliquées dans cette affaire. De plus, la Cour a autorisé le plaignant à renouveler sa requête de sanctions pour incapacité à conserver des données électroniques concernant les dix harceleurs présumés et lui-même, dans le cas où des documents électroniques manquants se trouveraient sur les cassettes de sauvegarde de l'entreprise. Dans l'affaire *Consolidated Aluminum*

Corp contre Alcoa, Inc., 2006 U.S. Dist. LEXIS 66642 at *18 (M.D.La. 2006), la Cour a condamné Alcoa à payer pour la redéposition de tous les « acteurs clés » et pour les frais de requête et de recherche d'éléments manquants, car cette société avait attendu environ deux ans et demi après l'envoi de sa propre requête à Consolidated Aluminium avant d'interrompre sa procédure de destruction des documents. Dans l'affaire *Samsung Elecs. Co. contre Rambus, Inc.,* 2006 U.S. Dist. LEXIS 50007 (E.D.Va. 2006), Rambus, alors défendeur ayant émis une demande reconventionnelle, avait anticipé le litige en identifiant l'objet probable de celui-ci, les arguments légaux sur lesquels il s'appuyait et les documents connexes qu'il convenait de conserver et de détruire avant de riposter. La Cour en a conclu que Rambus avait volontairement détruit des données pertinentes et a prononcé des sanctions pour dissimulation de documents. Rambus avait ensuite annulé sa demande reconventionnelle avant que la Cour n'ait imposé ces sanctions.

Les sociétés qui, dans la perspective d'un litige, n'interrompent pas les procédures de suppression des informations et ne mettent pas en place un stockage des données à titre conservatoire, s'exposent à des conséquences désastreuses. Dans le cas *Zubulake,* la Cour a non seulement ordonné le paiement des frais d'enquête par le défendeur, mais elle a également émis des conclusions défavorables devant le jury. Ainsi, la Cour a indiqué au jury qu'il pouvait conclure que les documents détruits auraient étayé la plainte pour

discrimination émise par le plaignant, car ces documents n'étaient plus conservés depuis la date d'enregistrement de la plainte auprès de l'office américain de lutte contre les discriminations professionnelles (Equal Employment Opportunity Commission, EEOC), soit dix mois avant qu'un procès soit intenté. Le verdict du jury à l'encontre du défendeur a été exemplaire : 29 millions de dollars. Dans l'affaire *États-Unis d'Amérique contre Philip Morris USA Inc.*, 327 F. Supp. 2d 21 (D.D.C. 2004), la Cour a condamné Phillip Morris à payer 2,75 millions de dollars pour non application des règles de conservation des documents mises en place dans la société, soit 250 000 dollars pour chacun des onze responsables mis en cause. En outre, la Cour a interdit à ces onze responsables de témoigner au procès au bénéfice du défendeur. Dans l'affaire *Krumwiede contre Brighton Associates LLC,* 2006 U.S. Dist. LEXIS 31669 (N.D. Ill. 2006), la Cour avait dû rendre un jugement par défaut. Le plaignant/demandeur reconventionnel avait modifié des méta-données en continuant d'utiliser un ordinateur portable sans toutefois en supprimer l'intégralité. Il avait en effet omis de stocker cet ordinateur à titre conservatoire et continué de supprimer, de modifier et d'accéder à des fichiers avant de remettre l'ordinateur portable à un expert judiciaire. Dans l'affaire *Dempsey contre Pfizer,* 813 S.W. 2d 205 (1991), la Cour texanne avait prononcé une fin de non-recevoir à la requête de 42 000 000 de dollars américains pour compenser la suppression de documents.[30]

Le FRCP exige des parties adverses qu'elles collaborent au sujet des données électroniques tout au long de la procédure.

[30] Les cas suivants, tous prononcés avant l'entrée en vigueur des amendements au FRCP, ne sont pas non plus aberrants. Dans l'affaire *Quintus Corp. contre Avaya, Inc.* 2006 Bank.LEXIS 2912 (Bank. D. De. 2006), la Cour a prononcé un jugement de 1,88 million de dollars à l'encontre du défendeur, puisque ce dernier avait délibérément détruit des preuves qu'il était censé conserver, conformément aux lois en vigueur et en prévision d'un litige. Dans l'affaire *3M Innovation Properties C. contre Tomar Electronics, Inc.*, 2006 U.S. Dist. LEXIS 80571 (D. Minn 2006), la Cour a émis des conclusions défavorables, car le défendeur n'avait pas mis en place de stockage à titre conservatoire. Dans l'affaire *Napster,* 462 F.Supp.2d 1060, 1077-78 (N.D. Cal. 2006), le défendeur n'avait pas instauré le stockage à titre conservatoire en temps voulu et la Cour a également émis des conclusions défavorables. Dans l'affaire *NTL, Inc. Sec. Litig.* 2007 U.S. Dist LEXIS 9110 (S.D.N.Y. 2007), la Cour a considéré que l'entreprise, récemment reformée à la suite d'une faillite, ne conservait pas ses documents, et prononcé des conclusions défavorables assorties de sanctions pécuniaires. En décembre 2006, l'association NASD (National Association of Securities Dealers) a déclaré, dans le cadre d'une affaire encore en instruction, que Morgan Stanley avait faussement attribué la perte de millions d'e-mails à l'attentat du 11 septembre 2001 sur le World Trade Center.

Outre les sanctions pécuniaires, les tribunaux peuvent également engager la responsabilité civile des entreprises pour dissimulation de preuves et prononcer des sanctions pénales.

Outre les sanctions pécuniaires et les conclusions défavorables très lourdes évoquées plus haut, les tribunaux peuvent également engager la responsabilité civile des entreprises pour dissimulation de preuves et prononcer des sanctions pénales. Frank Quattrone, ancien employé au Credit Suisse First Boston, une banque d'investissement dans le secteur des hautes technologies, a été exclu définitivement du secteur boursier et condamné à payer une amende de 30 000 dollars américains par le NASD. Il avait été reconnu coupable d'obstruction à la justice et condamné à 18 mois d'emprisonnement pour avoir envoyé un e-mail demandant à son groupe de « faire du nettoyage dans leurs fichiers », selon les conclusions de l'enquête menée par la commission des opérations en bourse (Securities and Exchange Commission, SEC).

Comme l'indiquent les affaires précédemment citées, le FRCP n'a fait que codifier des décisions que les tribunaux ordonnaient depuis de nombreuses années au niveau fédéral,[31] et national, pour certains. Toutefois, les amendements au FRCP affectent également les plaideurs en ce qui concerne les deux éléments fondamentaux suivants : 1) ils répondent expressément à la question des preuves électroniques et obligent les parties et leurs avocats à rechercher, à conserver, à produire et à répondre des données électroniques, ce qui ne laisse aucun doute sur leur utilité ; et 2) ils exigent des parties prenantes qu'elles collaborent au sujet des données électroniques tout au long de la procédure. Durant les premiers mois de l'instruction, les parties adverses doivent se rencontrer afin de convenir des informations utiles

[31] En août 2006, une conférence réunissant des juges d'État a voté un document intitulé « *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information* » (Directives destinées aux tribunaux nationaux sur l'exploitation d'informations stockées électroniquement). Ces directives n'ont cependant aucun caractère obligatoire, à moins qu'elles n'aient été adoptées par l'État concerné. Le Massachusetts et la Caroline du Nord envisagent l'adoption de ces directives. Par opposition, l'État du New Jersey a voté le 1er septembre 2006 des règles relatives aux preuves électroniques basées sur celles du code fédéral de procédure civile. L'Arizona, la Floride, l'Idaho, le Maryland et le New Hampshire souhaiteraient également instaurer des règles similaires à celles du FRCP modifié. La diversité des règles applicables selon les États souligne encore davantage la nécessité de mettre en place des systèmes de gestion des données électroniques suffisamment flexibles pour convenir à tous les types de réglementation, de la plus stricte à la plus générale.

à conserver, de la forme à adopter pour les présenter (par exemple, format PDF, TIFF, d'origine, papier, etc.), d'indiquer si l'une des parties considère que ces données sont « inaccessibles », de préciser la manière dont les parties souhaitent gérer le coût exorbitant ou excessif des récupérations de données et la divulgation involontaire de secrets professionnels entre l'avocat et son client, des secrets commerciaux ou autres informations confidentielles ou protégées que pourraient dévoiler les documents papier ou électroniques produits conformément aux articles 16 (b) et 26. Contrairement aux entreprises qui se sont préparées et connaissent par avance les propositions les plus avantageuses, les sociétés qui n'ont pas su anticiper en instaurant des règles et des méthodes de conservation des documents, se trouvent généralement dans une position défavorable lors de ces rencontres préliminaires obligatoires.

Les modifications législatives apportées définissent également le rôle des données électroniques lorsque les parties doivent répondre à des questions écrites ou produire des documents physiques. Par exemple, l'article 33 (d) du code de procédure civile (FRCP) permet à la partie répondant de préciser que les informations demandées se trouvent dans des « documents professionnels de l'entreprise, y compris les données stockées sur des supports électroniques » si (i) ces réponses peuvent être vérifiées dans ces documents, (ii) le coût de vérification de ces informations est à peu près équivalent pour chacune des parties, (iii) la partie précise les documents qui doivent être examinés. Les modifications apportées à l'article 34

Il est probable que le format de présentation des données électroniques fera l'objet de débats mouvementés dans les années à venir.

du FRCP autorisent désormais expressément les parties à choisir la présentation à adopter pour les documents électroniques (papier ou électronique), bien qu'en l'absence d'accord à ce sujet ou sur décision du tribunal, l'amendement prévoie que les données électroniques stockées soient présentées au format sous lequel elles sont habituellement conservées ou sous une forme qui les rende raisonnablement exploitables.

Il est probable que le format de présentation des données électroniques fera l'objet de débats mouvementés dans les années à venir. Certains avancent que « la forme sous laquelle ils sont habituellement conservés » oblige les entreprises à produire des fichiers d'origine (ou natifs). D'autres objectent que le « format natif » ne facilite pas la suppression d'informations confidentielles ou protégées ou qu'il ne permet pas de contrôler le nombre de documents produits. Certains tribunaux et plaideurs ont estimé que les documents devaient être présentés en même temps que l'ensemble des méta-données associées. *C'est le cas des affaires Williams contre Sprint/United Management Company,* 230 FRD 640 (D. Kan. 2005), *D.E. Tech contre Dell Inc.,* 2006 U.S. Dist. LEXIS 87902 (W.D. Va. 2006), *Nova Measuring Instruments contre Nanometrics Inc.* 2006 U.S. Dist. LEXIS 49156 (N.D. Cal. 2006) et *Payment Card Interchange Fee and Merchant Discount Antitrust Litigation (action collective contre la société Visa, Inc. pour violation des lois antitrust)*, 2007 U.S. Dist. LEXIS 2650 (E.D. N.Y. 2007). Toutefois les

tribunaux et d'autres parties prenantes ont considéré que la présomption devait s'opposer à la production de méta-données, *notamment dans les affaires Kentucky Speedway contre National Association of Stock Car Auto Racing Inc.*, 2006 U.S. Dist. LEXIS 92028 (E.D. Ky. 2006), *Wyeth contre Impax Laboratories Inc.*, 2006 U.S. Dist. LEXIS 79761 (D. Del. 2006), *Tribu des Ponka (indiens d'Oklahoma) contre Continental Carbon Co.*, 2006 U.S. Dist. LEXIS 74225 (W.D. Okla. 2006). De son côté, l'association des Barreaux américains (ABA) a exprimé sa position dans sa publication n°06-442 en 2006 et préconise que les avocats susceptibles d'envoyer des méta-données protégées se chargent de « nettoyer » ces méta-données ou d'expédier une seconde version des documents sans méta-données, afin d'éviter la production involontaire de méta-données confidentielles ou protégées d'une quelconque manière. Les Barreaux de Floride et du Maryland imposent également aux avocats le « nettoyage » des méta-données protégées avant leur production. Quelle que soit la manière dont les tribunaux et Barreaux nationaux traitent ces questions, une chose est certaine : avant de produire des documents électroniques, les entreprises et leurs avocats doivent savoir de quelle façon leurs données sont stockées et la nature des méta-données qu'elles peuvent renfermer. Il est également dans leur intérêt de se préparer à ce type de difficulté bien avant les rencontres préliminaires obligatoires organisées par le tribunal fédéral.

L'article 37 modifié prévoit également une forme d'exonération de responsabilité en cas de défaut de production de données stockées électroniquement, lorsque ces données sont supprimées dans le cadre du fonctionnement habituel du système informatique et que la suppression est intervenue en toute bonne foi. Toutefois, comme indiqué précédemment, les tribunaux ne pourront pas considérer comme honnête une partie qui n'aura pas imposé de stockage à titre conservatoire en temps voulu. Cette obligation de conservation s'applique en outre aux cassettes de sauvegarde, disques durs, ordinateurs portables et autres matériels électroniques de stockage. Mais, si tous ces éléments semblent clairs, d'autres questions plus délicates peuvent se poser. Votre société utilise-t-elle des assistants personnels de type BlackBerry ? Certains e-mails sont-ils uniquement stockés sur ces assistants personnels et non sur les serveurs de la société ? Vos employés impriment-ils des copies papier des documents afin de les conserver, alors que ces documents sont régulièrement supprimés des supports électroniques ? Savez-vous où sont entreposés ces documents ? Certains de vos employés consultent-ils des forums électroniques, des programmes de messagerie instantanée ou leur messagerie personnelle au travail ? Le système informatique de votre société conserve-t-il des copies de ces documents ? Votre société procède-t-elle au suivi des suppressions ou des remplacements de données électroniques ? Ces procédures d'effacement peuvent-elles être interrompues pour certaines données contenant un terme particulier

(par exemple, le nom d'un plaignant éventuel, d'une fonction ou d'un produit acheté) ? Votre société a-t-elle suffisamment communiqué sur les règles relatives aux e-mails à conserver dans les dossiers personnels des ordinateurs de l'entreprise ? Ces règles sont-elles appliquées par vos employés de façon régulière ? Connaissez-vous la nature des méta-données que contiennent les ordinateurs de votre société ?

Un système efficace de gestion des données électroniques doit savoir traiter toutes ces questions en prévision d'un litige. Si une situation de litige se présentait, l'entreprise serait alors en mesure d'identifier et de consigner immédiatement les données connexes, quelle que soit leur forme.[32] Les données électroniques à stocker à titre conservatoire incluent non seulement les documents rédigés par la personne apparemment impliquée dans le futur litige, mais aussi tous les documents qui lui sont adressés ou qui la concernent. Ainsi, dans les cas de discrimination ou d'action collective, cela comprend toutes les personnes concernées par le litige éventuel.

Un système efficace de gestion des données électroniques doit savoir traiter toutes ces questions en prévision d'un litige. Si une situation de litige se présentait, l'entreprise serait alors en mesure d'identifier et de consigner immédiatement les données connexes, quelle que soit leur forme.

[32] Allen Smith, *Amended Federal Rules Define Duty to Preserve Work E-mails*, HR NEWS, 1er décembre 2006.





Ambiance de travail saine

De nombreux cas de harcèlement auraient pu être évités si des filtres avaient empêché l'envoi des e-mails incriminés.

Aux États-Unis,[33] on admet généralement que les systèmes de filtrage et de suivi des employés sont un mal nécessaire pour prévenir les plaintes relatives à l'ambiance de travail. « L'idée d'utiliser des filtres pour se décharger de certaines responsabilités semble être devenue une règle d'or. »[34] « De nombreux cas de harcèlement auraient pu être évités si des filtres avaient empêché l'envoi des e-mails incriminés. »[35]

Comme le démontrent les chiffres et même les études de cas les plus élémentaires en matière de conditions de travail hostiles, les systèmes de messagerie électronique ont été à l'origine de nombreuses plaintes pour discrimination et harcèlement. Par exemple, *EEOC contre Freddie Mac,* Civ. No. 97-1157-A, (3-4), E.D. Va. 24 juillet 1997, plainte enregistrée et suspendue pendant au moins trois ans, concernant la circulation dans l'entreprise de messages électroniques dégradants envers le mode d'expression des employés noirs américains (ebonics). L'employeur était alors tenu de « prendre rapidement toutes les mesures nécessaires pour éliminer le problème ». *Olivant contre Dept. of Environmental Protection (service de protection de l'environnement),* 1999 WL 430770 (N.J. Admin. Apr. 12), diffusion d'« humour » sexiste par le biais des systèmes de messagerie électronique constituant un harcèlement sexuel. *Trout contre la ville d'Akron,* plainte N° CV-97-115879 enregistrée le 17 novembre 1997 et ayant abouti au même verdict

[33] Sur le plan international, ces contrôles font l'objet de diverses restrictions et interdictions. Ce rapport décrit essentiellement les procédures applicables aux États-Unis, même si, comme l'indique la section VIII ci-après, il devient de plus en plus difficile de respecter l'ensemble des réglementations internationales en matière de gestion des données.
[34] Eugene Volokh, Professeur de droit à l'université UCLA, *Freedom of Speech, Cyberspace: Harassment Law and the Clinton Administration,* 63 LAW & CONTEMP. PROBS. 299 (2000).
[35] Wendy R. Leibowitz, *Avoiding E-mail Horror Stories: Policies and Filters the Best Defense,* N.Y. L.J., 15 décembre 1998, (5).

le 15 décembre 1998 : 260 000 dollars à l'encontre de la ville à cause d'employés municipaux qui consultaient des documents pornographiques sur leurs ordinateurs. Par opposition, dans l'affaire *Delfino contre Agilent,* 145 Cal. App.4th 790 (6th Dist., 2006), la Cour n'avait pas pu établir la responsabilité de l'entreprise pour les messages de menace qu'un employé envoyait sur Internet par le biais du système informatique de la société, car cette dernière avait réagi rapidement après avoir été informée de ce comportement malveillant. Par ailleurs, la législation fédérale interdit la pornographie pédophile qu'elle considère comme de la « contrebande », ce qui rend illégales la vente, la possession, la distribution, etc. de ce type de documents, conformément à la loi 18 USC 2251, entre autres. En effet, les entreprises sont dans l'obligation légale de signaler immédiatement au FBI toute utilisation de documents à caractère pédophile. Dans le cas contraire, elles se rendraient responsables des infractions commises dans ce domaine.

Les entreprises américaines sont toujours plus nombreuses à se protéger de tels abus en installant des systèmes d'analyse et de filtrage. Les employeurs américains qui ne contrôlent pas les communications électroniques émises ou reçues par leurs équipements s'exposent à des poursuites plus ou moins sérieuses. Aux États-Unis, les employeurs doivent par conséquent informer le personnel américain que leurs ordinateurs appartiennent à l'entreprise et sont fournis à titre professionnel, que les

communications sont susceptibles d'être contrôlées à tout moment et que le personnel ne peut prétendre à aucune confidentialité concernant l'utilisation des ordinateurs mis à sa disposition.[36]

En outre, les tribunaux apprécient de plus en plus les systèmes de filtrage qui, selon eux, constituent le moyen de protection le moins restrictif contre les contenus choquants diffusés sur Internet. Le 22 mars 2007 par exemple, un tribunal d'arrondissement de Pennsylvanie a jugé une affaire mettant partiellement en doute le caractère constitutionnel de la loi sur la protection de la vie privée des enfants en ligne (Child Online Protection Act)[37], au motif que les filtres ne constituaient pas un moyen suffisamment restrictif pour empêcher les enfants d'accéder à des contenus choquants sur Internet par rapport aux exigences prescrites par le Congrès.[38] Ce tribunal a déterminé que les filtres « bloquent généralement 95% des documents à caractère sexuel explicite »,[39] que les filtres sont « entièrement personnalisables et peuvent être configurés pour différents âges, différentes catégories de propos et peuvent être désactivés totalement. »[40]

Face au nombre croissant de réglementations, à la multiplication des litiges et à l'augmentation des frais engendrés par des erreurs qui auraient pu être évitées, les entreprises associent à présent technologies et règlements intérieurs pour contrôler la productivité, protéger leurs ressources et inciter le personnel à respecter les règles. Ainsi, au moins 80% des entreprises américaines

Face au nombre croissant de réglementations, à la multiplication des litiges et à l'augmentation des frais engendrés par des erreurs qui auraient pu être évitées, les entreprises associent à présent technologies et règlements intérieurs pour contrôler la productivité, protéger leurs ressources et inciter le personnel à respecter les règles.

[36] *Monitoring Employee E-mail: Efficient Workplaces vs. Employee Privacy*, 2001 DUKE L. & TECH. REV. 0026 (2001).
[37] Titre 47 du Code fédéral des États-Unis d'Amérique.
[38] *ACLU contre Gonzales*, No. 98-5591 (E.D. Pa. 22 mars 2007).
[39] *Idem.*
[40] *Idem.*

informent leurs employés qu'elles analysent les documents consultés, les séquences de touches frappées et le temps passé au clavier ; 76% d'entre elles contrôlent les sites Web consultés par leurs employés ; 65% bloquent l'ouverture de sites Web inappropriés ; 82% indiquent clairement que les fichiers des ordinateurs sont archivés et analysés ; 86% avertissent leurs employés du suivi effectué sur les messageries ; enfin, 89% des sociétés préviennent leur personnel que leur utilisation d'Internet fait l'objet d'un suivi.[41] En 2005, les sociétés américaines déclaraient avoir instauré des règles d'utilisation spécifiques, à proportion de 84% pour les messageries personnelles, de 81% pour Internet, de 42% pour les messageries instantanées personnelles. 34% d'entre elles interdisaient la gestion de sites Web personnels durant les heures de travail, 23% interdisaient la publication de messages personnels sur les blogs de l'entreprise, et 20% des règlements d'entreprise interdisaient la gestion de blogs personnels durant les heures de travail.[42] Au cours de cette même année, 26% des employeurs déclaraient s'être séparés d'employés utilisant Internet de façon inappropriée et 25% d'entre eux indiquaient avoir licencié des employés pour utilisation abusive de la messagerie.[43]

[41] AMA/ePolicy Institute Research, *enquête sur les contrôles et la surveillance électronique (Electronic Monitoring & Surveillance Survey)*, 2005.
[42] *Idem.*
[43] *Idem.*

Protection de la propriété intellectuelle : clé de la réussite de l'entreprise

Le volume des e-mails augmente de 30% chaque année et ces messages renferment la propriété intellectuelle de l'entreprise à hauteur de 80%.

Le volume des e-mails augmente de 30% chaque année et ces messages renferment la propriété intellectuelle de l'entreprise à hauteur de 80%.[44] Le risque de sinistre est tout à fait réel. Dans l'affaire *Sonoco Products contre Johnson,* 23 P.3d 1287 (Co. App. 2001), un procès pour appropriation frauduleuse de secrets commerciaux a permis à la société de récupérer près de 7 millions de dollars en dommages et intérêts. Un ancien employé s'était entendu avec son nouvel employeur en vue d'exploiter des informations électroniques et physiques protégées, préalablement soustraites à Sonoco par l'employé.[45]

Les tribunaux n'ont pas seulement reconnu la responsabilité de l'employé qui avait disparu avec les données électroniques, mais également celle du nouvel employeur. Dans l'affaire *Shurgard Storage contre Safeguard Self-Storage,* 119 F. Supp. 2d 1121 (W.D. Wash. 2000), le plaignant a porté plainte contre le nouvel employeur d'un de ses anciens employés en s'appuyant sur la loi relative aux fraudes informatiques (Computer Fraud and Abuse Act) pour avoir utilisé ses ordinateurs pour envoyer des informations protégées du plaignant à la société défenderesse, qui avait par la suite embauché l'employé en question. Dans l'affaire *Charles Schwab contre Carter,* 2005 U.S. LEXIS 21348, no. 04-C-7071 (N.D. Ill. 27 septembre 2005),

[44] Frank Chambers, *EDD Tips for Email from the Front Line,* LAW TECHNOLOGY TODAY, mars 2007.
[45] *Voir également, Sawyer contre Dept. of Air Force,* MSPB 1986, 31 MSPR 193 ; *US contre Middleton,* 35 F. Supp. 2d 1189 (N.D. Cal. 1999) ; *EF Cultural Travel BV contre Explorica Inc.,* 274 F.3d 577 (1st Cir. 2001) ; *Pacific Aerospace Electronics Inv. contre Taylor,* 295 F. Supp. 2d 1188 (E.D. Wa. 2003).

la Cour a donné raison au plaignant qui avait intenté une action contre le nouvel employeur d'un de ses anciens employés, invoquant une théorie de responsabilité indirecte incluse dans la loi sur les fraudes informatiques (Computer Fraud and Abuse Act). Alors que l'employé travaillait encore pour le plaignant, Schwab, il avait envoyé par e-mail des informations protégées de la société Schwab à son futur employeur, Acorn. Schwab accusait Acorn d'avoir incité son employé à accéder au système informatique de Schwab sans autorisation.

Dans l'affaire *Lowry's Reports contre Legg Mason,* 271 F. Supp. 2d 737 (D. Md. 2003), un employé distribuait et réimprimait des documents protégés par des droits d'auteur sur son lieu de travail. La Cour a considéré comme irrecevable l'hypothèse selon laquelle l'employeur n'avait pas connaissance des agissements de son employé (alors même que l'employeur avait demandé à son employé de cesser la distribution de documents protégés par des droits d'auteur). Le verdict du jury a imposé 20 millions de dollars en dommages et intérêts.[46]

Chacune de ces affaires démontre que si les entreprises/victimes américaines avaient détecté des fuites d'informations protégées, intercepté et filtré les envois de telles informations, elles auraient pu non seulement s'épargner des années de procédures, mais également la perte de données confidentielles. En définitive, les données confidentielles ne sont jamais vraiment récupérées, avec ou sans victoire en procès.

[46] La requête en appel du jugement sur des questions légales a été rejetée au cours de l'affaire *Lowry's Reports, Inc. contre Legg Mason, Inc.*, 302 F. Supp. 2d 455, 461 (D. Md. 2004).

Confidentialité : quand le surplus d'informations devient un handicap [47]

Contrairement aux pays de l'Union européenne (UE) et à d'autres régions du monde, les États-Unis n'abordent pas la question de la protection de la vie privée de manière globale. Leur approche tend à résoudre les problèmes de confidentialité des données par secteur d'activité en adoptant des lois distinctes concernant l'accès aux données d'ordre personnel, leur création, leur stockage et leur utilisation. Parallèlement au FRCP qui traite de la conservation des informations, aux règles de contrôle qui permettent d'éviter l'installation d'un environnement de travail hostile, ou au Computer Fraud and Abuse Act qui régit les fraudes informatiques, les lois de protection de la vie privée imposent des limites aux entreprises concernant la collecte, le traitement, la conservation, l'utilisation et la diffusion de données d'ordre personnel. Il est donc important que les systèmes de gestion des données informatiques soient suffisamment efficaces pour conserver et archiver les données si nécessaire, pour instaurer des contrôles (aux États-Unis, lorsque cela est autorisé) et pour restreindre l'utilisation et l'accès aux données d'ordre privé que les entreprises exploitent dans un cadre précis et limité.

La loi Gramm-Leach-Bliley, par exemple, concerne les institutions financières, notamment les banques, sociétés d'assurances, de bourse, de conseil financier et d'investissement. Elle fournit un cadre de protection

[47] Pour plus d'informations sur la confidentialité des données privées, pas seulement aux États-Unis, consultez le manuel Baker & McKenzie sur la confidentialité : *Global Privacy Handbook* (International Association of Privacy Professionals) ©2006.

La loi HIPAA réglemente la collecte, l'utilisation et l'accès aux données relatives à la santé pour les institutions concernées, à savoir les organismes de prise en charge, les organismes de gestion des remboursements et les professionnels de la santé qui transmettent des informations médicales.

de la vie privée contre la vente d'informations financières personnelles, contre le « pretexting », une technique qui consiste à se faire passer pour quelqu'un d'autre afin de soutirer des informations financières privées à des fins d'escroquerie. Cette loi donne au consommateur le droit de refuser le partage, même limité, « d'informations personnelles privées ». Elle exige également des institutions financières qu'elles utilisent des programmes de sécurisation des informations respectant certains critères déterminés par les autorités compétentes, telles que les normes de protection des informations client (Standards for Safeguarding Customer Information) élaborées par la commission fédérale du commerce (Federal Trade Commission).

La loi sur le reporting financier (Fair Credit Reporting Act), en plus de nombreuses autres lois nationales similaires, régit principalement l'utilisation et la divulgation d'informations dans des « rapports sur les consommateurs » et des « agences de renseignements sur les consommateurs », termes qui sont définis de manière très large. Cette loi comprend des restrictions sur la collecte, l'utilisation et la divulgation de procédures médicales, financières et judiciaires, ainsi que des limitations spécifiques concernant l'usurpation d'identité, les rapports sur les consommateurs dans le cadre des processus d'embauche et les « rapports d'investigation sur les consommateurs » impliquant des tiers. Cette loi pose de nombreuses obligations aux agences de renseignement sur les consommateurs et aux utilisateurs de rapports sur les consommateurs,

afin de préserver l'intégrité et l'exactitude des données recueillies et transmises. Cette loi réglemente en outre l'accès aux informations par Internet, l'utilisation et le stockage sécurisé des données tirées de rapports sur les consommateurs.

La loi sur la transférabilité et la responsabilité dans le cadre de l'assurance-maladie (Health Insurance Portability and Accountability Act, HIPAA) réglemente la collecte, l'utilisation et l'accès aux données relatives à la santé pour les institutions concernées, à savoir les organismes de prise en charge, les organismes de gestion des remboursements et les professionnels de la santé qui transmettent des informations médicales. Les lois HIPAA régissent entre autres l'utilisation et la divulgation de données médicales protégées, quel que soit leur format de stockage. Les entités concernées doivent nommer un régisseur des données, responsable de la mise en œuvre des règles et pratiques requises par ces lois et d'organiser la conservation des dossiers sur une durée de six ans. Ces entités doivent en outre se conformer aux normes de sécurité pour la protection des informations médicales électroniques protégées (Security Standards for the Protection of Electronic Protected Health Information, 45 CFR 160 et 164). En janvier 2007, le ministère américain de la justice a annoncé une première affaire tombant sous le coup de la loi HIPAA, dans le cadre de poursuites pour vol de dossiers médicaux électroniques concernant 1 130 patients de la clinique de Cleveland. Un employé de la clinique aurait utilisé le système

Les lois HIPAA régissent entre autres l'utilisation et la divulgation de données médicales protégées, quel que soit leur format de stockage.

informatique de l'établissement pour détourner et vendre des dossiers médicaux à une organisation criminelle qui s'en serait ensuite servi pour dérober 7 millions de dollars à l'assurance-maladie Medicare. Plusieurs États réglementent le contrôle des données d'assurance-maladie, notamment la Californie avec la loi sur la confidentialité des informations médicales (Confidentiality of Medical Information Act).[48]

De nombreux États ont également édicté des lois visant à protéger la confidentialité des numéros de sécurité sociale. Par exemple, la section 1798.85 du code civil californien interdit, entre autres, de demander à une personne de transmettre son numéro de sécurité sociale par Internet, à moins que la connexion soit sécurisée ou que le numéro de sécurité sociale soit crypté. La section 1798.81.5 du code civil californien oblige les entreprises à instaurer des procédures de sécurité suffisantes pour protéger toute une catégorie d'informations personnelles, notamment les numéros de sécurité sociale, de carte de paiement, de compte bancaire, de permis de conduire, etc. L'État de New York a voté une loi similaire réglementant la destruction de documents contenant des informations personnelles, telles que les numéros de sécurité sociale.[49]

Les entreprises doivent choisir avec soin leurs systèmes de gestion des données électroniques afin de pouvoir s'adapter au nombre croissant de lois sur la protection des données d'ordre privé. Les secteurs

[48] Selon une récente enquête, 98,5% des personnes interrogées indiquent que les organismes médicaux sont responsables de la sécurité des dossiers médicaux de leurs patients, moins de 40% d'entre elles sont convaincues que les professionnels de santé sécurisent leur dossier médical. Pratiquement tous les participants pensent que les organismes médicaux sont légalement tenus d'avertir leurs patients si des dossiers médicaux sont consultés sans l'accord du patient. Toutefois, 7 participants sur 10 estiment que les professionnels de santé n'informent pas les patients des éventuelles infractions aux règles de sécurité. www.epictide.com.
[49] NY CLS Gen. Bus. §399-h (2007).

médical et bancaire doivent tous deux mettre en place des fonctionnalités de cryptage afin de garantir que les informations confidentielles, qu'elles soient médicales ou financières, ne soient pas divulguées involontairement. Des pare-feu et des restrictions d'accès doivent être installés afin de prévenir toute diffusion non autorisée ou abusive. Des moyens de contrôle doivent exister afin que toute infraction aux règles de sécurité puisse être détectée et que des mesures appropriées soient immédiatement prises. Non seulement les infractions aux lois fédérales et nationales en matière de confidentialité des données privées sont passibles de sanctions pénales, mais elles nuisent également à l'activité des entreprises et ternissent leur image de marque. Là encore, le dicton « mieux vaut prévenir que guérir » se vérifie.

Non seulement les infractions aux lois fédérales et nationales en matière de confidentialité des données privées sont passibles de sanctions pénales, mais elles nuisent aussi à l'activité des entreprises et ternissent leur image de marque. Là encore, le dicton « mieux vaut prévenir que guérir » se vérifie.

Cryptage

Le cryptage est une technologie essentielle, qui n'est malheureusement pas suffisamment utilisée. « Le cryptage des données se définit comme le procédé qui consiste à brouiller les informations transmises ou stockées afin de les rendre inintelligibles jusqu'à leur décryptage par le destinataire de ces informations. »[50] Il est primordial de protéger les secrets commerciaux et les informations confidentielles communiquées via Internet.

Les sociétés qui n'utilisent pas de fonction de cryptage, livrent leurs secrets au public. « Dans le domaine de la sécurité, l'année 2005 restera celle qui a porté les pertes de données au premier rang des préoccupations, le tout renforcé par les lois américaines ordonnant la déclaration publique des vols ou pertes de données relatives à des clients. »[51] Le plus effrayant étant que des employés disposant d'un accès aux données confidentielles de leur employeur ne tiennent aucunement compte de la sécurité des données et ne connaissent rien de son fonctionnement. Dans leur article de référence intitulé « Pourquoi Johnny ne parvient-il pas à crypter ? » (Why Johnny Can't Encrypt),[52] deux chercheurs de l'université Carnegie Mellon ont indiqué que l'utilisateur moyen des messageries, bien que familier de cet outil et possédant un niveau de formation élevé, ne savait pas comment utiliser la fonction de cryptage. L'étude suivante, intitulée

[50] Fred Moore, *Preparing for Encryption: New Threats, Legal Requirements Boost Need for Encrypted Data,* COMPUTER TECHNOLOGY REVIEW, août-septembre 2005.
[51] Kevin Murphy, *Email Security Uncovered,* COMPUTER BUSINESS REVIEW ONLINE, 1er novembre 2005 (citation d'Alex Hernandez, responsable du développement de produits avancés chez CipherTrust).
[52] Alma Whitten & J.D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0,* disponible à l'adresse : http://www.gaudior.net/alma/johnny.pdf.

Les pirates savent que la majorité des entreprises moyennes investissent peu dans la sécurité et le cryptage. On estime à 4 000 le nombre des entreprises moyennes particulièrement exposées à ces attaques, si elles ne prennent pas rapidement des mesures de protection adéquates.

Johnny n'arrive toujours pas à crypter (Why Johnny Still Can't Encrypt),[53] a toutefois montré quelques améliorations dans ce domaine. Les entreprises doivent donc prendre toutes les mesures nécessaires pour adopter des systèmes de cryptage conviviaux et compatibles avec leurs exigences en termes de sécurité, puis former leur personnel à l'utilisation de ces technologies.

En stockant leurs données dans des systèmes non cryptés, les sociétés s'exposent à des vols d'informations client par des pirates informatiques. Cela risque de nuire à leur réputation auprès du public et de la clientèle, et de déclencher des procédures judiciaires coûteuses. Ainsi, la société TJX Companies, qui comprend les enseignes T.J. Maxx, Marshalls, Home Goods, Bob's Stores et d'autres chaînes de magasins, a annoncé en janvier 2007 que ses systèmes informatiques avaient été piratés entre 2005 et 2006. Durant cette période, les vols s'étaient portés sur les informations de 45,7 millions de cartes de paiement utilisées entre 2002 et 2004, et comprenaient les noms des personnes ainsi que leurs numéros de carte de crédit et de débit.[54] En mars 2007, Radioshack a constaté qu'elle avait jeté 20 cartons de disques contenant des reçus sur lesquels figuraient des numéros de carte de paiement de clients. L'avocat général du Texas avait alors initié une exécution forcée. En mars 2007 également, la société Group Heath Cooperative Healthcare System, a perdu deux ordinateurs portables contenant les noms, adresses, numéros de sécurité sociale et identifiants de patients et d'employés.

[53] Steve Sheng et autres, *Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software*, disponible à l'adresse : http://cups.cs.cmu.edu/soups/2006/posters/sheng-poster_abstract.pdf.
[54] TJX, Frequently Asked Questions, www.tjx.com/tjx_faq.htm.

Chacun de ces incidents aurait pu être évité par le biais du cryptage. Les entreprises moyennes sont particulièrement vulnérables à ce type d'attaque. En effet, les pirates informatiques ne cherchent plus simplement à devenir célèbres lorsqu'ils lancent un virus au niveau international. Ils cherchent à gagner de l'argent et savent que la majorité des entreprises moyennes investissent peu dans la sécurité et le cryptage. On estime à plus de 4 000 le nombre des entreprises moyennes particulièrement exposées à ces attaques, si elles ne prennent pas rapidement des mesures de protection adéquates.[55]

Comme indiqué précédemment, le cryptage est considéré comme un acte positif de prévention contre la publication accidentelle d'informations d'ordre privé, au moins selon la loi californienne sur la confidentialité du numéro de sécurité sociale (Confidentiality of Social Security Number Act).[56] Les sous-traitants de l'État ont eux aussi des normes de cryptage spécifiques à respecter qui sont liées aux exigences des services de renseignement.[57] Enfin, la nécessité de crypter apparaît évidente lorsque l'on souhaite éviter toute divulgation involontaire d'informations protégées. Les services informatique et juridique doivent donc déterminer ensemble les besoins de leur entreprise en matière de cryptage et savoir si le système en place protège suffisamment leur société en cas de piratage, de vol ou dans l'éventualité d'un procès.

[55] Allan Holmes, *De nombreuses entreprises moyennes disent ne pas avoir de temps, d'argent ni de ressources à consacrer à la sécurité. Cela explique peut-être qu'elles soient les cibles d'attaques et que le secteur des entreprises moyennes ait mauvaise réputation,* CIO, 1er mars 2007.
[56] CAL. CIV. CODE §1798.29 (la section évoquée est également connue sous l'identifiant SB 1386).
[57] National Institute of Standards and Technology (NIST), Data Encryption Standard Fact Sheet, disponible à l'adresse : http://csrc.nist.gov/cryptval/des/des.txt.





Questions internationales : quand différentes conceptions de la conformité se rencontrent

Pour les sociétés qui opèrent à l'international, il est donc essentiel d'intégrer les réglementations locales et internationales applicables aux données électroniques.

Les règles de collecte, de traitement, de conservation, d'utilisation, de contrôle, d'accès et de suppression des données peuvent non seulement différer selon les juridictions en dehors des États-Unis, mais dans certains cas, elles sont également en opposition complète avec les lois américaines. Pour les sociétés qui opèrent à l'international, il est donc essentiel d'intégrer les réglementations locales et internationales applicables aux données électroniques.

Dans l'Union européenne par exemple, chaque pays a mis en œuvre, conformément à la directive sur la protection de la vie privée, des lois régissant la collecte, l'enregistrement, l'organisation, le stockage, l'adaptation, l'altération, l'extraction, le blocage, le contrôle, l'utilisation, la divulgation, la transmission, le transfert et la destruction des « informations d'identification personnelle », et le cas échéant, des protections supplémentaires pour les « informations d'identification personnelle sensibles ». Contrairement aux États-Unis, l'Union européenne utilise une définition très large des « informations d'identification personnelle », qui n'est pas spécifique à un secteur d'activité particulier. Cette définition vise à prévenir le traitement ou la transmission de telles informations sans autorisation. Ces dernières peuvent inclure le nom, l'adresse, l'indemnisation, les revenus et des

Les entreprises doivent non seulement comprendre quels types de données elles sont en droit de recueillir, de traiter et de transmettre au niveau international, mais elles doivent également jongler avec des législations parfois contradictoires.

informations financières, ainsi que des données plus « sensibles » sur l'état de santé, l'origine ethnique, l'orientation politique, l'appartenance à un syndicat ou la situation familiale. Ces lois ne s'appliquent pas seulement aux employés, mais aussi aux consommateurs. L'Italie, l'Autriche et certains autres pays ont également étendu la notion de protection de la vie privée aux sociétés.

L'Union européenne n'ayant pas considéré la législation américaine comme suffisamment stricte, ce type d'information ne peut pas circuler légalement vers les États-Unis ou vers d'autres pays à la législation souple en la matière, que ce soit électroniquement ou par d'autres moyens, à moins que certaines mesures de sécurité aient été prises, telles que la signature de l'accord américano-européen sur la protection de la sphère privée (Safe Harbor Agreement), l'adoption des clauses type de l'Union européenne ou la mise en œuvre de règles de protection de la vie privée approuvées. Toutefois, l'utilisation de telles protections pour effectuer des transferts de données d'identification personnelle vers les États-Unis ne permet pas de réaliser d'autres transferts de ces données vers des sociétés tierces de traitement non identifiées ou vers d'autres pays, par exemple vers des services de saisie de données situés en Inde. L'Union européenne n'est pas la seule à procéder ainsi : le Canada, l'Argentine, le Japon, l'Australie et bien d'autres pays adoptent également des lois de protection de la vie privée plus ou moins strictes.

Ainsi, les entreprises doivent non seulement comprendre quels types de données elles sont en droit de recueillir, de traiter et de transmettre au

niveau international, mais elles doivent également jongler avec des législations parfois contradictoires. Par exemple, la loi Sarbanes-Oxley exige des sociétés cotées en bourse qu'elles mettent en place un service téléphonique anonyme permettant de dénoncer les éventuels cas d'infraction financière et de sécurité. Le service téléphonique anonyme prévu par cette loi permet aux employés de ne pas divulguer leur identité et donc de témoigner sans craindre des représailles. L'UE, en revanche, désapprouve en général les services téléphoniques anonymes, qu'elle assimile à une transgression du droit à la vie privée et elle restreint par conséquent le recours à ce type de procédés. Ainsi, les points de vue divergent entre la loi Sarbanes-Oxley et l'Union européenne sur la protection de la vie privée et cela pose un problème évident pour les entreprises multinationales faisant appel public à l'épargne. Elles doivent en effet déployer un système de gestion des données sophistiqué pour garantir, entre autres, que la conservation et l'accès aux données sont restreints, et que leur extraction est sécurisée, tout en respectant les exigences de la loi américaine Sarbanes-Oxley.[58]

D'autres pratiques recommandées aux États-Unis ne sont pas transposables au niveau international. Par exemple, la Cour de cassation française à considéré comme abusif, anticonstitutionnel et constitutif d'un crime, le fait qu'une entreprise française ait licencié un employé après avoir appris, en contrôlant les ordinateurs de la société, que ce dernier avait envoyé des messages électroniques contenant des informations confidentielles à un

[58] Pour plus d'informations sur les abus relatifs aux codes de conduite et l'utilisation abusive des services téléphoniques anonymes de dénonciation, consultez l'article « *Overreaching Global Codes of Conduct Can Violate the Law* », par Cynthia L. Jackson, LA and SF Daily Journal, 7 juin 2006.

concurrent potentiel. Cette Cour française a estimé que l'employé disposait d'un droit constitutionnel à la confidentialité pendant ses heures et sur son lieu de travail, même si son employeur avait interdit l'utilisation des ordinateurs de la société à titre personnel. La jurisprudence allemande est un peu moins dure, mais elle restreint également les contrôles sur les ordinateurs utilisés par les employés, lorsque l'employeur autorise ces derniers à utiliser le système de la société pour leur usage personnel. De nombreuses juridictions européennes exigent, au minimum, l'approbation de toute opération de contrôle des employés par les autorités locales compétentes.

Les entreprises doivent donc impérativement tenir compte de leurs obligations légales au niveau local en termes de collecte, d'utilisation et d'accès aux données, afin de sélectionner un système adéquat pour assurer la gestion de leurs données électroniques. Pour les entreprises multinationales qui recueillent des informations dans diverses juridictions, ou transfèrent des informations entre juridictions, il est primordial de respecter toutes les lois relatives à la confidentialité en installant des pare-feu et des restrictions d'accès adaptés sur tous les systèmes impliqués, afin de garantir que le traitement, le contrôle ou le transfert de ces informations s'effectue en toute légalité.

Conseils relatifs aux meilleures pratiques

1. **Prévoir.** N'attendez pas un procès, l'installation d'une ambiance de travail hostile, la divulgation d'un secret commercial ou la perte d'informations confidentielles pour organiser la gestion de vos données.

2. **Connaître ses obligations légales.** Analysez les obligations légales imposées par le secteur d'activité et les juridictions dans lesquelles votre entreprise opère. Par exemple, quelles sont les règles à appliquer en matière de conservation des divers types d'informations dans un pays ou une région donnée ? Quelles mesures de sécurité restreignent l'accès ou la conservation des données ? Quels éléments doivent être cryptés et quelles sont vos obligations en ce qui concerne la notification des éventuels incidents de sécurité ? L'application de filtres pour éviter la création de conditions de travail hostiles est-elle recommandée ou considérée comme une intrusion dans la vie privée ?

3. **Savoir s'adapter à son milieu.** Envisagez l'aspect parfois contradictoire des règles que votre système de gestion des données électroniques devra respecter dans le cadre de votre activité au niveau national ou international. Installez des pare-feu, des restrictions d'accès et désactivez les fonctionnalités que certaines juridictions ne permettent pas d'utiliser, telles que le contrôle et le filtrage.

4. **Affecter du personnel à la gestion du système.** Chargez des employés de l'entretien et de la gestion des données électroniques. Cette équipe peut regrouper des employés des services

informatique et juridique, avec des interventions ponctuelles des ressources humaines et d'autres services. Attribuez certaines responsabilités à des personnes qui devront actionner les systèmes en cas d'incident d'ordre légal.

5. **Identifier les divers types de données et de systèmes de stockage.** N'oubliez pas que les données peuvent être stockées sur un ordinateur de bureau, un assistant personnel, des ordinateurs personnels, des ordinateurs portables et à d'autres emplacements. Avant de pouvoir gérer les données susceptibles d'engager la responsabilité légale de l'entreprise, vous devez tout d'abord connaître leur forme et leur emplacement afin de vous assurer que le système adopté sera en mesure de récupérer les données pertinentes. Sachez également quelles méta-données sont en votre possession.

6. **Choisir un système souple pour assurer la gestion de vos données électroniques.** Choisissez un système suffisamment flexible pour répondre à vos besoins en termes de conservation, d'archivage, de contrôle, de filtrage et de cryptage, selon les juridictions dans lesquelles vous développez vos activités. Votre système devra être « convivial« afin que votre personnel ne s'emploie pas à le contourner. Choisissez un système capable d'évoluer en fonction des changements au niveau législatif. Prévoyez l'augmentation du volume de données et de méta-données.

7. **Ne pas devenir paperassier.** Si les nouvelles technologies vous autorisent à stocker

d'importants volumes de données, cela n'est pas toujours indispensable. Le stockage de données inutiles ne facilite pas la récupération des informations et peut accroître le risque de piratage. Par exemple, ne conservez pas les informations financières de vos clients, à moins que cela soit nécessaire. Si tel est votre cas, cryptez ces informations.

8. **Instaurer des règles.** Définissez des règles claires et précises, conformes à la législation applicable, afin d'organiser la conservation des documents. Commencez à stocker vos documents à titre conservatoire bien à l'avance, en prévision d'un éventuel litige. Aux États-Unis, exposez clairement votre politique en matière de contrôle des messageries électroniques des employés. Adoptez des règles de cryptage pour les informations confidentielles afin de prévenir toute divulgation accidentelle. Lorsque cela est autorisé, définissez des procédures disciplinaires susceptibles de dissuader votre personnel et appliquez-les.

9. **Se préparer.** N'attendez pas qu'un litige (encore moins un procès) intervienne pour mettre en place des procédures de stockage à titre conservatoire. Définissez dès à présent les procédures qui permettront de modifier les processus de destruction des documents, afin que le stockage à titre conservatoire puisse être déclenché rapidement, le cas échéant. Faites vos devoirs avant la procédure judiciaire des rencontres préliminaires qui permettent d'organiser la présentation de documents électroniques. Les parties qui savent quels éléments sont en leur possession et pourquoi,

sont mieux placées pour négocier des conditions favorables. N'attendez pas une infraction pour mettre en œuvre des processus permettant de détecter et de signaler rapidement tout problème lié à la sécurité.

10. **Former et évaluer, puis former et évaluer de nouveau.** Votre règlement et votre système de gestion des données fonctionneront uniquement si vos employés savent comment s'en servir. Cela implique une mise en œuvre et un suivi scrupuleux et pertinents. L'acquisition d'un système de gestion des données ne représente qu'une première étape vers la conformité. L'évolution des données, technologies, législations, risques et employés nécessite des adaptations, des formations et des évaluations permanentes.













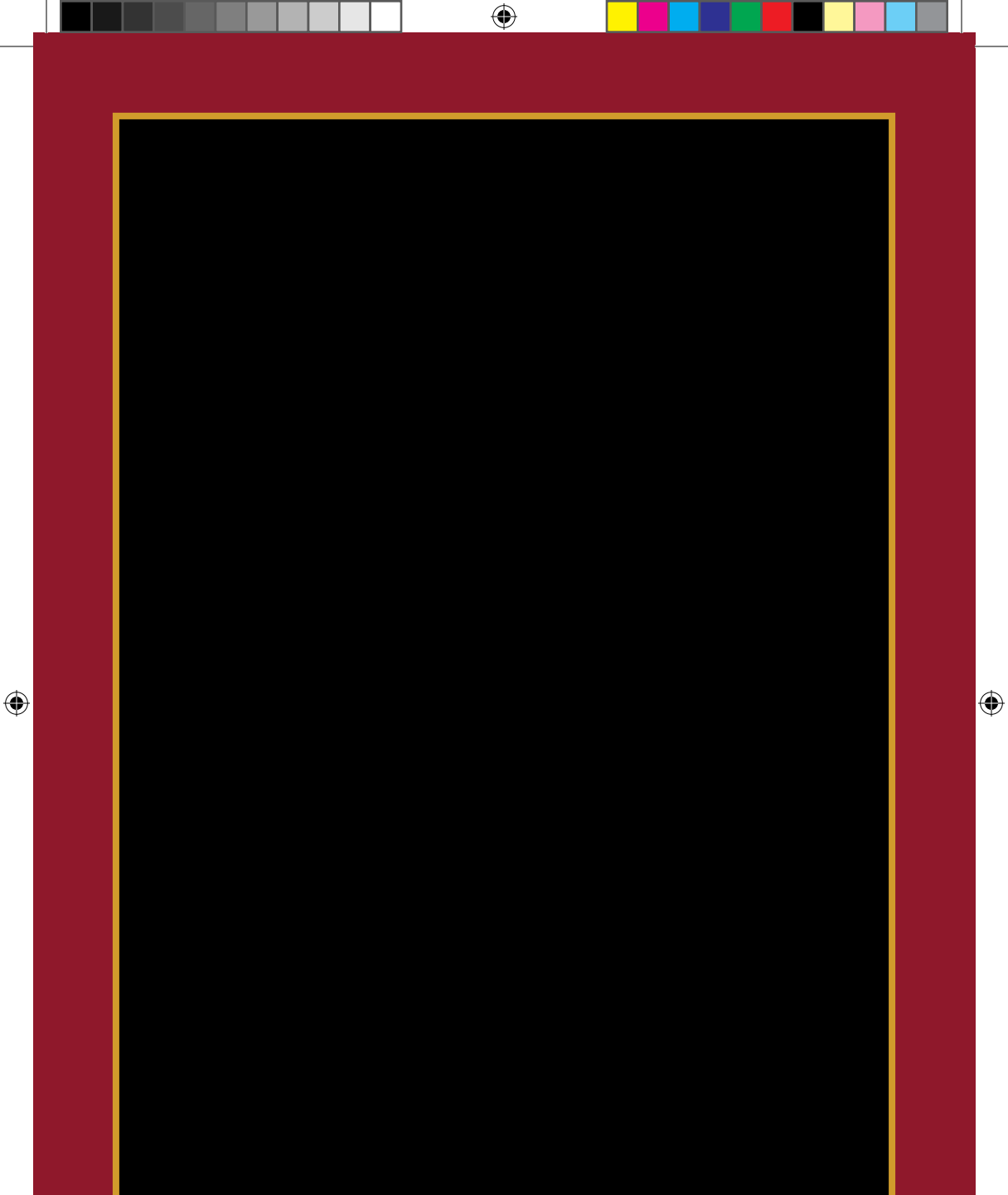

WP33-0705

postini