

Le vol d'identité et la fraude électronique sont les principales menaces de la dématérialisation des moyens de paiement.

Maîtriser les risques des transactions électroniques

par Linda Ducret

En temps de crise, plus que jamais la dématérialisation des documents comptables et achats doit permettre de réduire les coûts, de gagner en efficacité... La dématérialisation des moyens de paiement s'est également intensifiée en même temps que les risques liés à ce type de transaction électronique. Heureusement, diverses contre-mesures permettent de lutter contre la fraude et la cybercriminalité !

Markess International, société d'études et de conseil, a présenté les chiffres du marché extraits de son étude publiée en septembre 2008, consacrée à la dématérialisation des factures, parue récemment et intitulée : «Bénéfices & Gains de la Dématérialisation de Factures». Ainsi, cette société a évalué le marché autour des projets de dématérialisation de factures, quelle qu'en soit la forme, à 385 millions d'euros en 2008 (les deux tiers de ce marché - soit 255 millions d'euros - étant consacrés à l'ensemble des prestations de services associées à la dématérialisation de factures). Markess International en conclut que le marché de la dématérialisation des factures devrait être moins touché que d'autres marchés du secteur des technologies de l'information et de la communication par la conjoncture économique actuelle, les gains financiers tangibles qui y sont associés étant plus particulièrement recherchés par les entreprises en temps de crise. Ces chiffres, même s'ils ne représentent qu'une face de la dématérialisation (les factures), montrent à quel point la dématérialisation est l'une des préoccupations majeures des directions financières du moment. Car la dématérialisation des documents comptables, achats et administratifs (factures, commandes...) est devenue aujourd'hui une réalité pour les entreprises qui ne peut plus être occultée. En effet, cette dématérialisation concerne tous les documents et processus de l'entreprise : factures, données comptables, courriers, déclarations sociales. Réduction des coûts, rationalisation des processus achats et comptables, optimisation du service client... tels sont quelques uns des avantages de cette dématérialisation.

Comment protéger les données de l'entreprise ? Quels sont les enjeux juridiques et fiscaux, orga-



photo Anna Guessele

nisationnels de la dématérialisation des documents comptables ? Quels sont les services en ligne de dématérialisation ? Les solutions d'authentification forte ? Nous répondrons à ces questions et nous présenterons la Loi sur les comptabilités informatisées, les solutions dédiées au traitement automatisé des factures. Concernant les risques liés à la dématérialisation des moyens de paiement (fraude électronique, cybercriminalité...), nous vous donnerons quelques solutions afin de gérer ces risques.

Comment protéger les données de l'entreprise ?

La gestion des coûts et de la complexité liés à la protection des données est l'une des priorités

des responsables informatiques. En effet, de nouveaux risques sont apparus tels que le piratage, l'usurpation d'identité et la fraude en entreprise. Les entreprises commencent à prendre conscience de l'importance de la mise en place d'une véritable politique de sécurisation des données. En effet, si une entreprise ne prend pas les mesures qui s'imposent pour protéger les données électroniques, les conséquences peuvent être désastreuses en termes de divulgation de renseignements confidentiels, d'atteinte à son image de marque... De nouvelles pistes de réflexion sur la protection des données sont apparues dans les entreprises : auditer la nature des documents transmis (de nature contractuelle, officielle, documents de savoir ou de gestion interne à l'organisation), définir des

durées de vie sur les documents, associer des droits d'usage spécifiques pour des groupes d'utilisateurs différents. Bien entendu, il est crucial de protéger la sécurité et la confidentialité des documents inter-entreprises (format PDF). Cependant, il n'y a pas de solution préétablie contre ces nouveaux risques liés à Internet et le dirigeant devra construire sa propre politique de sécurité.

La dématérialisation des factures et documents comptables, un levier pour améliorer les processus comptables, achats, administratifs de votre entreprise

Selon l'étude Ernst & Young, «Le BFR, un réel enjeu pour l'entreprise : de l'émergence à la performance de la cash generation» menée en 2007 auprès de 180 entreprises, 67 % d'entre elles ont ou vont mettre en œuvre un projet de dématérialisation avec pour objectif principal d'améliorer le besoin en fonds de roulement. Ainsi, un projet de dématérialisation va bien au-delà des considérations économiques et informatiques, il doit en principe aller jusqu'à être un levier d'optimisation en termes d'organisation, de pilotage des coûts et d'amélioration de la productivité. Réduction des coûts, apport de productivité et de valeur ajoutée à la fonction comptable (suppression des tâches de saisie), traçabilité et contrôle accrus des informations financières, réduction des délais de traitement et validation des documents comptables, amélioration des relations fournisseurs... tels sont les nombreux avantages recensés par les directeurs financiers. Sans compter la vitesse et la qualité de traitement des documents comptables, gages de diminution des réclamations et des litiges.

Quels sont les enjeux juridiques et fiscaux (Loi sur les comptabilités informatisées) de la dématérialisation des factures et documents comptables ?

Les textes fondateurs des vérifications des comptabilités informatisées sont peu nombreux. Il s'agit des articles L13, L47A, L57 ; L74 et L102B du LPF issus de la Loi de finances ►►

Gestion des flux

La politique de la sécurité du commerce électronique peut également s'appuyer sur la signature électronique.

La loi 2000-230 du 13 mars 2000 précise que toutes les signatures électroniques sont recevables en justice dès lors qu'elles assurent, à l'aide d'un procédé fiable, l'identification du signataire et l'intégrité de l'acte. Le décret 2001-272 du 30 mars 2001 décrit les conditions de fiabilité du procédé de signature électronique.

Si ces conditions ne sont pas remplies, il est nécessaire en cas de contestation de prouver la fiabilité du procédé de signature électronique utilisé. Enfin, la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique prévoit les modalités de développement de la signature électronique et du chiffrement (protection contre l'espionnage électronique) : http://www.finances.gouv.fr/commerce_electronique/10mesures/securite.htm

Source: Sylvie Mary, l'EDI, l'échange des données informatisées, www.cerpeg.ac-versailles.fr

►► pour 1990 du 29 décembre 1989, étant précisé que l'article L47A du LPF a été modifié par la Loi de finances rectificative pour 2007. Les obligations attachées à la tenue d'une comptabilité informatisée sont celles de présentation et de conservation.

S'agissant de l'obligation de présentation, l'entreprise doit mettre à la disposition de l'Administration fiscale une documentation à jour et exhaustive permettant au vérificateur de connaître et de comprendre le système informatique utilisé (cf : instruction du 24 janvier 2006 BOI 13 L-1-06). S'agissant de l'obligation de conservation des données informatiques, le contribuable doit conserver ces données pendant en principe six ans. Ainsi, un soin particulier doit être apporté à la conservation dès leur constitution des fichiers historiques des mouvements (commandes, livraisons, mouvements de stocks, factures...).

Quelles sont les modalités de contrôle de l'administration fiscale en matière de comptabilité informatisée ? «Lorsque la réalisation du contrôle nécessite la mise en œuvre de traitements informatiques, le vérificateur doit indiquer par écrit la nature des travaux à réaliser et leur délai de réalisation en tenant compte des contraintes de l'entreprise. Sur la base de ces indications, l'entreprise peut demander au vérificateur d'opérer le traitement informatique directement depuis le matériel mis à disposition par l'entreprise ou lui proposer d'effectuer elle-même tout ou partie des traitements informatiques nécessaires à la vérification ou encore lui fournir une copie des fichiers informatiques nécessaires à sa vérification qu'il n'aura pas le droit de reproduire et qu'il sera tenu de restituer avant la mise en recouvrement», indique Régis Bernard, avocat associé du cabinet Kahn & Associés.

Quels sont les services en ligne de dématérialisation ?

Il existe de nombreux prestataires de services en ligne de dématérialisation des factures. Les avantages de ce type de service sont leur souplesse d'utilisation par rapport à un déploiement interne qui serait plus lourd à gérer. Avant de choisir un prestataire, nous vous recommandons d'une part, de vérifier la conformité du système proposé aux différentes législations en vigueur en matière de dématérialisation et d'autre part, de vérifier la capacité d'intégration aux applications comptables de l'entreprise.

Quelles sont les solutions d'authentification forte ?

D'abord, une définition. L'authentification forte consiste à ajouter au traditionnel système de login/mot de passe, une solution annexe supplémentaire qui peut être un code supplémentaire généré aléatoirement pour une courte durée, un algorithme de cryptage, des certificats ou un système de signature électronique. Avant de choisir un prestataire, sachez que plusieurs solutions existent notamment le principe de calculatrice, qui se présente sous la forme d'une petite calculatrice et génère un code automatique à durée de vie limitée, la clé USB, capable de stocker des mots de passe cryptés ou de gérer les certificats électroniques d'accès aux documents et enfin les cartes à puce.

Quels sont les enjeux et impacts de la sécurisation des transactions électroniques ?

Le marché mondial de la sécurité des systèmes d'information est estimé à 50 milliards d'euros. Il est en croissance forte d'environ 15 % par an. Car les enjeux de la sécurisation des transactions électroniques sont de taille : protection des intérêts supérieurs de l'Etat et des intérêts commerciaux des entreprises, développement du commerce et des échanges électroniques et protection de la vie privée. Le cadre législatif de la sécurisation des transactions électroniques et des contenus a un impact important sur ce domaine. Une précision : ce cadre a été élaboré pour l'essentiel au niveau européen. Ainsi, concernant les moyens de paiement, la proposition de directive a pour objectif la création d'ici 2012 d'un espace de paiement en euros (SEPA). Ces moyens de paiement sont le virement, le prélèvement et la carte interbancaire (dont les paiements se font par des virements de banque à banque). Les autres moyens de paiement français subsisteront : chèque, TIP, lettre de change et billets à ordre et cartes privatives (Finaref, Cofidis...)

Quelles sont les menaces de la dématérialisation des moyens de paiement ?

Le vol d'identité et la fraude électronique sont les principales menaces de la dématérialisation des moyens de paiement. Ces délits ne connaissent

pas de frontière et sont le fait de professionnels bénéficiant de vastes ressources financières ainsi que de réseaux bien établis et liés au crime organisé. Le problème que pose cette dématérialisation est celui d'une sécurisation maximale face à ces nombreuses menaces. C'est ainsi que les partenaires de l'e-commerce notamment les banques, les clients, les cybercommerçants sont soucieux de protéger les échanges dématérialisés avec une panoplie ciblée.

Comment gérer les risques liés au paiement ?

Gérer les risques liés au paiement implique de savoir d'abord identifier ces risques, de les hiérarchiser et de savoir les contrôler. Différentes étapes sont nécessaires mais l'une des plus importantes est la sécurisation de l'environnement du commerce électronique. En effet, l'utilisation d'Internet comme canal de commerce a entraîné une forte augmentation des fraudes et des manipulations des marchés (apparition de sociétés offshore pour le commerce de valeurs mobilières on line). En outre, l'utilisation de systèmes de chiffrement sophistiqués qui permettent d'assurer la sécurité des transactions entraîne également l'action des services de répression. «Les nouvelles technologies rendent impossible d'identifier les utilisateurs, augmentent le manque de transparence des transactions effectuées et rendent difficile voire impossible de conserver une trace comptable des transactions ou de signaler celles qui sont suspectes. Une aubaine pour le blanchiment d'argent», explique Sophie-Laurence Roy-Clémendot, avocate associée du Cabinet RCS & Associés. La législation européenne (directive 2001 : 97/CE du 4 décembre 2001) et française (Loi n° 2004-130 du 11 février 2004) imposent des règles de vigilance aux professionnels. Cependant, poursuit Sophie-Laurence Roy-Clémendot, «Internet n'a pas seulement des applications à l'échelon européen, Internet est par définition un réseau mondial, il va donc falloir trouver de nouvelles techniques en droit, en informatique afin qu'Internet ne soit plus l'autoroute du blanchiment». En matière de transactions électroniques, la connaissance des risques et la mise en place de systèmes sécurisés est la base essentielle de la confiance et du développement de l'e-commerce. La confiance des clients, mais aussi celle des partenaires bancaires chargés des transactions et celle de tout l'environnement d'hébergement

assurant la sécurité. «L'ensemble de ces acteurs constitue à différents titres des co-contractants de l'entreprise qui ne doit pas, comme c'est souvent le cas, considérer que tout contrat en la matière constitue une formalité inutile ou un contrat d'adhésion intouchable. Il faut savoir que 90 % des contrats pratiqués en l'occurrence sont des recopies ou des découpages de contrats copiés-collés sur le site d'un concurrent et n'ayant en définitive qu'une vague application à la matière concernée», soutient Jean-Louis Lasserri, avocat associé du cabinet LSK & Associés. Il convient donc de rédiger un contrat adapté (offre précise, paiement sécurisé, livraison et service après vente clairement mentionnés...mode de règlement des conflits : recours au centre de médiation et d'arbitrage).

Mais surtout, il appartient aux utilisateurs d'adopter un comportement vigilant sur Internet en s'assurant de la fiabilité du site et de l'utilisation d'un système de paiement sécurisé. Afin de sensibiliser ce dernier, le professionnel peut l'alerter par ses conditions générales ou un message d'alerte clair et non équivoque en début et fin de transaction sur l'importance de l'utilisation d'un navigateur équipé d'un système de protection, du choix d'un mot de passe personnel alliant caractères alphanumériques et spéciaux, du non-partage des données, des méthodes employées par les hackers. Cette information doit nécessairement s'accompagner de l'adoption par le professionnel de procédés techniques sécurisés, qui permettent la traçabilité et la surveillance des transactions, mais également le cryptage des informations confidentielles, le recours à une signature électronique, tels que les protocoles SSL (Secure Sockets Layer) et SET (Secure Electronic Transaction). «Pour susciter la confiance du consommateur dans l'e-commerce, différentes solutions de paiement en ligne doivent lui être proposées : par carte bancaire via un système sécurisé, par e-numéro, par adresse électronique via des organismes offrant des services de paiement en ligne tels que Paypal ou Google Checkout. Cette diversité de moyens de paiement permet de pallier les risques de fraude», explique Corinne Champagner Katz, avocate, spécialiste en Propriété Intellectuelle, Consultante en Intelligence Economique.

On le voit, la mission de protection contre ces risques de fraude ne s'improvise pas. Et l'entreprise doit rester un territoire protégé afin de ne pas courir à sa perte. ■

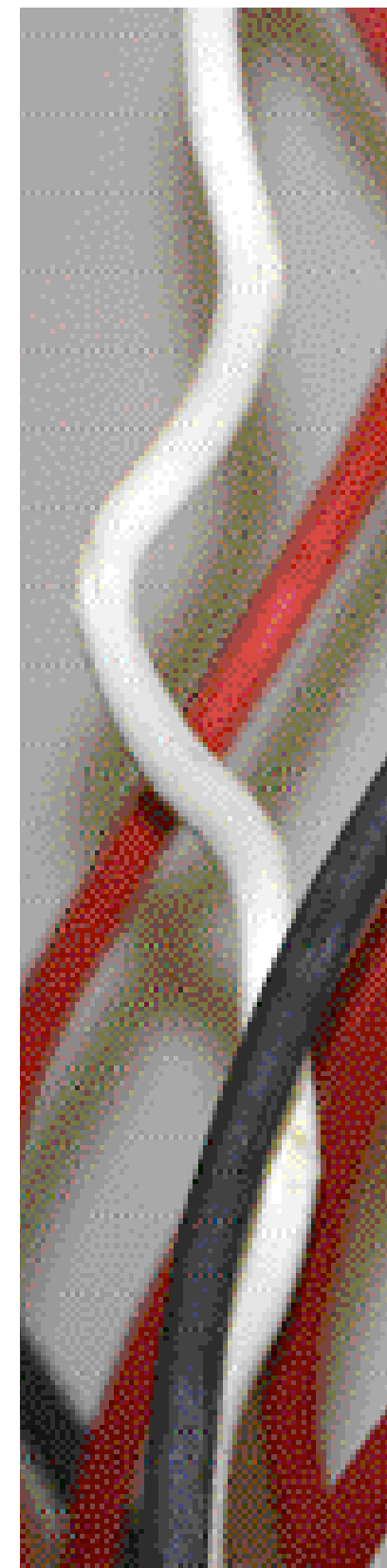


photo Anna Guessel