La responsabilité du notaire comme auteur, récepteur et utilisateur du document électronique

Wallemacq, A.; Montero, Etienne

Published in:
Authenticité et Informatique. Actes du colloque, Bruxelles, les 14 et 15 septembre 2000

Publication date:
2000

Document Version
le PDF de l'éditeur

LA RESPONSABILITÉ DU NOTAIRE COMME AUTEUR, RÉCEPTEUR OU UTILISATEUR DU DOCUMENT INFORMATIQUE

ETIENNE MONTERO (*)

PROFESSEUR AU FUNDP

ANDRÉ WALLEMACQ (**)

PROFESSEUR

SOMMAIRE

(*) Professeur de droit de l'informatique, membre du CRID, FUNDP, Namur.

(**) Notaire honoraire et professeur d'informatique juridique, EPHEC (Bruxelles) et IESN (Namur).

INTRODUCTION GÉNÉRALE

C'est un fait, l'informatique prend une place sans cesse croissante dans les études de notaire. Le recours à celle-ci présente de multiples avantages qui n'échappent à personne : facilité et rapidité de traitement de l'information, économie de tâches répétitives, commodité de gestion et de classement... Au revers de la médaille, le traitement informatique entraîne aussi son lot de mésaventures liées à des vicissitudes d'ordre technique ou à un mauvais usage de l'outil. Pour nombre d'études, l'informatisation est acquise depuis belle lurette. Aussi la pratique a-t-elle déjà permis de révéler certains chefs nouveaux de responsabilité, qu'il nous revient d'identifier dans un premier chapitre.

L'utilisation des réseaux numériques pour la consultation de services d'information, voire la conclusion de contrats et d'« actes », en ligne constitue le prolongement naturel de l'informatisation à des fins internes. Une fois les études bien équipées en matériel et programmes informatiques, rien ne s'oppose à leur interconnexion au sein d'un vaste réseau, susceptible de leur offrir, par ailleurs, une liaison avec leurs clients, leurs principales sources de renseignement – devenues, elles aussi, accessibles en ligne –, certains organismes publics et les banques.

Suite à un accord conclu entre la Fédération Royale des Notaires de Belgique (FRNB) et Isabel, le notariat dispose, aujourd'hui, d'un réseau Intranet professionnel basé sur la technologie Isabel (1). Ce réseau permet d'ores et déjà (ou permettra sous peu, c'est selon) aux notaires, dans de bonnes conditions de sécurité, d'échanger des messages électroniques, d'effectuer des opérations électroniques multibancaires, de transmettre des documents au Ministère de la Justice – en particulier, des actes de sociétés sous forme d'e-mail crypté pourvu d'une signature numérique, qui sont traités automatiquement dans le *Moniteur belge* –, d'accéder à diverses sources d'informations officielles de consultation courante (Registre Central des Testaments, Répertoire des faillites et des personnes sous interdiction judiciaire, Cadastre, Registre National, OVAM et bureaux hypothécaires, *etc.*).

(1) A cet égard, on lira avec profit la brochure « Informatique, internet, télécommunication : état de la question pour le notariat » insérée dans le *Notarius* du mois de septembre 1999.

Cette nouvelle forme de communication invite également à une réflexion sur les éventuels nouveaux aspects de la responsabilité du notaire découlant de l'usage des réseaux dans leurs activités quotidiennes. Tel est l'objet du second chapitre.

Avant d'entrer en matière, et puisqu'il sera question de responsabilité du notaire et de document électronique, il convient, sous peine de confusion, de préciser ces deux dernières notions.

Pour les besoins de la présente étude, la notion de « notaire » s'entendra non seulement de l'officier ministériel titulaire d'une étude notariale, mais aussi de tous ceux dont il assume la responsabilité du fait de sa charge, qu'il s'agisse de préposés ou d'associés, voire de sous traitants, dont il accepte la collaboration, en faisant sien le résultat de celle-ci, qu'il dispose ou non d'un recours contre eux.

Par « document électronique », on entendra toute information traitée par des moyens informatiques utilisés exclusivement, principalement ou accessoirement pour produire, traiter, transmettre ou conserver celle-ci, quels que soient le support ou le matériel utilisés.

La teneur du document est évidemment déterminante du niveau d'engagement de la responsabilité. Malgré l'adage « *in lege aquilia et levissima culpa venit* » et l'intime mélange entre l'office ministériel du notaire et sa profession libérale, nous distinguerons, d'une part, la responsabilité relative aux « actes », dont les lois font du notaire l'élaborateur, l'authentificateur ou le dépositaire, et d'autre part, celle liée aux « messages » qu'il émet ou reçoit.

CHAPITRE Ier. – LES RESPONSABILITÉS LIÉES À L'INFORMATISATION INTERNE

SECTION 1re. – *Risques physiques*

1.1. – *L'informatique soumise aux risques classiques*

Les ordinateurs sont sujets à des pannes et les logiciels à des dysfonctionnements d'ordres divers. Le notaire sera attentif à ces risques, d'autant qu'à supposer qu'il en résulte un préjudice pour autrui, il échappera difficilement à sa responsabilité en invoquant avec succès la cause étrangère libératoire (2). On s'avise, en effet, que les conditions de celle-ci seront rarement réunies dès lors qu'il dispose d'une large maîtrise sur les éléments informatiques, de manière à pouvoir conjurer efficacement le mauvais sort. Ainsi sera-t-il en peine de démontrer qu'un sinistre n'est aucunement imputable à sa faute dès l'instant où il aura négligé de prendre les précautions qui s'imposent à lui au titre de notaire normalement prudent et diligent. Tout au plus les interruptions d'électricité attribuables à l'opérateur de réseau, si elles devaient prêter à quelque fâcheuse conséquence, peuvent-elles être assimilées à des cas de force majeure.

On ne s'attardera guère sur les risques classiques tels que le feu, l'eau, la guerre, sauf pour souligner que, *mutatis mutandis*, les documents électroniques y sont exposés au même titre que les documents « papier ». Pour leur part, les documents électroniques sont soumis à des risques supplémentaires tels que la démagnétisation et, indirectement, les influences diverses de l'environnement de travail sur l'équipement. En plus des précautions d'usage contre les risques physiques, il convient dès lors de prévoir certaines mesures de protection des micro-ordinateurs. On placera ceux-ci, notamment le serveur, en un lieu approprié, à l'abri du passage et à bonne température.

(2) Sur les conditions de la cause étrangère libératoire, voy., par exemple, S. STIJNS, D. VAN GERVEN et P. WÉRY, « Chronique de jurisprudence. Les obligations : les sources (1985-1995) », *J.T.*, 1996, pp. 726 et s., nos 108 et s., et les réf.

1.2. – *Défaillances techniques et sauvegardes*

La sauvegarde régulière des fichiers, aux fins de prévenir les risques d'effacement accidentel des données qu'ils contiennent est un très vieux souci qui s'est habillé, concernant les fichiers informatiques, du terme anglais de *back-up*.

Toutes les formations, tous les manuels font de la sauvegarde régulière, et si possible bi-localisée, la mesure de prudence indispensable à tout traitement informatisé...

Et pourtant, très régulièrement, des sinistres se produisent faute d'avoir pris ces mesures : des disques durs ou autres fichiers sur supports mobiles sont effacés, bloquant l'activité du bureau pour plusieurs heures, voire pour plusieurs jours, condamnant l'entreprise à une nouvelle saisie au départ d'un état papier (s'il existe) de données à revérifier, ou même à leur longue et coûteuse reconstitution.

Le problème n'est en rien différent de celui, classique, de l'incendie, mais la sensibilité de la clientèle préjudiciée y est différente : à juste titre, l'accident est moins ressenti comme de force majeure parce que chacun sait que des mesures de simple prévoyance auraient pu l'éviter. L'assureur du risque informatique ne réagira d'ailleurs pas autrement.

A noter que le mauvais usage des *back-up* comporte lui aussi un risque : certains se font remarquer, notamment en début d'année ou à l'occasion d'une fusion, en « ressuscitant » des renseignements, des comptes, voire des personnes...

1.3. – *Archivage* « ad probationem »

La question de l'archivage est souvent traitée avec condescendance en doctrine, comme relevant du seul domaine matériel.

Elle n'en reste pas moins pour le notariat une notion essentielle, et, oserions-nous dire, fondatrice : une petite rime, au fond pas si sotte, n'affirme-t-elle pas que « *notaren is bewaren* » et la protection des archives « majeures » du notaire (ses minutes) n'est-elle pas à l'origine de bien des caractéristiques de la profession, comme le panonceau (si souvent confondu aujourd'hui avec une quelconque enseigne, alors qu'il signalait

aux pompiers les lieux de conservation des archives privées), l'organisation des protocoles, les règles du répertoire, *etc.*

Dans le cadre du présent rapport, cet aspect de la conservation ne sera toutefois ni le seul abordé, ni même principalement traité. L'archivage, considéré sous l'angle du document informatique, revêt en effet trois aspects : l'un, déjà évoqué, « de sauvegarde », celui « *ad probationem* », qui retient à présent l'attention, et l'archivage aux fins de réutilisation, envisagé au point suivant.

Pour la conservation des « actes » à des fins probatoires, les règles traditionnelles, pensées et mises au point dans un « contexte papier », ne sont pas prêtes, en droit notarial, à céder de sitôt la place à d'autres supports d'information, même si ceux-ci se sont imposés de longue date en droit commercial.

Il est à noter toutefois que le notaire, comme dépositaire légal des minutes, se voit rarement demander la production physique de celles-ci, et sera généralement cru, sur foi de son serment de fonction, quant à la conformité des reproductions.

Dès lors que la plupart des études utilisent désormais le traitement informatique pour rédiger les actes, grande est la tentation d'utiliser le réseau interne pour stocker ces actes. Si l'exigence d'un écrit (papier) signé (manuscritement) par les parties et le notaire semble faire obstacle à une telle conception de l'acte notarié, les progrès de la sécurité et de la signature informatique, et l'admission en notre droit de cette dernière, autorisent à envisager sérieusement cette éventualité. On y reviendra (*infra*, chap. 2, section 2, point 2.2).

Dans l'immédiat, on observera qu'il est dans l'usage du temps de produire des copies d'actes à partir de documents « papier » scannés/numérisés ou même des mémoires de l'ordinateur. Cette pratique, que d'aucuns jugeront « limite », ne modifie en rien la responsabilité de conformité assurée par le notaire, même s'il estime pouvoir la garantir au départ de documents qui ne sont plus les originaux (c'est le cas, notamment, des études qui, pour la facilité du traitement, mais aussi pour la sécurité des minutes, travaillent sur des microfilms de celles-ci). On est renvoyé ici aux risques et à la responsabilité du fait de l'homme (*infra*, 2.1.3.).

La gestion du risque, sur ce point, relève, une fois de plus, d'une réflexion sur l'organisation du bureau et la fiabilité de son matériel.

1.4. – *Les avatars de l'archivage pour réemploi*

D'un point de vue strictement utilitaire, on archive en traitement informatique **uniquement** ce qui est susceptible de resservir avec un certain degré de répétitivité et la chose peut même être établie par *ratios*. L'approche des études est, à ce sujet, nettement plus pragmatique : on y réutilise davantage ce que l'on trouve, que ce que l'on a conservé à cet effet.

En tout état de cause la réutilisation de données apporte un confort, voire une sécurité, appréciable. Décrire les risques inhérents à cet usage est aussi énoncer les règles qui l'optimisent. Les risques physiques confinent ici à ceux du fait de l'homme (*infra*, section 2). Le notaire y sera attentif car, naturellement, sa responsabilité pourra être engagée.

Le premier risque est celui de l'erreur répétitive, du nom, de l'adresse, du numéro de cadastre erronés inlassablement reproduits de document en document avec les conséquences, parfois désastreuses, que l'on devine : on croit avoir écrit, saisi le bureau compétent... et tout est à refaire alors que le temps s'est écoulé; on reproduit l'erreur d'état civil qui a porté préjudice et doit être réparée à grands frais judiciaires.

On insistera jamais assez sur le fait qu'une saisie de données, sauf indication contraire, doit être considérée comme acquise une fois pour toutes et, de ce fait, accomplie avec le plus grand soin (les débuts de l'informatisation ont même connu la double frappe, qui a survécu dans la saisie de certains mots de passe ou d'informations clés).

Un deuxième risque, tout aussi insidieux, est celui lié à l'obsolescence des informations : un changement d'adresse, d'état civil (divorce, veuvage...), *etc.* Ici aussi le document trompe, avec toutes les apparences de la véracité. L'information a sa date de péremption également, qu'il est peu d'usage de mentionner dans son travail, mais qui pourrait utilement être rappelée par la typographie ou un signe appelant à la vérification.

Un troisième risque est celui des emprunts malencontreux, de l'acte déshabillé de ses variables et rhabillé de celles d'une nouvelle affaire. Le résultat peut être heureux, parfois drôle comme la chemise du grand frère portée par son cadet, et parfois nettement moins drôle parce qu'il reste des noms, des tournures, des clauses indésirables...

A l'expérience, l'élimination du risque passe par l'élimination du procédé, mais même des instructions formelles données en ce sens sont vite oubliées...

1.5. – *Les hiérarchies dans l'accès à l'information*

La protection de l'archive doit se concevoir à différents niveaux, selon les exigences de la discrétion et du secret professionnel, à pondérer selon la gravité des risques encourus, mais aussi la motivation et le coût de l'indiscrétion.

La définition de niveaux d'accès à l'information (et, parallèlement à la décision) se développe au sein des études : tout un chacun ne dispose pas des « clefs » (en règle, des mots de passe) de la comptabilité, de certains fichiers d'adresses, de certains agendas, *etc.* Souvent la chose s'est faite au coup par coup, sans relever d'une réflexion ou d'une organisation globales pour lesquelles on plaide ici et qui devient indispensable si l'on travaille en réseau (*infra*, chap. 2, spéc. section 4).

Section 2. – *Risques du fait de l'homme*

2.1. – *Le document informatique, évolutif par nature*

Il ne faut pas se cacher qu'il est de l'essence même du traitement d'un document informatique d'y apporter des modifications, des corrections, des ajouts, des suppressions.

En ce sens, il peut être défini comme un « perpétuel brouillon » et il convient de s'interroger sur le moment et le motif précis du basculement du document vers un état dont le respect de l'intégrité va s'imposer.

2.1.1. *Le cas des « messages »*

La mise au point des messages, leur suivi, leurs critères de diffusion, la discrétion ou le secret professionnel imposeront la modification, et pourtant, la règle d'or restera de figer et protéger l'intégrité de tout texte adressé à un destinataire, quitte à lui permettre par ailleurs de poursuivre sa carrière en y adjoignant des notes, des correctifs nettement marqués, *etc.*

Tous les programmes de traitement de texte permettent cela facilement. Il suffit d'utiliser à bon escient la classique fonction « suivi des modifications-surlignage », par exemple, qui vise à faire apparaître à l'écran les corrections successives apportées au document. Encore faut-il avoir pensé l'organisation des procédures à appeler, les pouvoirs et éventuelles signatures d'intervention.

S'agissant plus particulièrement d'un texte « éclaté » vers divers services, une sauvegarde de la synthèse originale s'impose impérieusement.

A noter que sur le plan des responsabilités, retrouver le cheminement d'un texte querellé sera souvent fort utile pour organiser sa défense.

2.1.2. *Le cas des « actes »*

Les recommandations faites pour les messages s'appliquent pareillement aux « actes », mais les dispositions organiques du notariat imposent en outre des règles spécifiques (3) :

- lecture et explication spéciale, mentionnées à l'acte, devront être faites de toute modification apportée au projet d'acte préalablement communiqué aux parties.
- tout mot biffé ou raturé doit rester lisible sous le trait correcteur et les mots nuls doivent être comptés, numérotés et

(3) Voir l'article 12 de la loi du 25 ventôse an XI, tel que modifié par une loi du 4 mai 1999. On rappelle que deux lois ont été adoptées le 4 mai 1999, l'une *modifiant* la loi de ventôse et l'autre *complétant* cette dernière. Ces deux lois ont été publiées au *Moniteur belge* du 1er octobre 1999, pp. 37132 et s. Pour un commentaire de l'article 12 (nouvelle rédaction), voy. J.-F. Ledoux et D. Sterckx, « La réforme du notariat et des actes notariés », *J.T.*, 2000, pp. 209 et s., spéc. pp. 221-222.

approuvés dans leur suppression par une mention expresse en clôture de l'acte.
- les ajouts doivent figurer en renvoi et être approuvés.

Ces règles, qui viennent de la nuit des temps et de la civilisation de l'écrit tout court, sont parfaitement transposables à l'environnement informatique, et survivront sans doute encore bien longtemps (*supra*, 2.1.1.). Elles ne peuvent être gommées par le confort, pourtant évident, de la suppression et de l'ajout en traitement de texte, voire même par le souci de produire un acte impeccable.

Qu'on se rappelle la mise en cause de ce notaire qui, pour bien faire, lisait à ses clients, à l'écran, le texte de son acte, en faisait une dernière mise au point, et proposait un texte formellement parfait à la signature des parties : il s'est trouvé l'une d'elles pour affirmer qu'on lui avait fait signer autre chose que ce qui lui avait été lu.

2.1.3. Quid *des copies d'actes?*

Un mot doit être dit des copies d'actes, mais surtout de leurs expéditions, évidemment produites par le matériel informatique de l'étude. Ici aussi la tradition notariale connaît les maîtres mots de collationnement et de certification de conformité, dont l'oubli est à l'origine de très nombreux sinistres :
- formule exécutoire dont le début « est resté dans la machine ».
- formule exécutoire erronée reproduite plus de cent fois avant que l'on s'aperçoive de l'erreur (et de la nullité des grosses).
- expédition par trop conforme au projet : absence de date (très fréquent!), mention biffée qui réapparaît (pour une fois qu'on pouvait valablement utiliser la touche Delete!), renvoi non reproduit.
- pages manquantes et/ou en double
- « mixage » malencontreux entre deux actes fort ressemblants du même jour.
- réapparition indue des données de l'acte qui a servi de « modèle ».

On dira qu'il est facile de censurer après coup, d'oublier le rythme des affaires, le signataire qui déborde et tant de choses du quotidien des études. Nous ne faisons que plaider ici pour un meilleur usage des possibilités de traitement informatique du document, qui donnent les moyens de marquer les textes, d'indiquer où ils ont été modifiés, *etc.* Il s'agit de déblayer le terrain pour l'exercice d'une vigilance recentrée sur l'essentiel.

2.2. – *La vérification des données*

La vérification des données est un problème connu de longue date par la pratique notariale. Il est examiné dans un autre rapport auquel le lecteur est invité à se reporter.

Le fonctionnement du système hypothécaire en donne un bon exemple : l'information sur la situation hypothécaire d'un bien se passe à deux niveaux, l'un d'une (relative) rapidité, mais sans garantie ni responsabilité du conservateur des hypothèques, l'autre après un délai certain – qui peut atteindre dans certains bureaux plusieurs mois – engageant cette fois la responsabilité du conservateur en un certificat qu'il (anti)date et signe.

De pratique constante, le notaire engagera sa propre responsabilité sur la base des renseignements qui lui ont été donnés « sans garantie, ni responsabilité » (recherche préalable), et fera appel à son assureur si le renseignement ainsi obtenu est incomplet ou erroné. Il y fera aussi appel si, entre la date de la recherche – qui figurera sur le certificat – et la date de signature, de transcription ou d'inscription de l'acte, une inscription ou une transcription inattendue affecte le bien.

Seul l'Etat, pour lui-même, jouera la carte de la sécurité absolue et ne libérera les fonds, en matière d'expropriation, qu'au vu d'un nouveau certificat postérieur à la mutation elle même.

Ce rappel de faits, pour ahurissant qu'il soit vu de l'extérieur de la profession, serait dans ce rapport un exercice gratuit, si la situation qu'il décrit n'était appelée à se généraliser à d'autres domaines et dans un contexte qui s'élargira rapidement au delà de nos frontières, par suite de l'usage de moyens informatiques et télé-informatiques.

Pour parler sans nuances, ceux-ci ont l'avantage de la rapidité, si souvent déterminante dans le cours des affaires, mais au détriment de la sécurité dont on estimera toutefois le notaire débiteur, sans lui permette de subordonner son engagement aux délais et aux lenteurs de la vérification administrative.

Il faut donc s'attendre à ce que le notariat, dans d'autres domaines que celui de la sécurité hypothécaire, exerce son métier dans un contexte de risques plus ou moins calculés et de résultats qui ne seront que statistiquement satisfaisants, l'assurance étant sollicitée de prendre en charge l'échec et le dysfonctionnement.

L'analyse de ces risques se fait en termes de collecte et de vérification adéquate des données et peut être illustrée par les exemples suivants :

- combien d'identifications, dans les dossiers et dans les actes, au seul vu de la carte d'identité ou des données d'un « acte » antérieur (en fait, une copie ou un projet, et en tout cas une source invérifiable) ?
- combien de « titres de propriété » recherchés chez le seul receveur de l'enregistrement ou même au cadastre, *etc* ?
- combien de clients « bien connus de l'étude », et dont on ne vérifie plus la fiche, datant parfois de plusieurs années ?

Ce n'est pas le lieu ici d'allonger la liste, mais de constater qu'une fois obtenu, le renseignement n'est pas toujours « sécurisé » suivant les normes de qualité qui sont prescrites au notariat et dont il ne manque pas de s'enorgueillir.

Et la facilité de collecte apportée par l'informatique n'améliorera sans doute pas les choses (4)... Cependant, des procédures appropriées peuvent multiplier utilement les recoupements et provoquer, dès l'obtention d'une donnée, l'appel aux sources officielles, tout en « marquant » la donnée comme encore à vérifier. De même, une programmation adéquate peut – au stade du projet – dater la donnée, signaler son obsolescence, voire proposer sa mise à jour.

(4) Sur le sujet, voy., *ad generalia*, E. MONTERO, *La responsabilité civile du fait des bases de données*, P.U.N., Namur, 1998.

En tout état de cause, à mesure que les bases de données en ligne gagneront en fiabilité et les systèmes d'accès à celles-ci en efficacité, on peut se demander si la jurisprudence ne sera pas tentée de dégager une *obligation* de consultation de ces outils documentaires, déduite du devoir de prudence et de diligence. A la réflexion, il ne paraît pas incongru de penser que le notaire normalement prudent et diligent se devra, demain, d'interroger les bases de données en ligne dès l'instant où elles seront devenues performantes et de nature à conjurer le risque d'ignorer une donnée capitale.

CHAPITRE II. – LES RESPONSABILITÉS LIÉES À LA COMMUNICATION PAR LE BIAIS DES RÉSEAUX

SECTION 1er. – *Réflexions liminaires et limites de l'exposé*

Établir, passer, signer, expédier des actes uniquement par procédé informatique et télé-informatique relève, aujourd'hui encore, du « notariat fiction ». Mais, peut-être, pour pas bien longtemps... En effet, dès lors que les études de notaire, leurs clients, les banques et autres organismes publics ou dispensateurs de renseignements en ligne se trouvent interconnectés au sein d'un vaste réseau sécurisé, se pose, d'évidence, la question de l'irrésistible évolution de l'identité, de la fonction et des activités du notariat.

Pourquoi pas, demain, l'acte authentique conclu et signé, à distance, par voie électronique ? A cet égard, les limites du vraisemblable reculent à vive allure au point que nous sommes portés à reconsidérer ce que nous écrivions voici à peine quelques années, lorsque nous suggérions que l'acte authentique – dans la mesure où il requiert, en tout ou partie, l'écriture de l'acte, de la main du notaire, et sa signature également manuscrite en l'étude notariale en présence de toutes les parties – a été formellement constitué comme un « *quod plerumque fit* » de la transmission de l'information, laissant d'autres modes de la

transmettre (paroles, écrit privé, actes sous seing privé) aux risques de la non authenticité (5).

Ministre de l'authenticité, le notaire est garant de l'identité des parties, de l'exactitude et véracité des éléments essentiels et mentions de l'acte, de la date et du lieu de signature. Tenu de conseiller et d'éclairer les parties sur la teneur, la nature et la portée juridique de l'acte, il est aussi témoin privilégié que ce dernier reflète précisément les volontés en présence. Cependant, il s'impose aujourd'hui de réfléchir à la possibilité, pour le notaire, de s'acquitter, à distance par un biais électronique, des devoirs dont il est investi.

Si la proposition de directive européenne sur le commerce électronique, en passe d'être définitivement adoptée, prévoit la suppression de toutes les exigences de forme (6) qui constituent des obstacles à la conclusion de contrats *via* les réseaux, elle établit néanmoins, provisoirement (?), une exception en faveur de certaines catégories de contrats, parmi lesquelles ceux qui requièrent l'intervention des autorités publiques ou de professions exerçant une autorité publique (tel le notaire) (7). Cependant, les États devront faire rapport à la Commission européenne tous les cinq ans et justifier le maintien de ces exceptions (Art. 9, 3). C'est dire que l'on ne peut faire l'économie d'une réflexion en profondeur sur le rôle et les missions du notariat. A cet égard, il convient d'envisager aussi l'opportunité de confier au notaire certaines fonctions nouvelles dans le cadre de la société de l'information. On songe notamment à son intervention sur les plans de la certification, de l'archivage et de l'horodatage de documents électroniques, de l'offre d'un service de recommandé électronique avec accusé de réception (voir *infra*, section 3) pour attester de l'envoi et de la réception de messages, *etc.*

(5) Cf. A. WALLEMACQ, *Le document informatique et la sécurité juridique*, Actes du XX^e^ Congrès de l'Union internationale du notariat latin, Carthagène (Colombie), 27 avril-2 mai 1992, p. 153.

(6) Ou la prise en charge de leur fonction par des équivalents électroniques.

(7) Position commune arrêtée par le Conseil en vue de l'adoption de la directive du Parlement européen et du Conseil relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, art. 9, 1 et 2.

Ces brèves remarques n'avaient d'autre but que d'indiquer les limites de notre exposé, dans la mesure où ces prospectives sont explorées par d'autres rapports auxquels nous renvoyons (8).

En effet, pour l'heure, les notaires font des réseaux un usage encore bien limité. Sur le terrain des actes juridiques, ils se sont imposés, à ce jour, uniquement pour échanger des messages, établir des *projets* d'actes, les communiquer et, après signature, transmettre des copies. En tout cas et à proprement parler, il ne s'agit jamais que de « messages » à propos d'actes.

C'est à ces seules pratiques, encore forcément timides, que se limite, pour l'essentiel, notre examen des risques et responsabilités liés à la communication par le biais des réseaux.

SECTION 2. – *Identification de l'auteur et confidentialité des documents*

Comment s'assurer, avec quelque certitude, de l'identité du destinataire d'un message électronique et comment empêcher la divulgation de celui-ci au bénéfice de tiers par trop indiscrets ? La première question a pour réponse la *signature numérique*, la seconde renvoie à la notion de *confidentialité*.

Deux problèmes, une solution : la cryptographie ! En effet, les procédés modernes de cryptographie permettent, d'une part, de *signer* un message, d'autre part, de *garantir la confidentialité* des communications (9).

Après une brève description technique (10), il nous faudra mesurer l'impact de l'utilisation des cryptosystèmes en termes de risques et de responsabilités pour le notaire.

(8) A ce sujet, on ne saurait trop recommander la brillante étude de A. GOBIN, « Pour une problématique notariale des autoroutes de l'information. Le notariat et les contrats immatériels », *J.C.P.*, Ed. N, 1995, n° 3567, pp. 1749-1762.

(9) Sur l'ensemble de la question, voy. notamment l'étude récente de D. GOBERT et E. MONTERO, « La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle », in *Commerce électronique. Le temps des certitudes*, Cahiers du CRID, n° 17, Bruxelles, Bruylant, 2000, pp. 53-98.

(10) Pour une explication détaillée, S. PARISIEN et P. TRUDEL, *L'identification et la certification dans le commerce électronique*, Québec, Ed. Yvon Blais Inc, pp. 93 à 113; J. HUBIN, *La sécurité informatique, entre technique et droit*, Cahiers du CRID, n° 14, E. Story-Scientia, 1998, spéc. pp. 68-112.

2.1. – *Description (sommaire) des procédés de cryptographie*

Une première fonction des cryptosystèmes, appelée chiffrement, est de garantir la confidentialité des échanges. L'opération consiste en la transformation d'un message dit « en clair » en une chaîne de caractères alphanumériques qui ne sont compréhensibles que pour la personne autorisée. Les produits couramment utilisés à cet effet sont fondés, pour la plupart, sur le *Data Encryption Standard* (DES). Il s'agit d'un système cryptographique à clé unique (ou à clé secrète) utilisant un algorithme qui, comme le suggère son nom, chiffre et déchiffre un message à l'aide d'une seule clé. Pareil procédé, qui implique de communiquer la clé au destinataire, avec les inévitables risques d'interception, est surtout efficace dans les réseaux fermés. Par contre, il s'avère relativement inadapté aux réseaux ouverts ou pour une utilisation à des fins de signature.

Ce problème du partage des clés est résolu par le recours à la cryptographie asymétrique, ou « à clé publique ». Celle-ci permet d'expédier des messages confidentiels dans de meilleures conditions de sécurité. Elle peut servir aussi à des fins de signature. Le mécanisme repose sur l'utilisation d'une paire de clés, l'une secrète et l'autre publique, unies entre elles par une formule mathématique. L'application la plus répandue de cryptographie à clé publique est le *R.S.A.*, du nom de ses concepteurs (Rivest, Shamir et Adleman, du M.I.T.). Cette technologie est offerte notamment aux clients du réseau Isabel, et singulièrement aux notaires ayant souscrit un abonnement. Ces derniers ont donc le loisir d'envoyer des e-mails signés et encryptés.

Le fonctionnement du procédé de cryptographie asymétrique peut être schématisé comme suit : le message est signé par son auteur à l'aide de sa clé privée, puis il est expédié au destinataire, qui peut le déchiffrer uniquement avec la clé publique complémentaire à la clé privée de l'émetteur. Ainsi, le destinataire est certain que le message émane bien de son auteur dûment identifié, du moins à la condition qu'un certificat délivré par une autorité de certification confirme que la clé publique appartient réellement à l'émetteur (voir ci-après). Pour assurer la confidentialité d'un échange, l'expéditeur procédera inversement : il chiffrera le message à l'aide de la clé publique du destinataire, qui pourra uniquement le déchiffrer au moyen de sa propre clé secrète. Ce faisant, il est le seul à pouvoir prendre connaissance du message. Il va de soi que les deux fonctions peuvent être combinées pour l'envoi d'un message à la fois confidentiel et signé.

Le recours à la cryptographie à clé publique suppose naturellement l'organisation de la publicité des clés publiques et l'instauration d'un mécanisme de contrôle visant à s'assurer que celles-ci correspondent bien aux personnes qui s'en prétendent titulaires. Cette double mission de publicité et de certification est actuellement assumée par un tiers certificateur (appelé encore « autorité de certification »). Ce rôle est joué actuellement par Isabel dans le cadre du réseau qu'elle a mis en place et auquel participent, entre autres, les notaires. A ce titre, Isabel est habilité, d'une part, à *vérifier l'identité* des titulaires de clé publique et à *générer des certificats*, soit des structures de données signées digitalement qui font le lien entre une personne et sa clé publique, et, d'autre part, à *assurer la publicité* la plus large des certificats ainsi émis (11). L'autorité de certification est également tenue de maintenir à jour le répertoire contenant les certificats de clé publique, en veillant, selon le cas, à leur suspension, révocation ou renouvellement. On mesure l'importance du recours à ce genre de procédure pour assurer la fiabilité de la signature numérique et inscrire ainsi les échanges et relations jugées sensibles dans un cadre sécurisé.

2.2. – *Risques particuliers et responsabilités*

Le recours à la cryptographie pour assurer la confidentialité d'un échange ne semble pas soulever de question particulière sur le terrain de la responsabilité (si ce n'est une éventuelle

(11) Pour plus de détails, S. PARISIEN et P. TRUDEL, *op. cit.*, pp. 117 et s.; E. DAVIO, « Certification, signature et cryptographie », in E. MONTERO (éd.), *Internet face au droit*, Cahiers du CRID, n° 12, E. Story-Scientia, 1997, pp. 80 et s., et du même auteur, « Preuve et certification sur Internet », étude précitée; M. ANTOINE et D. GOBERT, « Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification », *R.G.D.C.*, 1998, n° 4/5,, pp. 285-310, spéc. pp. 293 et s.

violation du secret professionnel du notaire imputable à une négligence dans l'usage des outils de chiffrement). Il en est autrement de son usage à des fins de signature, qui retiendra surtout notre attention.

La doctrine considère traditionnellement qu'une double fonction est dévolue à la signature : elle permet d'identifier l'auteur d'un acte et exprime son adhésion au contenu de ce dernier. L'avènement de la signature électronique a mis en évidence une troisième fonction : elle sert aussi à vérifier si l'intégrité de l'acte a été préservée au cours de l'échange. A défaut d'être radicalement neuve, cette fonction présente, dans l'environnement numérique, un aspect relativement inédit.

Notre propos est d'évaluer, au regard de ces diverses fonctions de la signature, les risques et responsabilités encourus du fait du recours à un procédé électronique.

La fonction d'identification de la signature est assurée, de manière efficace et sûre, par le recours à la cryptographie asymétrique. De l'avis des experts, un cryptosystème performant, tel le RSA, serait pratiquement inviolable. Le risque de fraude le plus vraisemblable – quoique plutôt faible – est lié à la perte de maîtrise de la clé privée par son titulaire (dans le système Isabel, celle-ci est intégrée dans la puce de sa Smart Card). Ce dernier veillera donc à ce que celle-ci soit conservée dans de bonnes conditions de sécurité. En cas de négligence à cet égard, dont il résulterait un préjudice, il s'expose à une mise en cause de sa responsabilité. Par ailleurs, les notaires devront faire diligence, sous peine d'engager leur responsabilité, en adoptant le réflexe de consulter le répertoire central des clés publiques géré par Isabel pour vérifier la signature, et ainsi l'identité, des auteurs des messages électroniques qui leur sont adressés.

La deuxième fonction de la signature, inséparablement unie à la première, est l'appropriation, par le signataire, du contenu du document.

Dès l'instant où la clé de chiffrement est appliquée de manière volontaire et personnelle, *à l'exclusion de toute opération purement automatique*, par l'auteur d'un document électronique, il est permis de considérer qu'il en approuve la teneur.

Encore faut-il que la signature soit liée *logiquement* au document, à défaut d'un lien « physique » entre les deux (dans le cas des écrits signés manuscritement). Cette exigence – qui renvoie à la question de l'intégrité – conduit la doctrine à estimer que la signature électronique suppose nécessairement une *transformation de l'écrit*. Autrement dit, pour s'assurer du maintien du contenu intégral du document transmis, il importe que le fichier « signature » soit obtenu par application de la clé cryptographique au fichier « document » (voir ci-après). Le législateur belge se devra d'y être attentif au moment d'accueillir en notre droit la signature électronique. Le notaire, lui, sera conscient qu'un simple « clic » est susceptible de l'engager juridiquement. D'un point de vue psychologique, en effet, la contrainte de l'écrit papier a le mérite d'attirer l'attention du signataire sur la portée juridique de son geste. Or, il n'est plus question ici de la « solennité » qui accompagne le mouvement de la plume, ni de mention manuscrite du genre « lu et approuvé »... L'absence de ce « formalisme » dans l'environnement numérique ne saurait faire oublier les effets de la signature.

La signature numérique possède également la vertu d'assurer le maintien de l'intégrité du contenu du document. En réalité, la doctrine classique n'en souffle mot. En effet, sous l'empire de la signature manuscrite, cette fonction est assurée, non au moyen de la signature elle-même, mais par le biais du support papier sur lequel elle figure nécessairement. Il s'agit d'un support inaltérable (les fraudes sont difficiles à dissimuler : les ajouts ou ratures sont décelables) et stable (le papier se dégrade peu). Ces qualités fonctionnelles du papier expliquent, à cet égard, qu'il ait été placé au sommet dans la hiérarchie des modes de preuve. Le contenu étant, pour ainsi dire, matériellement indissociable du support, ce dernier permet d'assurer l'intangibilité et la non-répudiation du contenu.

En particulier, la signature numérique, fondée sur la cryptographie asymétrique, permet de vérifier adéquatement et de façon certaine si l'intégrité à été préservée.

La signature (soit le petit fichier numérique représentant cette dernière) est, en effet, le résultat de l'encryptage du fichier 'document'. Il suffit dès lors au destinataire, une fois

le fichier signature déchiffré, de procéder à la comparaison des deux fichiers et de constater ainsi la sauvegarde de l'intégrité. L'opération peut être facilitée grâce à une fonction dite « de hachage » (qui consiste à condenser au préalable le document, de manière à rendre plus aisée la comparaison des fichiers ainsi réduits).

Cette fonction de la signature numérique est évidemment déterminante dans le contexte des réseaux pour assurer la sécurisation des flux de données. Mais elle présente aussi un aspect particulièrement intéressant eu égard à la conservation des documents jugés significatifs. En effet, la même technologie permet aussi d'assurer l'intégrité (du contenu) *dans la durée*, peu importe à cet égard que le document, assorti d'une signature numérique, soit inscrit sur un disque dur (exploité en ligne) ou ait été soustrait à l'informatique en temps réel, pour *archivage* (inscription sur un CD-ROM, une bande plombée...) (12). En toute hypothèse, encore faut-il avoir prévu le moyen d'obvier à l'éventuelle obsolescence des supports (moyennant leur rajeunissement), des clés et des certificats de clé publique (13). Ces deux derniers aspects sont normalement du ressort de l'autorité de certification, qui veillera à recréer une nouvelle paire de clés et un nouveau certificat (si la paire de clés utilisées pour signer ne présente plus un degré de sécurité suffisant) et, plus largement, à contrôler que les certificats émis sont toujours exacts et conformes à la réalité (voir aussi ci-après). Mais le notaire ne pourra pas rester complètement indifférent à la question, sous peine, ici aussi, d'engager éventuellement sa responsabilité.

La signature, faut-il le rappeler, permet de conférer à un document le statut de document original. Il s'agit là d'une exigence essentielle de l'acte sous seing privé qui, par définition, doit être un écrit original (c'est-à-dire signé). Cet aspect mérite

(12) Comp. X. LINANT DE BELLEFONDS, « L'internet et la preuve des actes juridiques », *Expertises*, 1997, p. 226.

(13) On sera également attentif au problème de la lisibilité, le temps passant, des documents pourvus d'une signature numérique. En effet, il peut devenir malaisé de relire des documents créés avec des outils informatiques introuvables ou dépassés et de restituer en clair un document chiffré. Sur ce point, E. DAVIO, « Preuve et certification sur Internet », *R.D.C.*, 1997, n° 11, chap. 3, section 3.

aussi d'être brièvement évoqué, même si, dans l'actuelle pratique notariale, il n'est pas encore question de conclure et de conserver des actes par des moyens électroniques. Il convient néanmoins que le notaire soit d'ores et déjà sensibilisé à ce problème; tout porte à croire, en effet, qu'il y sera confronté dans un proche avenir.

Avec l'apparition des supports informatiques et la facilité de reproduction des données numériques y figurant, la distinction original/copie se trouve quelque peu bousculée. On aurait tort de croire que toute *reproduction* d'un document informatique s'analyse en une copie. En effet, l'unicité d'un document n'est pas la condition de son originalité, comme l'atteste la formalité des originaux multiples imposée par l'article 1325 du Code civil. L'existence d'une garantie d'intégrité ne suffit pas davantage au maintien de la forme originale d'un document, contrairement à ce qui est parfois affirmé. En fait, c'est la *signature*, et elle seule, qui élève un document au rang d'original. La copie s'en distingue précisément par la circonstance qu'elle en est une transcription non signée (14). La technique informatique présente la particularité de rendre aisée la reproduction, en original ou en copie, d'un document. Dès lors que la signature de l'émetteur reste attachée au document, nonobstant la transmission, et que sa conformité peut être vérifiée, le nouveau document a valeur d'*original*, à l'instar du document *originaire*. Dans le cas contraire, il s'analyse en une copie et a valeur de commencement de preuve par écrit ou de simple présomption. Ici encore, on doit constater que ce n'est plus le support qui assure l'indispensable maintien de l'intégrité du document, mais la signature, dont le mécanisme permet de *figer logiquement le contenu* du document (15).

Il s'ensuit que le document muni d'une signature numérique ne vaudra plus que comme copie dès l'instant où le certificat de clé publique se trouve révoqué ou frappé de caducité car, dans ce cas, la signature ne peut plus être vérifiée. D'où la

(14) H. DE PAGE, *Traité*, t. III, 3e éd., n° 832; R. MOUGENOT, *La preuve*, *Rép. not.*, t. IV, Livre 2, 2e éd., Bruxelles, De Boeck et Larcier, 1997, p. 185, n° 187; N. VERHEYDEN-JEANMART, *Droit de la preuve*, Bruxelles, Larcier, 1991, p. 201, n° 417.

(15) À ce sujet, E. DAVIO, *op. cit.*, *R.D.C.*, 1997, n° 11, pp. 664 et s.

haute importance de la mission de gestion des certificats confiée à l'autorité de certification. Il lui appartient de veiller à suspendre, voire révoquer, les certificats ou de procéder à leur renouvellement. En cas d'obsolescence des clés et, partant, des signatures, par suite d'une évolution technique (qui fait qu'un code indéchiffrable hier ne l'est plus aujourd'hui), il lui faudra aussi émettre un nouveau certificat. Comme déjà souligné, le notaire pourrait être tenu de faire diligence en cas d'inertie ou de négligence de l'autorité de certification.

Un bémol doit toutefois être apporté à ce propos. En effet, un document signé numériquement pourrait garder la valeur d'original, alors même que le certificat serait révoqué ou aurait expiré, voire que la technique serait devenue obsolète, si le document est conservé par un tiers « indépendant » – on songe, pour l'heure, à Isabel – dans le cadre d'un régime sécurisé d'archivage électronique, combiné à un système d'horodatage des documents. Ceci permettrait de répondre aux nombreuses exigences légales qui imposent la conservation des originaux pendant un nombre d'années largement supérieur à la durée du certificat. Pour ce faire, encore faut-il déterminer les conditions techniques et juridiques auxquelles l'archivage pourra être effectué. Ce problème, qu'il n'est naturellement pas possible d'examiner ici en détail, ne semble pas insurmontable et doit nécessairement être pris en compte.

Section 3. – *Échange de documents : preuve de l'envoi et de la réception*

L'échange de messages ouvre classiquement la discussion sur le terrain de la preuve de leur envoi et/ou réception : il incombe à l'émetteur de prouver l'envoi, preuve des plus difficiles quand il s'agit d'un document informatique. Sa présence sur son matériel, même appuyée d'une attestation du transmetteur (qu'il est actuellement rare de pouvoir se procurer) ne prouvera toujours pas son arrivée et sa réception par le destinataire.

Le cas de figure est bien connu des juristes depuis la généralisation de l'usage du fax, et la double solution a pour nom redondance et accusé de réception : le message important sera doublé d'une version « par courrier ordinaire » (même si ce dernier est susceptible en fait des mêmes critiques) ou, et c'est bien mieux, assorti d'une demande d'accusé de réception, reproduisant, si possible, le message transmis.

L'usage de pareille procédure sécurise au maximum la transmission, mais n'est pas sans inconfort si on ne confie pas à un processus informatisé, d'un côté, la capture du message reçu, de l'autre, le collationnement à l'original du message retourné.

On se demande si la technologie actuelle ne permet pas de réaliser aisément l'objectif recherché. On songe, en particulier, au recours à un tiers indépendant chargé de certifier la réception par le destinataire d'un message jugé particulièrement important. Ainsi, l'émetteur disposerait d'une preuve que son message a été effectivement envoyé et réceptionné. Une voie à explorer serait l'instauration d'un système de certification de la réception de messages électroniques, comparable à ce qui existe en matière de courrier postal, à savoir le recommandé avec accusé de réception. Nous verrions assez naturellement la Poste offrir un tel service. Ou pourquoi pas Isabel ?

Section 4. – *La sécurité vis-à-vis de l'extérieur*

1.1. – *Les précautions d'usage*

Par la force des choses et des réelles facilités qui en découlent, l'informatique du bureau s'est ouverte à la communication à l'extérieur, par télébanking, intranet, extranet ou internet, sans que l'on se protège ou s'interroge sur la possible inversion du rapport : si je puis envoyer et recevoir à mon gré, je m'expose au même transit à mon insu, voire contre ma volonté et non sans risques, que cela s'appelle virus, prises de profil, messages non désirés, piratage ou intrusions dans mon outil de travail.

Ici aussi, les solutions sont connues : d'une part, l'usage d'un anti-virus à jour est une nécessité, d'autre part, le poste branché sur l'extérieur doit rester vide de tout contenu sensible et physiquement coupé de toute connexion avec le restant du matériel, ou, si l'organisation du bureau requiert qu'il soit en réseau interne, être pourvu d'un « coupe-feu » (*firewall*)

efficace. Cela étant, grâce à la mise en place de pareils « murs de sécurité » par le gestionnaire du réseau Isabel, les notaires sont prémunis contre les intrusions et « attaques » de tous ordres de la part des usagers de l'Internet ne disposant pas d'un abonnement à Isabel.

1.2. – *Le législateur au secours du notaire*

Un projet de loi sur la criminalité informatique, voté à la Chambre le 31 mars 2000 et transmis au Sénat, définit quatre nouvelles incriminations (16). Rien n'interdit d'espérer que cette future loi sera de nature à dissuader les « hackers », fraudeurs et autres malveillants. Un texte susceptible de rassurer notamment les notaires!

Sans entrer dans le détail, bornons-nous à commenter brièvement ces nouveaux délits spécifiques : le faux en informatique, la fraude informatique, l'accès non autorisé et le sabotage de données et/ou de systèmes.

Le premier délit cité vise la manipulation de données informatiques en vue de leur falsification et de la modification de leur portée juridique : confection de fausses cartes de crédit ou de paiement, faux contrats numériques, *etc.* La fraude informatique est celle réalisée au moyen d'un système informatique, telle que l'utilisation d'une carte de crédit volée à des fins de retrait de fonds, l'obtention pour soi-même ou pour autrui d'un avantage financier illicite par l'introduction d'instructions informatiques pour modifier ou effacer des données qui y sont stockées ou modifier l'utilisation possible des données, le détournement de fichiers ou de programmes. L'accès non autorisé vise non seulement le « hacking » externe, perpétré par des tiers à l'organisation, mais aussi le « hacking » interne, perpétré par des personnes qui bénéficient en principe d'un accès à une partie du réseau, mais outrepassent leurs pouvoirs. Une intention frauduleuse ou un but de nuire est nécessaire au hacker interne, tandis qu'aucune intention particulière n'est requise dans le chef du hacker externe. Enfin, est également

(16) Projet de loi relatif à la criminalité informatique, Texte adopté en séance plénière et transmis au Sénat, *Doc. parl.*, Ch. R., sess. ord. 1999-2000, n° 0213/007.

puni le sabotage, la destruction ou l'endommagement de données et/ou de systèmes, la diffusion de virus. On ajoutera que le projet de loi prévoit diverses mesures visant à renforcer les moyens d'investigation du parquet et du juge d'instruction.

En conclusion

La description des risques liés au document informatique renvoie largement le notaire à ses responsabilités traditionnelles.

Plus que jamais, si elles sont « en ligne », il lui appartient de consulter, mais aussi de contrôler, les sources à sa disposition. Parfois, de les recouper, toujours de veiller à la fraîcheur des données, à la persistance de leur validité au moment de leur usage.

Le champ – ou, mieux, les facettes – de la diligence due par le notaire se trouve étendu du fait de l'usage de l'outil informatique dans sa pratique quotidienne. Il est tenu naturellement d'y faire recours en notaire prudent et diligent. Nous avons largement illustré tous les avatars qui peuvent résulter d'un mauvais usage, par le notaire, des moyens informatiques. Ainsi sera-t-il particulièrement attentif à s'entourer des précautions que l'on est en droit d'attendre d'un notaire prudent et diligent 1° quant au mode de conservation de la preuve des documents électroniques (archivage des messages échangés dans des conditions de sécurité garantissant leur intégrité), 2° quant à la fiabilité des systèmes de traitement et moyens informatiques mis à sa disposition, 3° quant à l'usage des nouvelles formes de signature.

La prévention des risques liés au document informatique se déclinera sur deux axes majeurs :

1° L'outil informatique, en toutes ses applications dans les études, ne peut plus être subi, ou simplement assimilé à un substitut de ce qui s'est toujours fait. Il doit être pensé, organisé dans sa spécificité, dans ses réelles possibilités d'optimisation des tâches.

2° A peine d'en être absent, ou à tout le moins le parent pauvre, le notariat, de par sa vocation première, se doit

d'être un acteur incontournable des mutations en cours dans les domaines de la transmission sécurisée de messages, des consentements échangés à distance, des nouveaux modes de conservation, de la certification et, osons le dire, de l'authenticité toujours, mais sous des formes nouvelles.

SAMENVATTING

DE AANSPRAKELIJKHEID VAN DE NOTARIS ALS AUTEUR, ONTVANGER OF GEBRUIKER VAN HET INFORMATICADOCUMENT

Informatica wordt steeds belangrijker in notariskantoren. De geautomatiseerde behandeling van informatie heeft zeker verschillende voordelen (gemak en snelheid van het methodisch gebruik van informatie, verminderen van steeds terugkerende taken, gemak van beheer en van ordening...). Maar deze behandeling van informatie veroorzaakt ook verwikkelingen van technische aard of gebonden aan een verkeerd gebruik van de apparatuur. Dit onderzoek nodigt uit tot nadenken over de nieuwe aspecten van de aansprakelijkheid van notarissen, die voortvloeien uit het gebruik in hun dagelijkse activiteit van informatica en netwerken. De beschrijving van deze risico's leidt de notaris in ruime mate terug naar zijn traditionele verantwoordelijkheid. Zo moet hij bij het gebruik van informatica en datacommunicatie er zeer nauwlettend op toezien dat hij de voorzorgen neemt die men mag verwachten van een voorzichtige en toegewijde notaris 1° wat betreft de wijze van bewaring van de elektronische documenten (archivering van uitgewisselde boodschappen in veiligheidsvoorwaarden die hun volledigheid waarborgen), 2° wat betreft de betrouwbaarheid van de informatiebehandeling – en informaticasystemen die hem ter beschikking gesteld worden, 3° wat betreft het gebruik van de nieuwe vormen van handtekening.

Een goede risicovoorkoming op dit vlak vereist in het algemeen dat de verschillende informaticatoepassingen niet louter ondergaan worden of gewoon geassimileerd worden met de gangbare procedures, maar uitgedacht en georganiseerd worden wat betreft hun bijzondere kenmerken en zo goed mogelijk geoptimaliseerd worden.

Het notariaat dient ook zijn kans te grijpen en creativiteit aan de dag te leggen om zich te profileren als een onmisbare actor bij de veranderingen die aan de gang zijn op het gebied van de beveiligde overdracht van boodschappen, de uitwisseling van toestemmingen op afstand, de nieuwe wijzen van bewaring van informatie, de echtverklaring en – waarom niet? – op het gebied van de authenticiteit, maar in nieuwe vormen.