De la lecture croisée à une réflexion commune juriste/informaticien*

Illustration, autour des virus informatiques et de la notion d'intégrité

Isabelle de Lamberterie** et Marion Videau***

CNRS CECOJI
27, rue Paul Bert
94204 Ivry-sur-Seine cedex
{delamberterie, marion.videau}@ivry.cnrs.fr

Résumé Cet article résulte de la confrontation des lectures que peuvent avoir des chercheurs en droit et en informatique sur les textes juridiques qui concernent la sécurité informatique. Nous considérons deux exemples. Le premier porte sur l'article 323-3-1 du code pénal — pouvant concerner, par exemple, toute personne s'intéressant aux failles de sécurité et aux virus. Dans le second exemple, nous nous interrogeons sur la notion d'intégrité dans le cadre des article 1316 et suivants du code civil définissant l'écrit dit *électronique* ainsi que les conditions de sa conservation et de sa signature.

1 Introduction

Lorsque l'informatique est passée d'un domaine réservé à une minorité de chercheurs et d'amateurs à une réalité quotidienne pour une majorité, il a nécessairement fallu prendre en compte la dimension *publique* de l'informatisation croissante. Il est indéniable que la massification a mis au jour des vulnérabilités amplifiées par le passage à l'échelle. Cette vulnérabilité conjointement à laquelle s'est développée l'informatisation s'est accompagnée du développement de réponses de sécurité informatique. Si celles-ci comportent inévitablement un aspect technologique, les techniques d'*ingénierie sociale* mettent régulièrement en évidence qu'elles ne peuvent être réduites à cette dimension. Ainsi, la prévention et la gestion de la vulnérabilité passent également par une prise en compte du facteur humain au travers d'une régulation qui peut-être *bottom-up* : chartes et autres codes de bonne conduite, ou *top-down* : textes législatifs ou réglementaires. Nous nous intéressons dans cet article à une confrontation des lectures que

* Cet article résulte de la collaboration menée dans le cadre du projet *Asphalès* de l'ACI Sécurité et Informatique.

** Directrice de recherche au CNRS-CECOJI.

*** Attachée temporaire d'enseignement et de recherche à l'Institut Gaspard Monge de l'université de Marne-la-Vallée, rattachée également au CNRS-CECOJI, chercheur extérieur au projet Codes de l'INRIA-Rocquencourt.

peuvent avoir des chercheurs en droit et en informatique sur les textes juridiques qui concernent la sécurité informatique. En effet, la régulation doit faire face à la prise en compte des caractéristiques intrinsèques au nouveau domaine qu'elle vise à réglementer, prise en compte qui ne va pas sans paradoxes quand les cultures et interprétations sont différentes.

La première partie de l'article concerne la recherche en sécurité informatique. La culture dans ce domaine est celle d'une confrontation permanente attaquant-attaqué[1], comme l'illustre par exemple l'évaluation de la sécurité d'un système de chiffrement. Des lois telles que celle visant à interdire la détention ou la mise à disposition de certains types de programmes[2] témoignent d'une certaine méconnaissance et incompréhension des mécanismes de recherche dans ce domaine, où la transposition de mesures de sécurité *physique* à la sécurité *logique* pourrait se révéler particulièrement inappropriée. Elles rendent bien incertaines les activités d'une communauté dont les contours, souvent flous, sont bien plus larges que la seule communauté académique[3].

Le deuxième sujet que nous allons traiter concerne les caractéristiques exigées de l'écrit dit *électronique* pour lui reconnaître une valeur juridique et une force probatoire dans le cadre d'échanges à court terme et sur le long terme. Que signifie la notion d'intégrité dans les domaines juridique et informatique ? Quelles sont les conséquences de ces différences d'interprétation ? Peut-on espérer concilier ce que permet et ne permet pas l'informatique avec ce dont la loi a besoin à travers l'écrit ?

2 Détention ou mise à disposition de virus informatiques

2.1 Le contexte législatif [4]

Dans la loi pour la confiance dans l'économie numérique, le législateur a voulu renforcer l'arsenal répressif en enrichissant le code pénal d'un nouvel article (323-3-1) visant directement la détention et la mise à disposition *d'équipements* conçus pour commettre les faits d'intrusion dans un système ou d'entrave au fonctionnement de ce système : « Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour

[1] « une logique bouclier/glaive sans doute durable » comme le souligne le rapport *Mesures techniques de protection des œuvres & DRMS* établi par Philippe Chantepie et disponible sur `http://www.culture.gouv.fr/culture/cspla/Mptdrms.pdf`

[2] Article 323-3-1 du code pénal, qui ne se limitent d'ailleurs nullement à cet aspect, voir ci-après.

[3] La seule dont il semblerait que les activités soient explicitement mises hors de cause, par un avis et non directement par le texte de loi.

[4] Une partie de cette présentation du contexte législatif est tirée d'une contribution d'I. de Lamberterie (Lecture juridique de la sécurité informatique) à une encyclopédie de l'informatique et des systèmes d'information à paraître, Vuibert, 2006.

l'infraction la plus sévèrement réprimée » [5]. Cette nouvelle infraction permet, par exemple, de sanctionner la détention d'un virus informatique avant que le virus n'ait été introduit frauduleusement dans un système informatique. Comme le fait remarquer le sénateur Alex Türk[6] dans son rapport[7], la comparaison peut être faite avec une disposition du code monétaire et financier qui punit « le fait de détenir, d'offrir, de céder ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données conçues ou spécialement adaptés pour commettre les délits de contrefaçon ou de falsification de cartes de paiement » [8]. Afin de permettre — entre autres — aux laboratoires en informatique de poursuivre leur recherche en sécurité informatique, le projet de loi initial limitait le champ d'application de l'infraction : celle-ci n'était pas applicable « lorsque la détention, l'offre, la cession et la mise à disposition de l'instrument, du programme informatique ou de toute donnée » pouvaient être justifiées par les besoins de la recherche scientifique et technique ou de la protection et de la sécurité des réseaux de communications électroniques et des systèmes d'information[9].

Lors des débats parlementaires, les notions de *besoins de la recherche scientifique et technique* ou de *protection de la sécurité des réseaux de communication* ont été qualifiées de particulièrement imprécises, susceptibles de recouvrir des organismes irréprochables et d'autres qui le seraient moins, certains pouvant être tentés de développer des virus informatiques en excipant de leur mission de sécurisation des réseaux[10]. Prenant en compte ces arguments, le Sénat a proposé la suppression du deuxième alinéa et l'introduction dans l'article 323-3-1 de la mention *sans motif légitime*. C'est ce qui a été retenu dans le texte de la loi. Pour mieux comprendre ce qu'il faut entendre par *motif légitime*, il faut se rapporter aux commentaires du sénateur Alex Türk qui précise que la recherche scientifique et la sécurisation des réseaux pourraient, naturellement, entrer dans le champ des motifs légitimes. Il reviendra, bien entendu, au juge d'apprécier la légitimité des motifs, dès lors qu'il est impossible dans la loi d'envisager toutes les hypothèses dans une telle matière. Le juge appréciera cette légitimité sur la base des preuves qui lui seront apportées par celui qui cherche à justifier qu'il entre dans l'exception à l'article 323-3-1, preuve difficile à rapporter comme nous le montre la lecture suivante de l'article.

2.2 Analyse de l'article 323-3-1 du code pénal

L'article 323-3-1 du code pénal a naturellement suscité beaucoup d'inquiétude dans la communauté informatique jusqu'à récemment peu habituée à une telle

[5] voir annexes.

[6] Également président de la Commission nationale de l'informatique et des libertés depuis le 3 février 2004.

[7] Avis n° 351 du sénateur Alex Türk, p. 133.

[8] Article L. 163-4-1 du Code monétaire et financier.

[9] Avis n° 351 du sénateur Alex Türk, précité, p 134.

[10] Avis n° 608 de Madame Michèle Tabarot, député, au nom de la commission des lois, 11 février 2003.

sollicitude de la part du législateur. Nul doute qu'avec un filet aux mailles aussi petites les auteurs d'actes malveillants ne sauraient échapper à tout le moins à la qualification de leurs actes. Néanmoins, même un chercheur en sécurité, normalement hors de cause, en viendrait rapidement à se demander si toute personne faisant preuve d'un tant soit peu de curiosité ne serait pas alors susceptible de tomber sous le coup de cet article. C'est tout le paradoxe de lois qui traitent de la sécurité *logique* comme elle le ferait de la sécurité *physique*, semblant négliger qu'avoir accès à un système n'admet aucun équivalent strict avec avoir accès à un lieu et qu'ériger des barrières à la réflexion n'est peut être pas la mesure la plus adaptée.

Cadre de lecture du texte par un chercheur en informatique[11] Les articles 111-4 : « La loi pénale est d'interprétation stricte. » et 121-3 : « Il n'y a point de crime ou de délit sans intention de le commettre. [...] » du code pénal constituent le contexte dans lequel l'expression *motif légitime* devrait protéger tous ceux qui agissent de bonne foi mais sur qui pèse néanmoins la charge de la preuve. Il reviendra ainsi au juge d'interpréter de manière stricte ce qu'une lecture attentive des articles ne peut manquer de faire apparaître comme exceptionnellement large et flou.

Une première interrogation sur les délits Reprenons la lecture méthodique des articles du code pénal et les quelques questions qu'ils soulèvent *naturellement*. Nous pouvons formuler une première remarque ; il semblerait que l'article 323-1 traite explicitement le cas d'un accès frauduleux suivi de conséquences. Les autres articles traitent des mêmes conséquences sans faire mention d'un accès frauduleux. Il semblerait donc qu'il faille entendre que les autres cas sont plus sévèrement punis. L'article 323-2 soulève en outre la question entière de son interprétation[12] : le terme *frauduleux* en est absent et rien ne précise à qui appartient le système.

Les interrogations portent sur les termes « système de traitement automatisé de données ». S'il est aisé de comprendre qu'ils visent à recouvrir d'une certaine manière toute la réalité informatique, la difficulté à définir explicitement ce qu'est le « système », qu'il soit physique, logique, un logiciel, une machine, un réseau, etc. nous conduit aux questions suivantes :

– Que signifie accéder ou se maintenir dans tout ou partie d'un système de traitement automatisé de données ? Il n'y a en effet aucun parallèle possible avec le monde physique où la question de s'introduire dans un domicile est, par exemple, parfaitement compréhensible. Cela peut-il signifier

[11] La lecture qui suit s'ajoute à de nombreux commentaires, tant de juristes que d'informaticiens, suscités par l'article 323-3-1 du code pénal depuis la parution de la LCEN en 2004. Elle ne vise donc pas à une simple accumulation mais plutôt à mettre en valeur une démarche de recherche qui consiste, pour un chercheur en informatique, à se pencher sur le droit qui s'applique à son domaine afin de participer à la construction du droit positif.

[12] Sont visées, par exemple, les attaques du type déni de service.

s'authentifier correctement auprès d'une (ou plusieurs) machine(s), utiliser une application qui s'exécute sur une (ou plusieurs) machine(s), utiliser des données enregistrées sur une (ou plusieurs) machine(s), etc. ?
- Quel est l'auteur qui sera retenu ? En effet, les actions précédentes peuvent aussi bien être exécutées par des applications. Qui rendre responsable en bout de chaîne ? L'utilisateur dont l'application a lancé l'application qui a lancé l'application (et ainsi de suite) contrevenante, l'administrateur du réseau d'où provient le délit, le fournisseur d'accès qui fournit la connexion ? Comment mettre en évidence l'*intention* de commettre de tels délits ? Doit-on pour cela évaluer la quantité de connaissance informatique d'une personne, ou lui fait-on grief de ne pas savoir en invoquant une « faute d'imprudence » ?
- Comment identifie-t-on l'unité d'un système : machine, réseau, partition, processus ? Quel est en le propriétaire ? Cela pourrait-il signifier, l'interdiction de toute action *personnelle* sur des biens *personnels* (console de jeu, logiciels, etc.) légalement acquis et soumis à une expertise par ses propres soins ? En effet, la tendance actuelle semble très clairement considérer qu'il serait bon que le possesseur n'ait pas accès au *contenu* de ces biens[13]. Cet accès est-il ainsi *frauduleux* ?
- Enfin, comment juge-t-on du caractère frauduleux ? Que faire dans la situation d'un nom d'utilisateur et d'un mot de passe évidents, par exemple ?

On est ainsi amené à se demander comment, à partir d'une réalité informatique que l'on cherche à définir comme un délit, est obtenue la définition du délit et d'autre part quel est l'ensemble des réalités informatiques qui sont caractérisés par les définitions ainsi obtenues. Cette dernière question se pose avec force dans le cas de l'article 323-3-1.

Lorsque la potentialité du délit devient un délit Nous revenons maintenant à l'article qui concerne l'amont des délits précédents. Ce ne sont plus les conséquences qui sont répréhensibles, mais la détention et la mise à disposition. On pourrait également faire un parallèle avec les armes à feu dont la détention et la mise à disposition est réglementée. Avec ce seul parallèle, nul doute que la loi semble totalement justifiée et raisonnable. Or la vocation première d'une arme à feu est bien de tirer. C'est un objet matériel à *finalités circonscrites*. La situation est complètement différente avec ce que décrit la loi : « un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour [...] ». L'ensemble des finalités d'un tel ensemble est si vaste et largement ambivalent qu'elle mène à une alternative simple : soit un article qui proscrit indistinctement pour cause de finalités n'ayant pas de motif légitime, soit un article inapplicable pour cause de motif légitime, qu'il est toujours possible de trouver.

[13] On peut faire un parallèle avec un livre qu'on n'aurait pas le droit de lire, dont on ne pourrait parler des techniques d'écriture ni faire aucune critique. La comparaison s'enrichit en outre de la réflexion qui suit sur l'écrit et la lecture.

Ainsi, qu'est ce qu'une « donnée conçue ou spécialement adaptée pour [...] » ? Un livre décrivant des faiblesses de sécurité est-il une « donnée conçue ou spécialement adaptée pour [...] » ? Un article, une quelconque publication décrivant des failles de sécurité, sont-ils des objets de délit ? On ne peut répondre à ces questions par la négative que s'il est possible d'arguer d'un *motif légitime*.

À quelle aune juger de la légitimité du motif de la possession de tels objets ? En effet, soit l'auteur d'une telle expression avait pour intention de protéger la recherche, il doit ainsi considérer que la curiosité est un *motif légitime* — motif qui peut être invoqué par à peu près quiconque et rend ainsi la loi absolument sans objet — soit il n'entend pas considérer un tel motif comme systématiquement légitime et il reviendra aux jurisprudences d'en fournir une explication. Comment ne pas penser, par exemple, que la mise à disposition de n'importe quel « équipement », « instrument », « programme informatique » ou « toute donnée » a forcément au moins le motif légitime de permettre à quiconque d'éprouver la sécurité de son système informatique contre les attaques existantes ? À quel expert sera laissé le soin d'apporter l'avis qui conduira à considérer tel ou tel motif comme légitime ou non ?

Si la volonté du législateur semble relativement claire — en quelque sorte *punir les pourvoyeurs* — l'opportunité d'un tel texte reste mystérieuse dès lors qu'il ne conditionne pas l'attribution de la qualité de délit à la lumière de l'usage qui est fait d'un outil aux finalités multiples et intrinsèquement ambivalentes mais à la lumière d'un hypothétique motif de possession de cet outil, dont la légitimité doit être démontrée. Perplexité grandissante lorsqu'on prend en outre connaissance de l'article 323-7 : « La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines. »

3 La double caractérisation de l'intégrité

Cette expression, empruntée à J. F. Blanchette[14], est aujourd'hui une évidence pour tous ceux qui ont affaire avec les notions de garanties et de sécurité dans la conservation des documents informatiques. En effet l'intégrité vise la « Prévention d'une modification non autorisée de l'information. Garantie de la présence et de la conservation sans altération d'une information ou d'un processus » [15]. L'intégrité est aussi la caractéristique de l'absence de modifications des données constituant un document. « Assurer l'intégrité de données consiste à permettre la détection de leurs modifications volontaires, telles celles qui découlent de la possibilité informatique d'altérer physiquement des informations-données dans une mémoire et/ou d'y introduire des instructions ou algorithmes qui fassent échapper la machine au contrôle de son maître[16] ».

[14] Jean-François Blanchette, « Modernité et intelligibilité du droit de la preuve français », Communication Commerce électronique, n° 3, mars 2005, pp. 21-26.

[15] `http://www.step-sa.fr/glossaire.html`

[16] `http://www.fsa.ulaval.ca/personnel/vernag/EH/F/cons/lectures/Glossaire\%20de\%20la\%20cyberguerre.htm`

3.1 Intégrité et sécurité juridique

En droit, il est aujourd'hui question d'intégrité dans la loi sur la preuve. Cette notion y est apparue comme le condensé des qualités attendues d'un écrit signé traditionnel : durabilité, fidélité et fiabilité. La valeur probatoire d'un écrit électronique dépend des conditions de son établissement et de sa conservation de nature à en garantir l'intégrité[17]. Il est encore question d'intégrité à propos de la signature électronique : « Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État » [18]. Que veut dire garantir l'intégrité ? L'une des finalités de la signature électronique n'est-elle pas d'apporter cette garantie ? Peut-elle encore le faire quand les migrations périodiques indispensables pour garantir la lisibilité du document peuvent remettre en cause le processus de vérification de signature ? Ce sont autant de questions qui requièrent les compétences du spécialiste de la sécurité informatique.

3.2 Intégrité et sécurité informatique

Un point important à soulever avant même de parler de l'intégrité d'un écrit *électronique* est celui de la nature de cet écrit[19]. L'article 1316 du code civil définit ainsi : « La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission ». La loi indique donc que toute suite de symboles intelligibles, directement ou indirectement, donc par exemple binaires, quel que soit le support, est un écrit, et ce sans discrimination de ce qui est représenté sous cette forme. Ainsi, d'un écrit qui dans l'acception courante est entendu comme le rendu visible d'un traitement de texte (par exemple) la loi reconnaît la valeur d'écrit à toute suite binaire. Dans ce sens, un programme exécutable, disponible seulement sous sa forme de fichier dit *binaire* est donc un écrit, ainsi qu'un enregistrement audio ou vidéo numérique. Aussi, compris dans ce sens, le problème de l'intégrité de l'écrit dit *électronique* renvoie-t-il au problème traditionnel de l'intégrité en informatique, c'est-à-dire du caractère de données numériques qui restent identiques (par rapport à une source ou par rapport à un état antérieur) quelles que soient les manipulations auxquelles elles sont soumises. La vérification

[17] Article 1316-1 du Code civil

[18] Art 1316-4 in fine.

[19] Notons qu'en informatique on parle plus volontiers en terme de *numérique* plutôt que d'*électronique*. Le premier adjectif se rapporte à la représentation de l'information grâce à un alphabet particulier, alors que le second est relatif à l'utilisation de matériel électronique (ce qui est tout aussi bien le cas de plaques de cuisson que d'un ordinateur).

de cette propriété est dévolue à différents algorithmes, selon les propriétés, cryptographiques ou non, attendues (cheksum, CRC, MAC, fonctions de hachage, signature, etc.).

Plusieurs questions délicates viennent à se poser lorsqu'on considère le procédé cryptographique de signature, venant mettre en doute le fait que l'intégrité telle qu'attendue par la loi se résume à l'intégrité informatique. En effet, à redéfinir l'écrit, il faut aussi redéfinir la lecture. Ainsi, que devra-t-on signer ? Une telle question s'impose lorsqu'on prend en compte le fait qu'aucun fichier n'est autosuffisant en lui-même pour l'accès au contenu écrit. Il y a en fait deux lectures successives : la première est effectuée par l'ensemble {ordinateur, système d'exploitation, logiciels} à partir d'un contenu fixé sur un support numérique, la seconde est la perception par un être humain du rendu du premier ensemble. La difficulté principale de la question de l'intégrité réside dans le fait que l'informatique porte son attention à l'écrit avant la première lecture (un fichier), alors que le droit s'intéresse au résultat de cette lecture (ce qui est visible à l'écran par exemple). Faudrait-il alors signer l'ensemble {fichier, {ordinateur, système d'exploitation, logiciels}}[20] pour parvenir aux mêmes caractéristiques que l'écrit traditionnel ? Cela n'est pas envisageable dans la pratique. Il faut donc pouvoir s'assurer de la fiabilité de la transformation effectuée par cette première lecture, fiabilité qui exige des formats ouverts et pérennes associés à des logiciels parfaitement spécifiés.

Par ailleurs, des questions complémentaires apparaissent concernant la signature cryptographique : quelle est l'exigence de sécurité que requiert la loi et pour quelle durée ? En effet, un procédé de signature cryptographique ne peut être réputé fiable qu'en l'état actuel des connaissances et de la puissance des ordinateurs. Rien ne le met à l'abri d'une avancée théorique, de la découverte d'une faille, et de l'accroissement continu de la puissance des ordinateurs. Il faut en outre souligner le changement qualitatif des risques liés à la possibilité de produire un faux. La capacité de production d'un ordinateur est en effet sans commune mesure avec celle d'un faussaire humain. En revanche, la difficulté à produire le premier faux est bien plus importante pour la signature cryptographique que pour la signature manuscrite.

3.3 Les points de divergence et de convergence

La médiation des archivistes, les spécialistes de l'archivage[21], apportent aujourd'hui des éclairages pour appréhender la notion d'intégrité et définir des politiques pertinentes d'établissement et de conservation. Ils se placent sur trois terrains complémentaires : tout d'abord celui d'une remise en cause du lien entre *intégrité physique* et *authenticité* du document. Même si la chaîne de bits est

[20] Sans compter la source d'énergie nécessaire que ne requiert pas l'écrit traditionnel.

[21] On renverra, entre autres, aux travaux du programme Interpares qui vise à déterminer les principes archivistiques pertinents à la conservation de documents électroniques authentiques. Il regroupe des représentants de nombreuses archives nationales. Voir le site `http://www.interpares.org`.

modifiée, ces modifications ne suffisent pas pour remettre en cause l'authenticité du document. Pour Interpares, « il n'est pas possible de conserver un écrit électronique en tant qu'objet physique entreposé. Il est seulement possible de préserver un document manifeste » [22] ; ensuite, il faut distinguer « authenticité d'un document qu'il soit ou non électronique » d'une part et *l'authentification* de la signature électronique d'autre part. L'authentification de la signature électronique doit être entendue dans son sens technique se limitant aux moyens mis en œuvre pour atteindre l'identification alors que l'archiviste vérifiera au sens juridique l'authentification d'un document (identification et adhésion au contenu d'un acte). La signature n'est alors qu'un élément parmi d'autres qui permet d'apprécier la valeur probatoire d'un document. Enfin, pour les archivistes, c'est sur le respect de la chaîne de préservation que s'apprécie l'authenticité d'un document, cette chaîne étant *l'ensemble des contrôles et des procédures qui assurent l'identité et l'intégrité d'un document au travers de la totalité de son cycle de vie.*

On trouve aujourd'hui une autre réponse dans le résultat de la coopération entre juristes et informaticiens qui a permis d'aboutir à la recommandation du Forum des Droits sur l'Internet[23] ; trois critères doivent être cumulativement réunis par le processus de conservation :

- la lisibilité du document ;
- la stabilité du contenu informationnel ;
- la traçabilité des opérations sur le document.

La lisibilité désigne la possibilité d'avoir accès, au moment de la restitution du document, à l'ensemble des informations qu'il comporte. Cette démarche est facilitée par les méta-données associées au document. La stabilité du contenu informationnel désigne la nécessité de pouvoir garantir que les informations véhiculées par le document restent les mêmes depuis l'origine et qu'aucune n'est omise ou rajoutée au cours du processus de conservation. Le contenu informationnel s'entend de l'ensemble des informations, quelle que soit leur nature ou leur origine, issues du document et, le cas échéant, de sa mise en forme. La traçabilité désigne la faculté de présenter et de vérifier l'ensemble des traitements, opérés sur le document lors du processus de conservation.

4 Conclusion

L'informatique et ses développements modifient profondément le paysage de la société. La nature de ces bouleversements ainsi que l'accélération de leur rythme font de la coopération entre spécialistes du droit et de l'informatique une nécessité qui doit s'inscrire dans le souci des rapports entre science, technologie et société et de l'inter-disciplinarité. Les conditions de succès d'une telle entreprise passe par l'écoute mutuelle et la compréhension des positionnements et

[22] Voir Duranti et al., « Strategy Task force Report » in The long term preservation of authentic electronic records : findings of the Interpares project, 2002, p. 4.

[23] `http://www.foruminternet.org/telechargement/documents/reco-archivage-20051201.pdf`

des valeurs défendues par chacun. Le résultat en serait une régulation juridique mieux comprise, mieux appliquée, mieux interprétée ; une régulation capable d'évoluer en tenant compte des acteurs concernés. Le programme est ambitieux, c'est l'affaire de tous.

Annexes : textes de lois cités

Code pénal
Livre III : Des crimes et délits contre les biens
Titre II : Des autres atteintes aux biens
Chapitre III : Des atteintes aux systèmes de traitement automatisé de données (Articles 323-1 à 323-7)

Article 323-1 *(Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002), (Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004)*

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

Article 323-2 *(Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002), (Loi nº 2004-575 du 21 juin 2004 art. 45 II Journal Officiel du 22 juin 2004)*

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3 *(Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002), (Loi nº 2004-575 du 21 juin 2004 art. 45 III Journal Officiel du 22 juin 2004)*

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3-1 *(inséré par Loi nº 2004-575 du 21 juin 2004 art. 46 I Journal Officiel du 22 juin 2004)*

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique

ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-4 *(Loi n° 2004-575 du 21 juin 2004 art. 46 II Journal Officiel du 22 juin 2004)*

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 323-5 Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1. L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
2. L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
3. La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4. La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5. L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6. L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
7. L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

Article 323-6 Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre. Les peines encourues par les personnes morales sont :

1. L'amende, suivant les modalités prévues par l'article 131-38 ;
2. Les peines mentionnées à l'article 131-39. L'interdiction mentionnée au 2 de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 323-7 *(Loi nº 2004-575 du 21 juin 2004 art. 46 II Journal Officiel du 22 juin 2004)*

La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

Code civil
Livre III : Des différentes manières dont on acquiert la propriété
Titre III : Des contrats ou des obligations conventionnelles en général
Chapitre VI : De la preuve des obligations et de celle du paiement (Articles 1315 à 1315-1)
Subsection 1 : De la preuve littérale
Paragraphe 1 : Dispositions générales (Articles 1316 à 1316-4)

Article 1316 *(Loi nº 2000-230 du 13 mars 2000 art. 1 Journal Officiel du 14 mars 2000)*

La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.

Article 1316-1 *(inséré par Loi nº 2000-230 du 13 mars 2000 art. 1 Journal Officiel du 14 mars 2000)*

L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

Article 1316-2 *(inséré par Loi nº 2000-230 du 13 mars 2000 art. 1 Journal Officiel du 14 mars 2000)*

Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support.

Article 1316-3 *(inséré par Loi nº 2000-230 du 13 mars 2000 art. 3 Journal Officiel du 14 mars 2000)*

L'écrit sur support électronique a la même force probante que l'écrit sur support papier.

Article 1316-4 *(inséré par Loi nº 2000-230 du 13 mars 2000 art. 4 Journal Officiel du 14 mars 2000)*

La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent

de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.