INTRODUCTION AU DROIT DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (SSI)[1]

Éric A. CAPRIOLI

Rédiger une introduction au droit de la sécurité des systèmes d'information (SSI) constitue une gageure au regard, d'une part, des domaines juridiques en cause, et d'autre part, de la permanence des interactions du droit avec les aspects techniques et organisationnels. Alors que le droit repose sur les moyens techniques utilisés (ex. : procédés cryptographiques, adresses IP, traces ou écrits électroniques), les systèmes d'information de l'entreprise (ou de l'autorité administrative) doivent être conformes aux lois et règlements applicables. Le droit de la sécurité des systèmes d'information se caractérise par ses multiples facettes. On peut aisément lui transposer ce que disait le dédicataire des présents *Mélanges* à propos du droit de l'informatique : « essentiellement un droit "carrefour" (H. Maisl), car la technicité des ordinateurs retentit sur de nombreuses branches du droit »[2]. Il couvre tout autant le droit privé que le droit public voire, selon les hypothèses, autant le droit interne que le droit international. La dimension juridique se décline à travers diverses branches du droit, notamment la protection des données à caractère personnel[3] et la vie privée, les contrats (formation, preuve, validité et exécution)[4], le droit du travail[5], les publications en ligne, les droits intellectuels, la réglementation

1. L'auteur tient à exprimer ses sincères remerciements à Me Pascal AGOSTI, avocat à la Cour (Caprioli et associés), et à Antoine GRAVEREAUX, élève avocat à l'EFB de Paris (stagiaire au cabinet Caprioli et associés), pour leur aide dans les recherches et la préparation du présent article.

2. X. LINANT DE BELLEFONDS, *L'informatique et le droit*, Paris, PUF, 4e éd., 1998, p. 7.

3. CNIL, délib. n° 2006-174 du 28 juin 2006, *Première sanction pécuniaire de la CNIL : une banque à l'amende ! : RD bancaire et financier* sept.-oct. 2006, p. 30 et s., note E. A. CAPRIOLI. – Cass. crim., 14 mars 2006 : *RD bancaire et financier* juill.-août 2006, p. 24 et s., note E. A. CAPRIOLI.

4. Cass. 1re civ., 27 juin 2006 : *Comm. com. électr.* oct. 2006, p. 51 et s., note E. A. CAPRIOLI. – Haute Cour de justice anglaise, 7 avr. 2006 : *Comm. com. électr.* juin 2006, p. 43 et s., note E. A. CAPRIOLI. – Cass. com., 4 oct. 2005 : *RD bancaire et financier* mai-juin 2006, p. 35 et s., note E. A. CAPRIOLI.

5. TGI Vannes, 13 juill. 2005 : *Comm. com. électr.* avr. 2006, p. 41 et s., note E. A. CAPRIOLI. – CA Rouen, 3 mai 2005 : *Comm. com. électr.* janv. 2006, p. 43 et s., note E. A. CAPRIOLI. – C. prud. Nanterre, 15 sept. 2005 : *RD bancaire et financier* mars-avr. 2006, p. 31 et s., note E. A. CAPRIOLI. – Cass. soc., 17 mai 2006 : *RD bancaire et financier* sept.-oct. 2006, p. 28 et s., note E. A CAPRIOLI.

de la cryptologie, les paiements électroniques ou la criminalité informatique[6]. La liste est longue et n'a d'intérêt que par les principes que l'on peut en extraire.

La transversalité du sujet s'explique par la place considérable de l'informatique[7] dans notre vie quotidienne, que ce soit dans la vie des affaires, mais aussi sur notre lieu de travail ou à notre domicile. Qui n'utilise pas un traitement de texte pour rédiger ses documents, ou l'internet pour envoyer et recevoir des messages électroniques, rechercher et échanger des informations ? L'informatique et plus largement les technologies de l'information et de la communication (TIC) sont donc consubstantielles de l'essor de notre société postindustrielle et dont l'unité de valeur est l'information[8]. Ne parle-t-on pas de la « Société de l'information »[9] ? Avec la numérisation de l'information, une nouvelle ère est arrivée, pour preuve les lois et ordonnances publiées de 2004 à 2006 (ex. : la Loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004).

L'information est devenue un enjeu majeur et l'une des principales richesses d'un État, d'une entreprise ou même d'une personne. Plusieurs significations peuvent être données à la notion d'« information ». Certains auteurs la rapprochent de la notion de communication mais aussi du dialogue qui comporte un échange de renseignement[10]. L'arrêté du 3 octobre 1984 du ministre de l'Éducation nationale et du ministre chargé des PTT, portant enrichissement du vocabulaire de télécommunications[11], la définit comme « un élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement ».

---

6. Cass. crim., 29 mars 2006 : *Comm. com. électr.* juill.-août 2006, p. 39 et s., note E. A. CAPRIOLI ; E. A. CAPRIOLI, *Les technologies de l'information et la lutte antiterroriste : Comm. com. électr.* mai 2006, p. 45.
7. J. HUET, *(Droit de l')Informatique et du multimédia.* Contribution au *Dictionnaire de la culture juridique*, PUF, 2003, sous la direction de D. ALLAIS et S. RIALS, p. 824 et s. Disponible sur : *www.jeromehuet.com.*
8. Selon le professeur Jérôme Huet, il est préférable de parler de droit de la communication plutôt que de droit de l'information, le terme étant trop large. V° *Droit de la communication*, in *Clé pour le siècle*, Université Panthéon-Assas/Paris II, Dalloz, 2000, p. 485.
9. Terme utilisé volontiers dans les directives de l'Union européenne pour faire référence à une nouvelle conséquence de la communication électronique, qui permet un accès plus ou moins illimité à des informations se trouvant n'importe où dans le monde. V. M. BANGEMANN, *La société de l'information : un modèle européen : DIT* 1998/3, p. 6 et s. V. la communication de la Commission au Conseil et au Parlement européen, *Vers la société de l'information en Europe : un plan d'action*, COM (94) 347 final et le rapport BANGEMANN, *L'Europe et la société de l'information planétaire, Recommandation au Conseil européen*, Bruxelles, 26 mai 1994. V. en matière économique, M. CASTELLS, *La société en réseaux (Ère de l'information*, t. I), Fayard, 1998. « La création, le traitement et la transmission de l'information deviennent les sources premières de la productivité. »
10. Dans ce sens : J.-M. AUBY et R. DUCOS-ADER, *Droit de l'information*, coll. précis Dalloz, 1re éd., Paris, Dalloz, 1976 et E. DARAGON, *Étude sur le statut juridique de l'information : D.* 1998, p. 63-68.
11. Arrêté du 3 octobre 1984 du ministre de l'Éducation nationale et du ministre délégué auprès du ministre du Redéploiement industriel et du Commerce extérieur, chargé des PTT, portant enrichissement du vocabulaire de télécommunications : *JO* 10 nov. 1984.

Présentée sous forme informatique, l'information est constituée de données ; une donnée est définie par l'arrêté du 22 décembre 1981 du ministre de l'Éducation nationale et du ministre de l'Industrie, relatif à l'enrichissement du vocabulaire de l'informatique, comme étant « la représentation d'une information sous forme conventionnelle destinée à faciliter son traitement ». C'est cette représentation de l'information qui peut être protégée. Ainsi, l'ensemble de ces données peut être traité sous forme de bases de données **protégeables**. L'article L. 341-1, alinéa 1, du Code de la propriété intellectuelle énonce ainsi que : « Le producteur d'une base de données, entendu comme la personne qui prend l'initiative et le risque des investissements correspondants, bénéficie d'une protection du contenu de la base lorsque la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain substantiel. » De sorte que la protection des données (et donc de l'information qu'elles véhiculent) se justifie aussi par l'investissement qui les concerne.

Selon le professeur Catala, « l'information est d'abord expression, formulation destinée à rendre un message communicable ; elle est ensuite communiquée, ou peut l'être, à l'aide du signe choisi pour porter le message à autrui » [12]. Si la représentation et la communication constituent deux des fondements de l'information, la sécurité permet sa protection et sa gestion : création, collecte, traitement, conservation et communication dans des conditions d'utilisation optimale.

Sécurité et Communication. Il s'agit là des fonctions essentielles des systèmes d'information (SI) : une information qui n'est pas communicable ne possède pas de valeur économique et/ou juridique ; une information qui n'est pas sécurisée peut être considérée comme source de risque car sujette à des atteintes diverses : altération, destruction, appropriation ou consultation indue. Les systèmes d'information sont devenus le système nerveux des organisations. La communication des informations doit s'opérer entre les acteurs avec des niveaux de sécurité adaptés à leurs besoins. La sécurité est étroitement imbriquée à la communication. Mais la sécurité des SI doit assurer la confidentialité des données et garantir le système contre les accès non autorisés. La sécurité des systèmes d'information a pour objectif d'assurer protection et garantie d'intégrité sur les données qui en font partie ainsi que sur celles des infrastructures matérielles et logicielles qui permettent leur mise en œuvre.

Sécurité et Confiance. Les deux notions sont intimement liées, notamment dans le domaine des communications électroniques. La notion de confiance est ainsi utilisée dans la terminologie du législateur presque comme un synonyme de sécurité. La loi pour la confiance dans l'économie numérique (LCEN [13]) est à cet égard exemplaire. Notons que la notion de confiance n'est pas définie en droit, à tout le moins l'est-elle négativement : l'abus de confiance se définit ainsi comme « le fait par une personne de détourner, au préjudice d'autrui, des fonds, des

12. P. CATALA, *Le droit à l'épreuve du numérique, jus ex machina*, Paris, PUF, 1994, p. 228.
13. Loi n° 2004-575 du 21 juin 2004 : *JO* 22 juin 2004, p. 11175 et s.

valeurs, ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé » (C. pén., art. 314-1), ou encore la perte de confiance en droit du travail. À l'heure actuelle, l'internet et les réseaux numériques inspirent encore de la méfiance, voire de la défiance chez certains internautes et parfois des incertitudes auprès des professionnels[14] : sécurité des transactions, contrats électroniques, cybercriminalité, piratage, virus, spamming, autant de sujets largement relayés par les médias. La confiance est l'élément-clé pour assurer le développement des échanges électroniques dans l'économie numérique.

Or, la confiance est une donnée essentiellement psychologique[15], elle se construit à la fois autour de la notion de sécurité, qu'elle soit juridique, technique ou organisationnelle, et de celle de responsabilité des acteurs de l'économie numérique. Tel était l'apport essentiel de la LCEN : associer un corps de règles juridico-techniques applicables à l'économie numérique à un régime de responsabilité rendu nécessaire par la spécificité de l'activité des divers intervenants (FAI, hébergeurs, fournisseurs de services de stockage temporaire, prestataires de services de certification électronique...)[16].

Sécurité et intelligence économique et stratégique. Les systèmes d'information doivent être considérés comme des outils stratégiques des entreprises. Des données commerciales, fournisseurs, clients, transitent ou demeurent sur les serveurs et leur espionnage industriel[17] constitue une pratique de plus en plus répandue dans le monde des affaires. Ceci explique, à tout le moins pour partie, pourquoi les entreprises recourent à des outils de sécurisation de leurs systèmes d'information et de leurs échanges.

Or Platon déjà dans la *République* s'interrogeait : « Qui garde les gardiens ? » En effet, que doit faire une entreprise vis-à-vis de son prestataire en charge de la maintenance ou du contrôle des matériels et logiciels de sécurité des systèmes d'information de la société dès lors qu'elle apprend que son capital est contrôlé par un de ses concurrents ?

---

14. V. sur le manque de confiance des consommateurs, Ch. HUARD, *Le consommateur et l'électronique : Rev. conc. consom.* 2001, n° 123, p. 22. V. égal. dans un autre registre : C. CARON, *Le consommateur en droit d'auteur :* in *Liber amicorum Jean Calais-Auloy*, Paris, Dalloz, 2003, p. 245 et s.
15. La notion de « confiance » qui peut prendre des formes très diverses est rapidement décrite en droit des contrats, de la responsabilité, en droit communautaire..., par E. A. CAPRIOLI, *Confiance et communications électroniques : éléments provisoires de réflexion juridique*, disponible à l'adresse : *http://www.fing.org/ref/confiance/Fing_Confiance_ECaprioli_260204.pdf* et sur le site : *http://www.caprioli-avocats.com.*
16. E. A. CAPRIOLI, P. AGOSTI, *La confiance dans l'économie numérique : LPA* 3 juin 2005, p. 4 et s.
17. « L'espionnage économique privé est le fait, pour une personne physique ou morale, de rechercher dans un but économique, pour soi ou pour autrui, de manière illégitime – c'est-à-dire le plus souvent à l'insu et contre le gré de son détenteur – des informations techniques ou de toute nature lorsque ces informations présentent une valeur, même potentielle, dont la divulgation serait de nature à nuire aux intérêts essentiels de ce dernier. » J. DUPRÉ, *Pour un droit de la sécurité économique de l'entreprise, de l'espionnage industriel à l'intelligence économique*, thèse, Nice, 2000, introduction, p. VI.

La sécurité des systèmes d'information constitue un domaine sensible dans lequel les investissements d'entreprises étrangères sont réglementés conformément à l'article L. 151-3 du Code monétaire et financier, modifié par le décret n° 2005-1739 du 30 décembre 2005 pris en application de ce nouvel article L. 151-3 du Code monétaire et financier[18]. La France commence à découvrir le « patriotisme économique », expression bien connue en pratique dans des pays comme les États-Unis d'Amérique ou la Chine, par exemple.

La sécurité des systèmes d'information constitue l'un des domaines d'application de l'intelligence économique. Elle s'entend de « l'ensemble des actions coordonnées de recherche, de traitement et de distribution en vue de son exploitation, de l'information utile aux acteurs économiques. Ces diverses actions sont menées légalement avec toutes les garanties de protection nécessaires à la préservation du patrimoine de l'entreprise dans les meilleures conditions de qualité, de délais et de coûts »[19]. Au regard de cette définition, l'intelligence économique doit être considérée notamment comme une méthode de veille concurrentielle et technologique, voire d'influence ou de lobbying. Or, l'intelligence peut également être juridique. Dans ce cas, **il s'agit de la maîtrise, de la valorisation et de la protection du patrimoine informationnel appartenant à une entité publique ou privée par la mise en place de procédés légaux, réglementaires, contractuels ou organisationnels**[20]. Ainsi, les actions relatives à l'intelligence juridique peuvent être préventives ou offensives.

Sécurité et État. La sécurité a longtemps été liée aux missions régaliennes de l'État, en matière militaire, diplomatique et gouvernementale. Cette mission se poursuit sur les réseaux numériques. Tel est le rôle de la Direction centrale de la sécurité des systèmes d'information (DCSSI) du Secrétariat général de la défense nationale (SGDN)[21] qui a notamment en charge de définir les normes de la sécurité des systèmes d'information en France[22].

---

18. *JO* 31 déc. 2005, p. 20779, rect. *JO* 4 janv. 2006, p. 124. La rectification du 4 janvier 2006 a eu pour objet d'inclure les États parties à l'accord sur l'Espace économique européen ayant conclu une convention d'assistance administrative avec la France. E. A. CAPRIOLI, *Le décret du 30 décembre 2005 réglementant les relations financières avec l'étranger, Vers l'émergence de l'intelligence juridique : RD bancaire et financier* n° 2, mars-avr. 2006, p. 38.
19. Rapport MARTRE, *Intelligence économique et stratégie des entreprises*, Commissariat général au plan, 1994.
20. V. E. A. CAPRIOLI, préc.
21. Deux arrêtés établissent son organisation :
– l'arrêté du 15 mars 2002 portant organisation de la direction centrale de la sécurité des systèmes d'information : *JO* 15 mars 2002, p. 4838 ;
– et l'arrêté du 15 mars 2002 relatif à l'organisation en bureaux des sous-directions de la direction centrale de la sécurité des systèmes d'information : *JO* 15 mars 2002, p. 4839.
22. La DCSSI a comme rôles principaux :
– la définition interministérielle et l'expression de la politique gouvernementale en matière de sécurité des systèmes d'information ;
– une fonction de régulation ;
– l'évaluation des menaces pesant sur les systèmes d'information, donner l'alerte, développer les capacités à les contrer et à les prévenir ;
– la fonction de centre de référence et d'expertise scientifique et technique.

Ce rôle de sécurité est relayé au niveau européen par l'Agence européenne chargée de la sécurité des réseaux et de l'information. Elle a pour mission principale la réalisation des analyses à long terme sur les risques émergents et qui affectent les systèmes d'information en Europe. L'agence a pour but d'« assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de la Communauté et en vue de favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information »[23]. On peut d'ailleurs noter avec intérêt la définition de la sécurité des systèmes d'information – l'une des premières à notre connaissance – qui y figure (art. 4. c) : « sécurité des réseaux et de l'information : la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent **la disponibilité, l'authenticité, l'intégrité et la confidentialité** de données stockées ou transmises et des services connexes que ces réseaux et systèmes offrent ou qu'ils rendent accessibles ». Cette définition reprend les quatre grandes fonctions de la sécurité des systèmes d'information qui seront étudiées par la suite.

Bien évidemment, l'État français ou la Communauté européenne ne sont pas les seuls à se préoccuper de la question des systèmes d'information. Les attaques et les menaces autour des systèmes d'information peuvent constituer des failles essentielles au bon fonctionnement des entreprises et des organisations administratives. Dans les grandes entreprises, la sécurité des systèmes d'information relève de la direction des systèmes d'information ou d'un service dédié, rattaché à la direction générale ou au secrétariat général (SSI). En effet, les systèmes d'information sont aujourd'hui la cible de nombreuses attaques. La criminalité informatique a considérablement évolué depuis ses débuts en 1966 aux États-Unis[24]. Les criminels ne se contentent plus de s'introduire dans des systèmes informatiques pour inoculer des virus et les contaminer. Les pirates s'approprient des informations stratégiques, violent la confidentialité des fichiers des organismes de l'État et des entreprises, détruisent des données ou des programmes, s'infiltrent de façon non autorisée dans les serveurs, puis dans les réseaux auxquels ils donnent accès[25].

Aujourd'hui, une criminalité « high tech » voit le jour, tournée notamment vers les profits financiers. Elle est sous le feu de l'actualité depuis les attaques de février 2000 contre des sites de commerce électronique très connus (*Yahoo.com*, *Amazon.com*, E-bay, etc.) et la prolifération de virus comme « I love you », « Melissa »

---

23. Article 1er du règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (*JOUE* 13 mars 2004, p. 1 et s.).
24. Il s'agissait alors d'une altération des comptes d'une banque de Minneapolis.
25. En reprenant la convention du Conseil de l'Europe sur la cybercriminalité de 2001, les comportements incriminés sont les suivants :
– infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques ;
– falsifications et fraudes informatiques ;
– pornographie enfantine ;
– infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

ou « Red code ». On ne compte plus les atteintes aux systèmes d'information et/ou aux données informatisées, les attaques de serveurs par saturation (spamming), les violations des correspondances privées et de la protection de la vie privée, l'espionnage industriel ou militaire, la contrefaçon de droits de propriété intellectuelle (brevets, marques, dessins, droits d'auteur...), les délits de presse (diffamation, racisme, négationnisme), la fraude fiscale, la fraude à la carte bancaire, le blanchiment d'argent, les réseaux de pédophiles, les jeux et paris en ligne, l'organisation de la prostitution[26]...

Or, le risque zéro n'existe pas en terme de sécurité. Toute organisation a son talon d'Achille et on peut faire confiance aux hackers, phreakers et autres pirates du cyberespace pour trouver de nouveaux moyens afin de mettre à mal les meilleures protections informatiques, voire pour utiliser les technologies les plus récentes à des fins délictueuses[27] (le « *vishing* » pour la voix sur IP connaît un développement préoccupant).

Nombreux sont encore ceux qui pensent que la SSI est essentiellement technique. Cette idée est erronée, étant donné que le principal facteur de risque en la matière, c'est le facteur humain. À la vérité, la technique doit être associée aux dimensions juridiques et organisationnelles, de sorte que les utilisations soient encadrées et que la sensibilisation et la formation des personnels soient assurées. La SSI fait aussi partie de la culture de l'entreprise ou de l'organisation. Les enjeux portent sur le patrimoine informationnel de l'entité et sur le management de la connaissance[28].

On l'aura compris, le droit de la sécurité des systèmes d'information est un droit transversal, dont les sources sont protéiformes ; il se fonde à la fois sur des textes juridiques et sur des normes techniques (I). Ce préalable est nécessaire pour déterminer l'environnement juridique de la sécurité des systèmes d'information sur la base duquel la « gouvernance » du système d'information peut être construite (II).

I. – LES SOURCES DU DROIT DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Il convient, au préalable, de rappeler que les sources du droit de la sécurité des systèmes d'information sont plurales et qu'elles portent également sur les aspects techniques et le management. Ainsi, l'expertise juridique se double forcément d'une bonne connaissance technique des procédés et systèmes utilisés et l'on ne peut faire l'économie d'une analyse des principales normes techniques pour disposer d'une vision pleine et entière du domaine ; « l'état de l'art » technique contribue effectivement aux règles juridiques applicables[29] tant sur le plan de la

---

26. Telle est la liste déjà fort complète des cybercrimes, E. A. CAPRIOLI, *Les moyens juridiques de lutte contre la cybercriminalité : Risques* n° 51, sept. 2002. Égal. D. MARTIN et F.-P. MARTIN, *Cybercrime : menaces, vulnérabilités et ripostes*, Paris, PUF, 2001 ; Ch. FÉRAL-SCHUHL, *Cyberdroit, Le droit à l'épreuve de l'internet*, Dalloz, 2006, spéc. p. 585 et s.
27. TGI Paris, 21 sept. 2005, *Le phishing saisi par le droit : Comm. com. électr.* févr. 2006, p. 48, note E. A. CAPRIOLI.
28. P. COHENDET, F. CRÉPLET, O. DUPOUËT, *La Gestion des Connaissances*, Economica, 2006.
29. E. A. CAPRIOLI, *Aperçus sur le droit du commerce électronique (international)* : in *Souveraineté étatique et marchés internationaux à la fin du XXe siècle : Mélanges en l'honneur de Philippe Kahn*, 2000, p. 253.

conformité légale que celui de leur mise en œuvre opérationnelle. En matière de sécurité, droit et technique sont étroitement imbriqués[30]. Il faut « sécuriser l'entreprise connectée »[31].

Pour les États et les organisations, l'importance des systèmes d'information et des données constituant l'information et ses traces se manifeste dans le cadre des textes juridiques et des normes techniques quelle que soit l'échelle sur laquelle on se place : nationale (C), communautaire (B) ou internationale (A). Les sources mentionnées *infra* n'ont pas vocation à être exhaustives.

A. – Les sources internationales

La sécurité des systèmes d'information constitue une des préoccupations majeures des pays industrialisés. Les organisations internationales se sont penchées sur cette question tant pour faciliter les échanges de données que pour réprimer les comportements délictuels sur les réseaux[32]. Tous les textes mentionnés ci-après (1) n'ont pas de caractère contraignant dès lors qu'ils n'ont pas été transposés, ratifiés ou introduits par la loi dans le système juridique d'un État (ex. : loi-type, lignes directrices, recommandations). Il en va de même pour les normes techniques (2) qui n'auront un impact direct sur la sécurité des systèmes d'information que si un usage, un contrat ou un texte particulier les y contraint. Toutefois, si le respect de telles dispositions est pour l'essentiel facultatif, il est recommandé de les prendre en compte dans la mesure où, bien souvent, elles posent les bases de « l'état de l'art » et des bonnes pratiques du marché.

1) Les textes

• **Convention du 28 janvier 1981 du Conseil de l'Europe n° 108** pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[33].

• **Convention sur la cybercriminalité (STE n° 185)**, du Conseil de l'Europe, signée à Budapest le 23 novembre 2001[34].

La loi française n° 2005-493 du 19 mai 2005[35] a ratifié cette convention et a été publiée par le biais du décret n° 2006-580 du 23 mai 2006[36], en France. Cette convention est désormais applicable en France et peut servir de fondement à une action judiciaire.

---

30. CRID, J. HUBIN et Y. POULLET, *La sécurité informatique, entre technique et droit : Cahiers du CRID*, n° 14, Namur, Éd. Story Scientia, 1998.
31. P.-L. RÉFALO, *Sécuriser l'entreprise connectée*, Éd. d'Organisation, 2002.
32. E. A. CAPRIOLI, *Droit international de l'économie numérique*, Paris, Litec, 2e éd., 2007.
33. Disponible à l'adresse : *http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm*.
34. Un protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques a été inséré à Strasbourg le 7 novembre 2002.
35. Loi autorisant l'approbation de la convention sur la cybercriminalité et du protocole additionnel à cette convention relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques : *JO* 20 mai 2005, p. 8729 et s.
36. *JO* n° 120, 24 mai 2006, p. 7568.

Ce texte prévoit un titre relatif aux infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques. Les États signataires de la convention se sont engagés à prévoir des dispositions législatives pour ériger en infraction pénale l'accès illégal à tout système informatique, les interceptions illégales et sans droit de données informatiques, l'atteinte à l'intégrité des données, l'atteinte à l'intégrité du système et certains cas d'abus de dispositifs.

• **Lignes directrices de l'OCDE** sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, adoptées le 23 septembre 1980[37].

• **Recommandations du conseil de l'OCDE** relatives aux lignes directrices régissant la politique de cryptographie du 27 mars 1997[38].

• **Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité**[39].

Ces lignes ont été adoptées sous la forme d'une recommandation du conseil de l'OCDE lors de sa 1 037e session, le 25 juillet 2002. L'objectif de ces lignes directrices était de promouvoir une culture de la sécurité en tant que moyen de protection des systèmes et réseaux d'information, de renforcer la sensibilité aux risques en adoptant des politiques, mesures et pratiques pour y faire face et, par là, une plus grande confiance dans les systèmes et réseaux d'information et la façon dont ils sont mis à disposition et utilisés. Elle vise à créer un cadre général de référence relatif à la sécurité, créer une coopération et un partage des informations entre les parties et élaborer et mettre en œuvre des normes de sécurité.

• **Loi-type de la Commission des Nations unies pour le droit du commerce international (CNUDCI) sur le commerce électronique** (résolution 51/162 de l'assemblée générale du 16 décembre 1996, *www.uncitral.org*).

• **Loi-type de la CNUDCI sur les signatures électroniques** (résolution 56/80 de l'assemblée générale du 12 décembre 2001, *www.uncitral.org*).

• **Convention de la CNUDCI sur l'utilisation des communications électroniques dans les contrats internationaux** (résolution 50/21 de l'assemblée générale du 9 décembre 2005, *www.uncitral.org*).

• **Arrangement de Wassenaar** relatif au contrôle multilatéral des exportations pour les armes conventionnelles et les marchandises et technologies à double usage[40].

---

37. Disponible sur le site *www.oecd.org*. V. à ce sujet, pour une déclaration postérieure, E. A. CAPRIOLI, *Sur les trois déclarations ministérielles lors de la conférence interministérielle à Ottawa : DIT* 1998, n° 3, p. 100-102.
38. Disponible à l'adresse : *http://www.oecd.org/dataoecd/54/58/1814722.pdf*. E. A. CAPRIOLI, *Les lignes directrices de l'OCDE régissant la politique de cryptographie : Lamy droit de l'informatique, Cahiers Lamy du droit de l'informatique*, n° 92 supplément B, mai 1997, p. 1-5.
39. Disponible sur le site *www.oecd.org*.
40. Les négociations ont abouti en juin 1996 et l'arrangement a été signé par trente et un pays. Il a été révisé en décembre 1998 à Vienne. Désormais, les produits cryptographiques inférieurs à 56 bits sont libres à l'exportation (disponible à l'adresse : *http://www.wassenaar.org/2003Plenary/initial_elements2003.htm*).

2) Les normes[41]

La sécurité des systèmes d'information est un des domaines où un grand nombre de travaux normatifs a été entrepris ces dernières années. La norme technique se définit comme étant un « document, établi par le consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné »[42]. Il a ainsi été jugé que l'existence d'une norme[43] permet de représenter un état de l'art dans le domaine auquel elle se rapporte[44].

Il convient de citer les principales normes internationales relatives à la sécurité des systèmes d'information :

• **ISO 13335 (Guide de management de la sécurité informatique)**[45] : Cette norme trouve son origine dans quatre rapports techniques. Elle se compose de quatre parties. La première est relative aux concepts et modèles pour la gestion de la sécurité des technologies. La deuxième traite des techniques pour la gestion de la sécurité informatique (organisation). La troisième est relative à la sélection des sauvegardes et à la gestion du risque. Enfin, la quatrième partie est un guide pour la gestion de sécurité du réseau (mesures préventives).

• **ISO/CEI 15408-1 : 1999 (E) : Critères communs (ou Common Criteria for Information Technology Security Evaluation)**[46]. Les Critères communs (CC) font la synthèse des critères à respecter en matière de sécurité pour les systèmes informatiques suivant les prescriptions européennes, américaines et canadiennes. Ils sont structurés en trois parties : l'introduction et le modèle général, les exigences fonctionnelles de sécurité et enfin les exigences d'assurance de sécurité. Les concepts développés concernent principalement les systèmes directement impliqués dans la sécurité comme les antivirus, les firewalls, l'authentification, le contrôle biométrique, les systèmes de détection d'intrusion (IDS), les systèmes d'accès...

---

41. Sur les principales normes internationales, v. AFNOR, *La sécurité informatique, manager et assurer*, Afnor, 2004.
42. *Guide ISO/IEC, Normalisation et activités connexes – Vocabulaire général*, 3 nov. 2004, disponible à l'adresse : *http://webstore.iec.ch/webstore/webstore.nsf/artnum/033740?opendocument* (payant).
43. F. VIOLET, *Articulation entre la norme technique et la règle de droit*, préf. J. SCHMIDT-SZALEWSKI, PUAM, 2003 ; A. PENNEAU, *Règles de l'art et normes techniques*, Paris, LGDJ, 1989, n° 285, spéc. p. 203, du même auteur, *Respect de la norme et responsabilité civile et pénale de l'homme de l'art : LPA* 11 févr. 1998, n° 18, p. 28-34.
44. Cass. 3e civ., 4 févr. 1976 : *Bull. civ.* III, n° 49.
45. La norme ISO 1335 se scinde en quatre parties :
– ISO 13335-1 : Concepts et modèles pour la gestion de la sécurité des technologies de l'information et de la communication (2004) ;
– ISO 13335-3 : Techniques pour la gestion de la sécurité informatique (1998) ;
– ISO 13335-4 : Sélection de sauvegardes (2000) ;
– ISO 13335-5 : Guide pour la gestion de sécurité du réseau (2001).
46. Les documents décrivant les Critères communs sont disponibles sur le site de la DCSSI (Direction centrale de la sécurité des systèmes d'information), qui est l'autorité nationale de régulation de la sécurité des systèmes d'information, dépendante des services du Premier ministre.

• **ISO/CEI 17799 (Technologies d'information – Technologies de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information, version du 15 juin 2005).** C'est une norme internationale publiée en décembre 2000 par l'ISO sur la base d'une norme du British Standard Institute. Elle définit un code de bonnes pratiques destinées à être utilisées par tous ceux qui sont responsables de la mise en place ou du maintien des systèmes de gestion de la sécurité des informations. Cette sécurité des systèmes d'information est définie au sein de la norme comme « la préservation de la confidentialité (s'assurer que les informations sont accessibles des seules personnes autorisées), de l'intégrité (conservation de la validité et de l'intégralité des informations et méthodes de traitement), et de la disponibilité (les utilisateurs autorisés doivent avoir accès aux informations chaque fois que c'est nécessaire) ».

• **ISO/CEI 27001 (Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Exigences).** Elle définit les exigences pour créer un Système de management de la sécurité de l'information (SMSI), systèmes de gestion de la sécurité des informations (ou ISMS – Information Security Management System). Elle définit l'ensemble des tests et contrôles à effectuer pour s'assurer du bon respect de la norme ISO/CEI 17799.

Les documents juridiques ou techniques internationaux constituent une trame permettant d'exposer les bonnes pratiques en matière de sécurité des systèmes d'information. Ils sont souvent repris aux niveaux communautaire et national.

B. – Les sources communautaires

Plusieurs textes importants, qu'ils soient juridiques ou techniques, ont été adoptés par les institutions européennes qu'il convient de citer ci-après.

1) Textes

• **Recommandation 95/144/CE du Conseil, du 7 avril 1995,** concernant des critères communs d'évaluation de la sécurité des technologies de l'information[47]. Le Conseil demande notamment que les États membres négocient une reconnaissance mutuelle bilatérale, européenne ou internationale, des certificats d'évaluation de la sécurité.

• **Directive communautaire 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995,** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[48].

La section VIII est consacrée à la confidentialité et à la sécurité des traitements. L'article 17 relatif à la sécurité des traitements prévoit que « le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données [...] contre la destruction accidentelle ou illicite,

47. *JOCE* n° L. 93, 26 avr. 1995, p. 27 et 28.
48. *JOUE* n° L. 281, 23 nov. 1995, p. 31 à 50.

la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés [...] ainsi que toute autre forme de traitement illicite. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger. » Cette directive a également un impact sur la conservation des données à caractère personnel.

• **Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999**[49] sur un cadre communautaire pour les signatures électroniques.

• **Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000** relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« *directive commerce électronique* »)[50].

• **Règlement (CE) du Conseil n° 1334/2000 du 22 juin 2000** instituant un régime communautaire de contrôles des exportations de biens et technologies à double usage[51], modifié par le **règlement (CE) n° 2889/2000 du Conseil du 22 décembre 2000**[52].

• **Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001** sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information[53].

• **Résolution 2002/C 43/02 du Conseil du 28 janvier 2002** relative à une approche commune et à des actions spécifiques dans le domaine de la sécurité des réseaux et de l'information[54]. Cette résolution vise notamment à inciter les États membres de l'Union européenne à lancer des campagnes afin d'attirer l'attention sur les problèmes relatifs à la sécurité des réseaux et de l'information ou à renforcer les campagnes en cours. Par ailleurs, le Conseil incite à recourir à une gestion de l'information fondée sur des normes internationales ou encore, à promouvoir l'utilisation de la norme relative aux critères communs (ISO 15408) et à favoriser la reconnaissance mutuelle des certificats qui s'y rapportent.

• **Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002** concernant le traitement des données à caractère personnel et la

---

49. *JOCE* n° L. 13, 19 janv. 2000, p. 12 et s. V. notamment E. A. CAPRIOLI, *La loi française sur la preuve et la signature électroniques dans la perspective européenne : JCP* G 2000, I, 224, et *La directive européenne n° 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques : Gaz. Pal.* 29-31 oct. 2000, p. 5 et s.
50. *JOCE* n° L. 178, 17 juill. 2000, p. 1 et s. V. J. HUET, *La problématique du commerce électronique au regard du projet de directive du 23 décembre 1998 : Comm. com. électr.* 1999, chron. 4. V. *Cahiers du CRID (Centre de recherches informatique et droit) : Le commerce électronique européen sur les rails*, n° 19, Bruylant, Bruxelles, 2001.
51. *JOCE* n° L. 159, 30 juin 2000, p. 1 et s., modifié par le règlement (CE) du Conseil n° 1504/2004 du 19 juill. 2004 : *JOUE* n° L. 281 du 31 août 2004, p. 1 et s.
52. *JOCE* n° L. 336, 30 déc. 2000, p. 14 et s.
53. *JOCE* 22 juin 2001, p. 10 et s.
54. *JOUE* n° C. 43/2, 6 févr. 2002, p. 2 et s.

protection de la vie privée dans le secteur des communications électroniques (dite « directive vie privée et communications électroniques »)[55].

• **Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004** instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information[56]. Cette agence a pour mission principale la réalisation des analyses à long terme sur les risques émergents affectant les systèmes d'information en Europe, ayant pour but d'« assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de la Communauté et en vue de favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information »[57]. En pratique, elle doit conseiller les États membres et la Commission, promouvoir la coordination des activités de sécurité des systèmes d'information au sein de l'Union et sensibiliser les citoyens, les entreprises et les administrations sur cet enjeu.

• **Décision cadre 2005/222/JAI du 24 février 2005** relative aux attaques visant les systèmes d'information[58]. Cette décision cadre est l'aboutissement des souhaits exprimés lors du Conseil européen de Tampere de 1999. Les États membres se sont accordés sur les définitions relatives au système d'information, données informatiques, personne morale et sur l'expression « sans en avoir le droit ». Certaines actions sont considérées comme des infractions pénales répréhensibles : l'accès illicite à des systèmes d'information, l'atteinte à l'intégrité d'un système et l'atteinte à l'intégrité des données.

• **Directive n° 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006** sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public et modifiant la directive n° 2002/58/CE[59].

2) Normes

• **Information Technology Security Evaluation Criteria (ITSEC).** Cette norme est un standard pour la sécurité des systèmes d'information qui définit une politique de sécurité du système d'information. L'ITSEC est le produit du travail commun de plusieurs pays de l'Union européenne (France, Allemagne, Royaume-Uni, Pays-Bas) réalisé en 1991.

La norme définit des critères de sécurité portant principalement sur les mesures techniques de sécurité mais également sur les aspects non techniques tels que les procédures d'exploitation liées à la protection du personnel, la sécurité physique et la sécurité organisationnelle. L'intérêt d'élaborer de tels critères harmonisés au plan communautaire est de fournir une base compatible pour la certification par

55. *JOCE* n° L. 201, 31 juill. 2002, p. 37. V. E. DROUARD, *Directive « communications électroniques » : la prospection et la traçabilité en question : Expertises* oct. 2002, p. 338 et s.
56. *JOUE* 13 mars 2004, p. 1 et s.
57. Article 1er du règlement CE n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information.
58. *JOUE* n° L. 69, 16 mars 2005, p. 67 et s.
59. *JOUE* n° L. 105, 13 avr. 2006, p. 54 et s. E. A. CAPRIOLI, I. CANTÉRO, P. AGOSTI, *Traçabilité des échanges électroniques et droit, Techniques de l'ingénieur*, Doc TR 850, 2006.

les organismes de certification nationaux des quatre pays qui y coopèrent, avec pour objectif final de permettre la reconnaissance mutuelle des résultats des évaluations (v. la Recommandation 95/144/CE du Conseil, du 7 avril 1995).

Une décision de la Commission vient préciser les normes admises pour les produits de signature électronique. Ainsi la liste des normes généralement admises pour les produits de signatures électroniques dont les États membres présument qu'ils sont conformes aux exigences visées à l'annexe II, point f), de la directive 1999/93/CE est la suivante :

– CWA 14167-1 (March 2003) security requirements for trustworthy systems managing certificates for electronic signatures – Part 1 : System Security Requirements.

– CWA 14167-2 (March 2002) security requirements for trustworthy systems managing certificates for electronic signatures – Part 2 : cryptographic module for CSP signing operations – Protection Profile (MCSO-PP).

De plus, la Liste des numéros de référence de normes généralement admises donnant présomption de conformité des produits de signatures électroniques aux exigences de l'annexe III de la directive 1999/93/CE relative aux dispositifs sécurisés de création de signature électronique est :

– CWA 14169 (March 2002) : secure signature creation devices[60].

Les nombreuses sources européennes relatives à la sécurité des systèmes d'information prévoient une harmonisation des législations européennes mais elles donnent également aux États des objectifs à suivre pour mieux encadrer la sécurisation des systèmes d'information.

C. – Les sources du droit français

Parmi les textes législatifs et réglementaires et les normes techniques, on prendra le parti de ne mentionner que les principaux. Ainsi les codes ne seront pas cités (ex. : pénal, civil ou propriété intellectuelle).

1) Textes :

• **Loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et Libertés » modifiée par la **loi n° 2004-801 du 6 août 2004** relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel[61]. Cette loi a créé la Commission nationale

60. Décision 2003/511 du 14 juillet 2003 relative à la publication des numéros de référence de normes généralement admises pour les produits de signatures électroniques, conformément à la directive 1999/93/CE du Parlement européen et du Conseil : *JOCE* n° L. 175, 15 juill. 2003, p. 45 et s.

61. *JO* 7 août 2004, p. 14063. V. les contributions du numéro spécial *Comm. com. électr.* févr. 2005 ; v. le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ; v. I. CANTÉRO, *Décret du 20 octobre 2005 pris en application de la loi « Informatique et Libertés » : Comm. com. électr.* févr. 2006, n° 6. V. I. CANTÉRO, E. CAPRIOLI, *Le choix d'un correspondant à la protection des données (CPDCP) : JCP* E juin 2006, p. 1104 et s.

informatique et libertés (CNIL), autorité administrative indépendante, qui est chargée de veiller au respect de la loi « Informatique et Libertés », notamment lors de la collecte et de la mise en œuvre des traitements de données à caractère personnel. Elle pose comme principe de sécuriser les données à caractère personnel qui ont été traitées par une entité de droit public ou privé.

• **Loi n° 2000-230 du 13 mars 2000** portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique[62] : v. notamment les articles 1316 à 1316-4 introduits par la loi dans le Code civil et relatifs aux écrits et signatures électroniques. Le législateur y a redéfini la preuve littérale afin d'intégrer dans le système probatoire français les écrits sous forme électronique. Ces dispositions ont une incidence sur les conditions d'établissement et de conservation d'un écrit électronique à titre de preuve.

• **Décret n° 2001-272 du 30 mars 2001** pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique[63].

• **Loi n° 2001-1062 du 15 novembre 2001** relative à la sécurité quotidienne[64].

• **Décret n° 2002-535 du 18 avril 2002** relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information[65].

• **Loi n° 2003-239 du 18 mars 2003** pour la sécurité intérieure[66].

• **Loi n° 2004-204 du 9 mars 2004** portant adaptation de la justice aux évolutions de la criminalité[67].

• **Loi n° 2004-575 du 21 juin 2004** pour la confiance dans l'économie numérique[68]. Cette loi prévoit un titre complet sur la sécurité dans l'économie numérique (art. 29 et s.). Un chapitre est consacré aux moyens et prestations de cryptologie qui ont pour objet de garantir le stockage et la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité. La loi précise le régime de responsabilité des prestataires techniques, ainsi que l'obligation qu'ils ont de fournir les données permettant l'identification d'une personne.

---

62. *JO* 14 mars 2000, p. 3968. V. sur la question de la preuve électronique : E. A. CAPRIOLI, *Écrit et preuve électroniques dans la loi n° 2000-230 du 13 mars 2000 : JCP* E 2000, n° 2, p. 1 et s. ; *La loi française sur la preuve et la signature électroniques dans la perspective européenne : JCP* G mai 2000, I, 224, p. 787 et s. ; *Le juge et la preuve électronique*, 10 janv. 2000, disponible sur *www.juriscom.net*.
63. *JO* 31 mars 2001, p. 5070 et s. E. A. CAPRIOLI, *Commentaires du décret n° 2001-272 du 30 mars 2001 relatif à la signature électronique : RD bancaire et financier*, n° 3, mai-juin 2001, n° 105, p. 155 ; L. JACQUES, *Le décret n° 2001-272 du 30 mars 2001 relatif à la signature électronique : JCP* G 2001, aperçu rapide, p. 1601 ; F. COUPEZ, C. GAILLIÈGUE, *Vers une signature électronique juridiquement maîtrisée. À propos de l'arrêté du 31 mai 2002 : Comm. com. électr.* nov. 2002, p. 8 et s.
64. *JO* 16 nov. 2001, p. 18215.
65. *JO* 19 avr. 2002, p. 6944 et s. V. A. PENNEAU, *La certification des produits et systèmes permettant la réalisation des actes et signatures électroniques* (à propos du décret n° 2002-535 du 18 avr. 2002) : *D.* 2002, n° 26, p. 2065 ; et *Dr. et patrimoine* févr. 2003, p. 116, obs. E. A. CAPRIOLI.
66. *JO* 19 mars 2003, p. 4761.
67. *JO* 10 mars 2004, p. 4567.
68. *JO* 22 juin 2004, p. 11175 et s. E. A. CAPRIOLI, P. AGOSTI, *La confiance dans l'économie numérique : LPA* 3 juin 2005, p. 4 et s.

• **Loi n° 2006-64 du 23 janvier 2006** relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers[75] ;

• **Loi n° 2006-961 du 1er août 2006** relative au droit d'auteur et aux droits voisins dans la société de l'information[76]. Cette loi traite notamment des mesures techniques de protection concernant les œuvres numériques. Cette mesure de sécurité technique est actuellement au cœur de débats polémiques sur la notion d'interopérabilité[77].

2) Normes

• **La norme AFNOR Z 42-013** « Archivage électronique – Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes », modifiée en décembre 2001. Cette norme fournit un ensemble de spécifications concernant les mesures techniques et organisationnelles à mettre en œuvre pour l'enregistrement, le stockage et la restitution de documents électroniques afin d'assurer la conservation et l'intégrité de ceux-ci. Pour atteindre l'objectif d'intégrité, cette norme préconise de stocker les documents sur des supports non réinscriptibles de type WORM (Write Once Read Many) ou équivalents, gérés, du point de vue fichiers et volumes, conformément aux standards ISO 13490 ou 13346. Cette norme a été conçue pour les copies numériques de documents papier conformément à l'article 1348, alinéa 2, du Code civil. Étant devenue obsolète avec l'évolution des technologies, cette norme est en cours de révision.

• **Le fascicule de documentation AFNOR SSI FD Z 74-260-1** « Technologie de l'information – Guide pour la gestion de la sécurité des systèmes d'information » d'août 1998. Ce guide énonce les grands principes et concepts de gestion de la sécurité des systèmes d'information, l'univers de la sécurité des systèmes d'information (biens de l'entreprise, menaces, vulnérabilités, risques, parades...) ainsi que la gestion opérationnelle de la sécurité (risque, configuration des ordinateurs, etc.).

• **Le référentiel de bonnes pratiques AFNOR BP Z74-500 d'août 2002** « Sécurité des informations stratégiques – Qualité de la confiance – Comment préserver la confidentialité des informations ». L'objectif de ce référentiel de bonnes pratiques est de faciliter la mise en place de la démarche nécessaire pour assurer la « Qualité de la confiance » qu'une structure peut accorder, à son organisation et à celle de ses partenaires, lorsqu'il s'agit de protéger la confidentialité des informations. Accompagné d'exemples de mesures simples à mettre en œuvre, le référentiel vient en complément de l'utilisation des moyens juridiques de protection du patrimoine informationnel et des innovations, par l'utilisation des droits et

---

75. *JO* 24 janv. 2006, p. 1129 et s. E. A. CAPRIOLI, *Les technologies de l'information et la lutte antiterroriste : Comm. com. électr.* mai 2006, n° 87, p. 45 et s. V. également le décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques (*JO* 26 mars 2006, p. 4609).

76. *JO* 3 août 2006, p. 11529 et s. ; v. le numéro spécial *Comm. com. électr.* nov. 2006.

77. V. notamment E. A. CAPRIOLI, *Mesures techniques de protection et d'information des droits d'auteur : Comm. com. électr.* nov. 2006, p. 29 et s. ; J.-M. BRUGUIÈRE, *Le droit à l'interopérabilité : Comm. com. électr.* févr. 2007, étude n° 3, p. 8 et s.

• **Loi n° 2004-669 du 9 juillet 2004** relative aux communications électroniques et aux services de communication audiovisuelle[69]. Cette loi, qui a remplacé le Code des postes et télécommunications par le Code des postes et des communications électroniques (CPCE), fixe notamment le régime juridique applicable à la conservation des données de connexion (CPCE, art. L. 34-1)[70]. Cette disposition, qui a pour objet de faciliter la lutte contre la cybercriminalité, entre pleinement dans une logique de renforcement de la sécurité.

• **Arrêté du 26 juillet 2004** relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation[71].

• **Ordonnance du 16 juin 2005 relative à l'accomplissement** de certaines formalités contractuelles par **voie électronique prise en** application de l'article 26 de la loi pour la confiance dans l'économie numérique[72].

• **Ordonnance n° 2005-1516 du 8 décembre 2005** sur les échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives[73]. Le chapitre 4 de l'ordonnance prévoit qu'un référentiel général de sécurité fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique telles que les fonctions d'identification, de signature électronique, de confidentialité et d'horodatage. Ainsi, lorsqu'une autorité administrative met en place un système d'information, elle doit préalablement déterminer les fonctions de sécurité nécessaires pour protéger ce système eu égard au référentiel général de sécurité (RGS) et aux différents niveaux de sécurité prévus. Enfin, cette ordonnance traite de l'interopérabilité des services offerts par voie électronique en précisant qu'un référentiel général d'interopérabilité (RGI) fixe les règles techniques à cet effet. Ainsi, l'article 11 dispose que le référentiel général d'interopérabilité « détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives ». Qu'il s'agisse du référentiel général de sécurité ou de celui d'interopérabilité, un décret viendra en préciser les conditions d'élaboration, d'approbation, de modification et de publication[74]. Il convient cependant de préciser que les systèmes d'informations traitant d'informations relevant du secret de la défense nationale n'entrent pas dans le champ d'application de cette ordonnance.

---

69. *JO* 10 juill. 2004, p. 12483 et s.
70. V. notamment, E. A. CAPRIOLI, I. CANTÉRO, P. AGOSTI, *Traçabilité des échanges électroniques et droit, Techniques de l'ingénieur*, Doc TR 850, 2006.
71. *JO* 7 août 2004, p. 10223 et s.
72. *JO* 17 juin 2005. V. *L'ordonnance n° 2005-674 du 16 juin 2005 : un nouveau formalisme contractuel pour les échanges électroniques*, disponible sur le site *www.caprioli-avocats.com.*
73. *JO* n° 286, 9 déc. 2005, p. 18986. Pour un commentaire de l'ordonnance, v. E. A. CAPRIOLI : *JCP* A 2006, 1079.
74. V. E. CAPRIOLI, *L'État ne doit pas imposer un* **standard unique aux** *administrations : 01 Informatique* 12 janv. 2007, p. 22 ; égal. sur le site *www.caprioli-avocats.com.*

de données[79]. Ces peines ont, par ailleurs, été fort logiquement alourdies par la loi du 21 juin 2004 pour la confiance dans l'économie numérique[80] et peuvent désormais aller jusqu'à cinq ans d'emprisonnement et 75 000 € d'amende. Il était, en effet, paradoxal de constater que les défauts de protection des données à caractère personnel (C. pén., art. 226-17) étaient sanctionnables plus lourdement que les atteintes ; un peu comme si l'on pénalisait plus fortement la victime potentielle négligente (celui qui doit défendre son SI) que le délinquant (celui qui attaque le SI) !

L'article 323-3-1 nouveau du Code pénal, introduit par la LCEN, a pour objet de réprimer le fait 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 les infractions prévues par les articles 323-1 à 323-3 du Code pénal. Cette disposition est très large car elle permet d'appréhender ce que l'on appelle les virus informatiques de façon neutre techniquement, ce qui a pour effet d'assurer la pérennité de la disposition pour appréhender toutes les formes de virus tels les vers, les spywares, les chevaux de Troie (*Trojan*) ou leurs mutants. Le domaine d'application des articles 323-1 à 323-3 se trouve considérablement élargi. Les nouvelles hypothèses visées se situent en amont des habituelles pratiques qui imposent souvent le caractère frauduleux des faits incriminés, exception faite de l'article 323-2 du Code pénal. Cette nouvelle disposition trouve sa source à l'article 6 de la convention du Conseil de l'Europe sur la cybercriminalité[81]. Aucun article du Code pénal ne prévoyait clairement une sanction relative à la prolifération des virus ou des « programmes malicieux ». En effet, l'article 323-1 du Code pénal réprime l'accès frauduleux dans tout ou partie d'un STAD, alors même que, dans bien des cas, les virus y sont introduits d'une façon régulière, par l'intermédiaire des messageries électroniques. Pour sa

79. V. notamment TGI de Vannes, 13 juill. 2005, disponible sur le site : *www.juriscom.net*.

80. E. A. CAPRIOLI, P. AGOSTI, *La confiance dans l'économie numérique : LPA* 3 juin 2005, p. 4 et s.

81. Cet article dispose : « Abus de dispositifs

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit :
   a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition
      i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions [...] ;
      ii. d'un mot de passe, d'un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions [...] ; et
   b. la possession d'un élément visé aux paragraphes (a) (i) ou (ii) ci-dessus dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions [...]. Une partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.
2. Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes n'a pas pour but de commettre une infraction [...] comme en cas d'essais autorisés ou de protection d'un système informatique. »

titres de propriété intellectuelle (brevets d'inventions, dessins et modèles, certificats d'utilité, marques, droit d'auteur), de la mise en œuvre de dispositifs particuliers (contrat de confidentialité, etc.).

L'ensemble de ces sources démontre l'étendue du champ d'application du droit de la sécurité des systèmes d'information. Une analyse plus précise des différents textes permet toutefois de déterminer leurs modalités d'application et leurs conséquences juridiques.

II. – ENVIRONNEMENT JURIDIQUE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

On remarquera que la plupart des textes juridiques applicables en matière de sécurité des systèmes d'information ne traitaient pas toujours de la protection des données en elles-mêmes (exception faite notamment de la loi du 6 janvier 1978 ou de la loi sur le secret des correspondances) mais plutôt du système d'information, quel que soit le vocabulaire utilisé[78]. Depuis une dizaine d'années, en revanche, les données numériques, qu'elles soient directement ou indirectement liées au contenu informationnel, sont devenues une préoccupation dominante : les données relatives aux communications électroniques (trafic, connexion, permettant l'identification, ou la traçabilité comme celles qui ont trait à la lutte contre le blanchiment), les données protégées par des droits intellectuels, la fiabilité des données constituant une signature électronique, celles contenues dans un certificat électronique...

Or, les entreprises comme les collectivités publiques préfèrent anticiper les risques en mettant en place des solutions permettant d'assurer la sécurité de leur système d'information. Sun Tzu, dans *L'art de la guerre*, disait : « Celui qui excelle à résoudre les difficultés, les résout avant qu'elles ne surgissent. Celui qui excelle à vaincre ses ennemis triomphe avant que les menaces de ceux-ci ne se concrétisent. »

La sécurité des systèmes d'information ne saurait reposer sur les seuls outils de sécurité comme les antivirus, les IDS, les routeurs ou les pare-feux. La vigilance des utilisateurs est primordiale ainsi qu'un suivi des mises à jour des applications et de l'organisation humaine et juridique.

La détermination du cadre juridique de la sécurité des systèmes d'information commande que l'on précise, d'une part, les principaux domaines juridiques à prendre en compte (A) et, d'autre part, les outils juridiques et techniques sur lesquels se fonde la protection de l'organisation (B).

A. – Les principaux domaines juridiques de la SSI

1) Aspects de droit pénal

Traditionnellement, les atteintes aux systèmes d'information sont souvent limitées aux atteintes aux systèmes de traitement automatisé de données (STAD). Ainsi, les articles 323-1 et suivants du Code pénal prévoient les peines relatives à l'accès frauduleux, au délit d'entrave ou encore à l'introduction, la modification ou la suppression frauduleuse de données dans un système de traitement automatisé

78. On parle ainsi de Système de traitement automatisé de données (STAD) dans le Code pénal.

part, l'article 323-2 punit le fait d'entraver ou de fausser le fonctionnement d'un STAD. De même, l'article 323-3, qui sanctionne le fait d'introduire frauduleusement des données dans un STAD, ne permet pas de réprimer l'introduction non frauduleuse de telles données par un virus. Or, cette incrimination sanctionne davantage les conséquences de l'introduction d'un virus dans un STAD que le fait de détenir ou de concevoir un tel programme informatique. La réponse pénale devait être plus pertinente au regard des nouveaux contours pris par les faits délictuels. Dès lors, si la preuve permettant d'identifier l'auteur d'une introduction illicite n'est pas établie, le simple fait de trouver chez cette personne (détention) un dispositif technique spécialement adapté pour commettre une des atteintes aux STAD suffit pour engager des poursuites.

Les peines encourues par les détenteurs ou les fabricants de virus informatiques sont celles prévues pour l'infraction commise à l'aide de leur programme ou pour l'infraction la plus sévèrement réprimée. Si l'on prend en considération l'aggravation des peines proposée à l'article 45 de la LCEN, les détenteurs, vendeurs ou pourvoyeurs de programmes informatiques ayant permis la commission des infractions prévues à l'article 323-1 seront désormais passibles d'une peine de trois ans d'emprisonnement et de 45 000 euros d'amende, tandis que les auteurs des délits prévus aux articles 323-2 et 323-3 encourront cinq ans d'emprisonnement et 75 000 euros d'amende.

De plus, ces programmes doivent être « conçus ou spécialement adaptés » pour commettre les infractions, contrairement à l'article 6 de la Convention sur la cybercriminalité qui incrimine les dispositifs « principalement conçus ou adaptés ». Cette formulation témoigne d'une approche différente du législateur français. Ainsi, dans le rapport explicatif de la Convention sur la cybercriminalité[82], au point 73, les auteurs ont longuement examiné la question de savoir si les dispositifs visés devaient être ceux qui étaient conçus exclusivement ou spécialement pour permettre la commission d'infractions. Cette approche, jugée trop restrictive, risquait de « créer des difficultés insurmontables en ce qui concerne l'établissement de la preuve dans les procédures pénales, ce qui rendrait la disposition pratiquement inapplicable ou applicable uniquement dans de rares cas ». Le champ d'application de l'article 323-3-1 du Code pénal semble donc plus restreint qu'il n'y paraît.

Les sanctions pénales ne sont pas applicables lorsque la détention, l'offre, la cession et la mise à disposition sont justifiées par des motifs légitimes. Il convient de déterminer ce que l'on entend par cette expression[83]. Pour ce faire, en reprenant

82. Disponible sur le site *www.coe.int*.

83. Une première version de cet article disposait : « Art. 323-3-1. – Le fait 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.
Les dispositions du présent article ne sont pas applicables lorsque la détention, l'offre, la cession et la mise à disposition sont 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. » V. le projet de loi déposé le 15 janvier 2003 (*Doc. AN* n° 528).

les travaux parlementaires, les cas visés par cette expression semblent précisément énumérés. » Cette exclusion du champ d'application de la sanction pénale a pour premier objet de permettre aux laboratoires scientifiques en informatique, y compris ceux qui travaillent en matière militaire, de poursuivre leurs nécessaires travaux en ce domaine. Elle se justifie également au regard des pratiques des sociétés chargées de concevoir des programmes informatiques de veille, de sécurisation ou de défense des systèmes informatiques et qui ont besoin de concevoir des virus afin de tester la fiabilité de leur propre programme antivirus.[84] » Tant les laboratoires de recherche que les sociétés chargées de la veille ou de la sécurisation des systèmes informatiques sont, *a priori*, exempts de toute intention de commettre un crime ou un délit à l'aide de leurs outils informatiques. Mais avec une formulation énumérative, on aurait pu s'interroger sur l'application de cet article dans le cas d'un service de sécurité interne à l'entreprise (ex. : RSSI[85]) qui peut être amené à stocker des virus interceptés, soit pour les transmettre à un éditeur d'antivirus ou à un prestataire de services de sécurité, soit pour les mettre en quarantaine pour destruction ou analyse.

Les dispositions du Code pénal en matière d'atteinte aux STAD ont donc été actualisées pour prendre en considération le développement de l'utilisation des réseaux numériques, tel l'internet, par les entreprises, les personnes publiques et les citoyens avec son pendant, la délinquance informatique (attaques intrusives et création/propagation de virus informatiques capables de faire des ravages sur les réseaux)[86].

D'autres infractions peuvent également être applicables. Ainsi, le droit à la sécurité soulève également l'existence d'une protection du secret professionnel[87] ainsi que l'existence des secrets « par nature », qui concernent la défense[88], l'économie, l'industrie et la vie privée[89].

La loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie de communications électroniques[90] doit être respectée et ce, y compris pour les correspondances électroniques personnelles (c'est-à-dire non professionnelles). Il convient, en outre, de rappeler à cet égard que la jurisprudence a considéré que les courriers électroniques peuvent être considérés comme des

84. Avis de la Commission des lois, M. Tabarot, (*Doc. AN* n° 608), 11 févr. 2003.
85. Responsable de la Sécurité des systèmes d'information.
86. Pour une proposition de révision du Code pénal, v. J.-F. CASILE, *Le Code pénal à l'épreuve de la délinquance informatique*, Aix-Marseille, PUAM, 2002, préf. G. FAURÉ.
87. C. pén., art. 226-13.
88. C. pén., art. 413-7 et s.
89. C. pén., art. 226-1 (atteinte à la vie privée portant sur les paroles et les images d'une personne se trouvant dans un lieu privé). En outre, le droit au respect de la vie privée a été consacré à plusieurs reprises comme étant une liberté fondamentale avec un rang de liberté constitutionnelle. Il est consacré dans l'article 12 de la Déclaration universelle des droits de l'homme adoptée le 10 décembre 1948, par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, et dans l'article 9 du Code civil issu de la loi du 17 juillet 1970.
90. Publiée au *JO* 13 juill. 1991.

correspondances privées bénéficiant du secret[91], reconnaissant dans certains cas l'application des sanctions pénales prévues pour l'atteinte au secret des correspondances[92].

2) Les données à caractère personnel

La loi Informatique et Libertés modifiée précise les sanctions pénales applicables à toute entreprise qui ne respecterait pas les principes en matière de données à caractère personnel[93]. Aux termes de la loi, c'est en principe le responsable du traitement qui engage sa responsabilité pénale en cas de non-respect des prescriptions de la loi (obligation d'information, droits d'accès, de rectification, formalités préalables). Toutefois, les personnes morales peuvent être déclarées pénalement responsables (C. pén., art. 226-24) et sont passibles de peines plus lourdes (le taux maximum de l'amende est porté au quintuple de celui prévu pour les personnes physiques).

L'utilisation des données biométriques pour les accès physiques ou l'authentification est soumise à autorisation (deux autorisations uniques ont été adoptées en 2006 pour la reconnaissance du contour de la main).

De plus, en vertu de l'article 34 de la loi Informatique et Libertés, l'entreprise doit prendre toutes les mesures de sécurité utiles afin de préserver les données saisies qui ne doivent pas être « déformées, endommagées ou que des tiers non autorisés y aient accès ». Cette obligation est en principe une obligation de moyens[94]. L'article 226-17 du Code pénal prévoit des peines allant jusqu'à cinq ans d'emprisonnement et 300 000 € d'amende[95]. Cependant, ce manquement peut aussi avoir pour conséquence d'engager la responsabilité civile du responsable du traitement[96] accompagnée de sanctions prononcées par la CNIL[97]. La sécurité de ces données doit être proportionnelle à leur nature, à leur finalité, et au risque qu'implique le traitement concerné.

---

91. TGI Paris, Ord. réf., 27 janv. 2003 : *Expertises* juin 2003, p. 240. – Cass. soc., 2 oct. 2001 (affaire *Nikon*) : *Bull.* V, n° 291, p. 233 ; *D.* 2001, p. 3148, note P.-Y. GAUTIER.
92. T. corr. Paris, 2 nov. 2000, chron. J. DEVÈZE et M. VIVANT : *Comm. com. électr.* 2001, n° 24, p. 7 et s. ; confirmé par CA Paris, 17 déc. 2001, consultable sur le site *www.foruminternet.org*.
93. V. en ce sens, I. CANTÉRO, *Présentation de la nouvelle réglementation applicable à la protection des données à caractère personnel : Journal des sociétés* mai 2005, p. 28 et 29.
94. Cass. crim., arrêt 30 oct. 2001, pourvoi 99-82136, inédit.
95. V. par exemple, Cass. crim., 19 déc. 1995 : *Bull. crim.* n° 387 ; *Rev. sc. crim.* 1996, 676, obs. J. FRANCILLON.
96. La cour d'appel de Paris, dans un arrêt du 15 février 1994, a condamné un centre gestionnaire d'impayés d'avoir provoqué une erreur ayant abouti au refus d'un centre de crédit sollicité en raison d'une homonymie et d'une date de naissance. Sur le terrain civil, ces dispositions caractérisent des agissements ou imprudences constitutifs de fautes civiles pouvant mettre en cause la responsabilité civile.
97. « Au travers de la délibération n° 84-40 du 20 novembre 1984 relative au détournement du fichier de gestion du personnel sur ordinateur d'EDF-GDF, la CNIL devait adresser un avertissement public aux organismes responsables et destinataires de ce fichier (fichier qui avait été communiqué au parti communiste qui ne devait pas en être le destinataire). » V. aussi la délibération n° 89-137 du 5 décembre 1989 (au sujet de la MNEF). Commission nationale de l'informatique et des libertés. *15e Rapport d'activité*, 1994. Disponible sur : *www.cnil.fr*. V. également, les premières sanctions pécunières infligées par la CNIL en 2006 : banques, étude d'huissier,...

À ce titre, il pourra être opportun pour des entreprises de toute taille d'**élaborer une politique « Vie privée et données personnelles »**. Cette politique pourrait **démontrer le cas échéant** le respect des principes de la loi Informatique et Libertés devant un tribunal. En outre, le suivi d'une telle politique comme la réalisation du recensement des fichiers et des formalités préalables aux traitements doivent être assurés dans le cadre de la direction de la sécurité des SI (ou de la conformité, ou de la DSI) en nommant un « Responsable Vie privée et données personnelles » de l'entreprise ou du groupe. Dans certains cas, l'entreprise pourra également choisir de désigner un Correspondant à la protection des données à caractère personnel[98].

3) La cryptologie

La loi pour la Confiance dans l'économie numérique prévoit un titre III intitulé « De la sécurité dans l'économie numérique ». Outre le chapitre II relatif à la cybercriminalité et intégré dans le Code pénal, elle a opéré une refonte complète de la réglementation de la cryptologie[99], entendue comme tout processus de transcription d'une information intelligible en une information inintelligible par l'application de conventions secrètes dont l'effet est réversible[100].

La généralisation de l'utilisation des technologies dans notre société a multiplié l'usage des moyens et des prestations de cryptologie ; confidentialité des échanges, et des données stockées sur disque dur, au regard de la protection de la vie privée, du secret des correspondances et des secrets du commerce électronique[101]. En effet, les informations doivent pouvoir circuler sur les réseaux sans être lues, altérées, détournées par des personnes non autorisées. Désormais, il existe des produits cryptologiques efficaces pour assurer la sécurité et l'« authentification »[102] des communications électroniques, disponibles sur le marché.

La cryptologie permet de garantir la confidentialité des communications électroniques mais aussi d'identifier de manière certaine l'auteur d'un message. Outre cette fonction d'authentification, la cryptologie asymétrique permet également le contrôle d'intégrité du message, c'est-à-dire la possibilité d'établir que son contenu n'a pas été modifié. Les fonctions d'identification et d'intégrité sont assurées par la signature électronique fondée sur un certificat à clé publique. De plus, les mesures de chiffrement sont utilisées dans les entreprises pour chiffrer les données, mais aussi les disques des ordinateurs portables afin d'éviter que les informations qui y sont contenues ne soient accessibles à des personnes non autorisées.

---

98. E. A. Caprioli et I. Cantéro, *Le choix d'un correspondant à la protection des données : JCP* E 2006, 1976.

99. V. d'un point de vue technique, J.-S. Lair, *De l'usage de la cryptologie*, Sécurité informatique (publication du CNRS), n° 24, avr. 1999, p. 1 et s.

100. V. E. A. Caprioli, *Le nouveau régime juridique de la cryptologie (suite aux deux décrets du 24 février 1998)* : supplt au *Bulletin d'actualité du Lamy droit de l'informatique*, n° 101, mars 1998, p. 1 et s.

101. E. A. Caprioli, *Sécurité, cryptologie et libertés : Bulletin du barreau de Nice*, oct. 2002, p. 10 et s. ; disponible sur le site *http://www.caprioli-avocats.com*.

102. Ce mot, utilisé par les techniciens, doit être pris ici au sens de vérification de l'origine d'un message ou d'identification et non au sens juridique du terme.

Le régime juridique des moyens et des prestations de cryptologie couvre donc une large palette de fonctions liées à ces techniques d'où son importance, eu égard aux restrictions d'usage, de fourniture, d'exportation et d'importation qui ont pu exister par le passé. La réglementation est neutre techniquement, elle se fonde sur les fonctions remplies par les moyens utilisés et non pas sur les technologies. Le principe de la liberté d'utilisation de tous les moyens de cryptologie est acquis quelles que soient les fonctions dudit moyen : confidentialité, authentification ou intégrité. Les règles pour la fourniture, le transfert, l'import et l'export des moyens ont été assouplies. Cependant, la liberté a un corollaire, le renforcement de la responsabilité des personnes offrant ou utilisant des moyens de cryptologie [103].

Ainsi, les fournisseurs de moyens ou de prestations de cryptologie et les Prestataires de services de certification électronique (PSCE) se sont vu imposer dans le cadre de la LCEN un régime spécial de responsabilité.

Pour les premiers (prestataires de services de cryptologie), l'article 32 de la LCEN dispose : « Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes fournissant des prestations de cryptologie à des fins de confidentialité sont responsables, au titre de ces prestations, nonobstant toute stipulation contractuelle contraire, du préjudice causé aux personnes leur confiant la gestion de leurs conventions secrètes en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions. »

Cette responsabilité contractuelle du fournisseur porte sur l'obligation essentielle d'assurer la gestion des conventions secrètes qu'on lui a confiées. Toute échappatoire contractuelle, exonération ou limitation de responsabilité est expressément exclue. Le recouvrement ou le séquestre de clés de chiffrement sont des opérations à manier avec les plus grandes précautions étant donné les conséquences pécuniaires qu'elles peuvent générer par la simple absence du résultat attendu : l'indisponibilité des données/absence de déchiffrement, la perte d'intégrité ou de confidentialité des données. Toutefois, il semble difficile de tenir ces fournisseurs responsables des atteintes aux données transformées par des conventions secrètes qui leur ont été confiées, lorsque cette atteinte n'a rien à voir avec une opération cryptologique (par exemple, en cas de destruction physique du (ou des) support(s) lors d'un incendie).

Enfin, on peut penser que cette responsabilité des fournisseurs de prestations de cryptologie constitue un moyen de pression du législateur pour que ces derniers soient en mesure d'assurer le recouvrement des clés de chiffrement. Sans cette possibilité de recouvrer les clés de chiffrement, ces prestataires pourraient voir leur responsabilité civile engagée pour des préjudices pécuniaires conséquents. Imaginons le cas où une personne publique (par exemple, la personne responsable des marchés) a « égaré une convention secrète » relative à l'ouverture d'un appel d'offre

103. E. A. Caprioli, P. Agosti, *La confiance dans l'économie numérique*, LPA 3 juin 2005, p. 4 et s.

public au quantum important et que le fournisseur soit dans l'impossibilité de fournir la prestation de recouvrement ou de restitution de la clé séquestrée. Le prestataire devra indemniser l'intégralité du préjudice. Toutefois, il cessera d'être responsable s'il prouve notamment qu'il n'a commis aucune négligence. Par exemple, il devra démontrer qu'il a tout mis en œuvre pour assurer la sécurité du système électronique en charge des conventions secrètes, en démontrant, par exemple, que ses pratiques techniques et organisationnelles sont fiables.

Pour les seconds (prestataires de services de certification électronique), l'article 33 de la LCEN transpose l'article 6 de la directive européenne du 13 décembre 1999 qui énonce une présomption de responsabilité pour les PSCE qui délivrent des certificats présentés comme étant qualifiés. Sont ainsi concernés les PSCE qui ont fait l'objet d'une qualification volontaire[104] pour une famille de certificat et les PSCE qui se prétendent conformes aux exigences posées pour les certificats qualifiés en vertu du décret du 30 mars 2001. Cette qualification est volontaire et ne peut être imposée par les États. Les certificats présentés comme qualifiés et les dispositifs sécurisés de création de signature au sens du décret du 30 mars 2001 (spécialement l'article 2, la définition figurant à l'article 1 étant sans effet juridique) ne sont pas indispensables pour conférer une valeur juridique à une signature électronique ; mais les signatures électroniques sécurisées bénéficient d'un avantage juridique non négligeable : la présomption de fiabilité du procédé d'identification. En cas de litige, l'utilisation d'une signature électronique sécurisée aura pour conséquence d'opérer un renversement de la charge de la preuve au profit du signataire, la preuve négative étant toujours difficile à établir. Ainsi, celui qui conteste la fiabilité du procédé aura la lourde tâche d'en rapporter la preuve. Toutefois, le juge est libre d'apprécier la fiabilité d'une signature électronique, que celle-ci soit sécurisée ou non notamment en vertu des articles 287, 288 et 288-1 du nouveau Code de procédure civile pour la vérification d'écriture[105].

Le législateur a précisé les obligations sur lesquelles porte la présomption de responsabilité. Ainsi, sont uniquement visées les obligations du PSCE que l'on peut considérer comme étant essentielles, eu égard aux conditions de délivrance des certificats présentés comme qualifiés par le PSCE :

– garantir l'exactitude de toutes les informations contenues dans le certificat à la date où le certificat a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié ;

104. Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation : *JO* 7 août 2004.

105. D. n° 2002-1436, 3 déc. 2002 : *JO* 12 déc. 2002, p. 20482. V. J. DEVÈZE, Perseverare diabolicum, *A propos de l'adaptation du droit de la preuve aux technologies de l'information par le décret n° 2002-1436 du 3 décembre 2002* : *Comm. com. électr.* mars 2003, p. 12 et s.

responsabilité de l'entreprise. Les cas d'exonération de l'employeur sont interprétés très strictement par les tribunaux, spécialement lorsque le salarié utilise des moyens de communications électroniques mis à sa disposition par l'employeur, dans le cadre de son travail [109].

31 Droits de propriété intellectuelle

Les œuvres de l'esprit au rang desquelles figurent les créations des entreprises (bases de données, logiciels, pages web,...) sont protégées par le droit d'auteur. Il convient de rappeler qu'un monopole est reconnu au titulaire des droits sur l'œuvre assorti de certaines exceptions. L'atteinte portée à ce monopole est constitutive du délit de contrefaçon [110]. Les affaires concernant des contrefaçons de bases de données ou de logiciels sont nombreuses.

Pour se protéger contre ces agissements répréhensibles, les titulaires de droits ou leurs ayants droit ont la possibilité de mettre en place des dispositifs techniques visant à restreindre l'accès ou l'utilisation de leur création : les mesures techniques de protection et d'information [111].

Des dispositions législatives ont été prises pour sanctionner l'atteinte aux mesures de protection technique. La loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information [112] introduit les articles L. 335-3-1 (pour le droit d'auteur) et L. 335-4-1 (pour les droits voisins) du Code de la propriété intellectuelle qui sanctionnent l'atteinte contre ces mesures comme suit :

Alinéa 1 : est punie de 3 750 € d'amende toute atteinte délibérée, à des fins autres que la recherche et la SSI, aux mesures techniques réalisée par un internaute par ses propres moyens ;

Alinéa 2 : est puni de six mois d'emprisonnement et de 30 000 € d'amende le fait de procurer ou de proposer sciemment à autrui, directement ou indirectement, des moyens de contournement.

Le décret n° 2006-1763 du 23 décembre 2006 relatif à la répression pénale de certaines atteintes portées au droit d'auteur et aux droits voisins [113] fixe les sanctions pénales encourues à l'occasion de certaines atteintes portées au droit d'auteur et aux droits voisins. L'article premier du texte ajoute deux articles à la partie

109. TGI Marseille, 1re ch. civ., 11 juin 2003, *Escota c/ Lucent Technologies : http://www.juriscom.net* ; confirmé par CA Aix-en-Provence, 13 mars 2006, pourvoi n° 2006/170, disponible sur le site *www.legalis.net*.

110. C. pén., art. L. 122-6-2 (pour les logiciels), L. 335-2.

111. V notamment E. A. Caprioli, *Dispositifs techniques et droit d'auteur dans la société de l'information : Mélanges offerts à J.-P. Sortais*, Bruylant, Bruxelles, 2002, p. 39 à 72 ; *Mesures techniques de protection et d'information des droits d'auteur : Comm. com. électr.* nov. 2006, p. 30 et 31.

112. Loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information : *JO* n° 178, 3 août 2006, p. 11529. V. le numéro spécial *Comm. com. électr.* nov. 2006 et le dossier : *Le nouveau droit d'auteur au lendemain de la loi du 1er août 2006 : D.* 2006, p. 2351 et s.

113. *JO* 30 déc. 2006.

– assurer la vérification de la détention par le signataire identifié, au moment de la délivrance du certificat, de la « convention privée »[106] correspondant à la convention publique du certificat[107] ;

– faire procéder à l'enregistrement de la révocation du certificat et tenir cette information à la disposition des tiers (dans une liste des certificats révoqués publiée en ligne).

Actuellement, les certificats électroniques ne contiennent pas de champs prévus pour inscrire les limites d'utilisation et de valeur – et cela n'est pas sans incidence sur les risques qui pèsent sur les PSCE. En ce qui concerne les signatures qui se fondent sur des certificats non qualifiés ainsi que pour toutes les autres obligations, c'est le droit commun qui s'applique : les articles 1382 et suivants du Code civil pour la responsabilité délictuelle et le droit des obligations contractuelles pour les rapports entre le PSCE et son client[108].

Enfin, en vertu du troisième alinéa de l'article 33, le PSCE devra justifier d'une garantie financière suffisante ou d'une assurance « garantissant les conséquences pécuniaires de sa responsabilité civile ». Cet élément est difficile à appréhender concrètement dans la mesure où la réponse quantitative dépend du montant et de la nature du préjudice, du contenu et des limites de garantie de la police d'assurance du PSCE, des limites contenues dans le certificat et de leur accessibilité. L'appréciation s'effectuera donc au cas par cas, en fonction des circonstances de l'espèce.

4) La responsabilité civile

Les articles 1382 et 1383 du Code civil énoncent un principe de responsabilité à raison des dommages causés de son propre fait mais encore par sa négligence ou par son imprudence. Pour écarter cette responsabilité de droit commun, il est possible d'apporter la preuve que la cause du dommage relève d'un cas de force majeure d'un cas fortuit ou du fait d'un tiers. L'appréciation de ces cas d'exonération de responsabilité ne pourra se faire qu'au cas par cas.

Dans le cadre des relations de travail, l'article 1384, alinéa 5, du Code civil pose le principe de responsabilité de l'employeur du fait des dommages causés par ses salariés (les « préposés ») dans les fonctions pour lesquelles ils sont employés. Ainsi, le préjudice causé à un tiers du fait du manquement ou d'une faute incombant à un salarié ou au responsable de la sécurité des systèmes d'informations engage la

106. On peut regretter l'utilisation de ces termes. Il eût été plus pertinent de conserver le vocabulaire utilisé dans les premières versions du projet, à savoir « données de création de signature » et « données de vérification de signature ». En effet, ces termes sont définis dans le décret du 30 mars 2001, et l'article 33 de la LCEN s'inscrit uniquement dans le prolongement des « certificats présentés par eux (les PSCE) comme qualifiés ».

107. Il importe, dès lors, que le PSCE veille à ce que le signataire auquel le certificat est délivré pour un bi-clé donné soit bien détenteur, lorsque ce certificat lui est délivré, des données relatives à la création de signature correspondante, c'est-à-dire de la clé privée.

108. Pour de plus amples renseignements sur la responsabilité de plein droit, v. Ph. LE TOURNEAU, *Droit de la responsabilité et des contrats*, Dalloz Action, 2004/2005, Dalloz, 2004.

réglementaire du Code de la propriété intellectuelle : l'article R. 335-3 relatif à la détention en vue d'un usage personnel ou l'utilisation d'un dispositif anti-mesures techniques de protection (MTP) « efficace » mentionné à l'article L. 331-5 du Code de la propriété intellectuelle ou au recours à un service pour y porter atteinte, et l'article R. 335-4 relatif à la détention en vue d'un usage personnel ou l'utilisation d'un dispositif anti-mesures techniques d'information (MTI) mentionné à l'article L. 331-22 du Code de la propriété intellectuelle ou au recours à un service pour porter atteinte à un droit d'auteur, un droit voisin ou à un droit de producteur de base de données. Tous les actes visés sont désormais passibles de contraventions de quatrième classe, soit une amende de 750 euros. À la lecture du texte, il s'avère que les sanctions n'ont pas vocation à s'appliquer à la détention d'un dispositif de contournement ou de neutralisation d'une MTP (ou d'une MTI) en vue de sa distribution, mais uniquement à la détention pour un usage personnel. La recherche informatique et la sécurité des systèmes d'information constituent les exceptions à ces règles.

6) Archivage électronique sécurisé

L'archivage électronique sécurisé répond à certaines exigences juridiques essentielles pour une entreprise ou une personne : se préconstituer une preuve de ses droits et de ses obligations. Parfois, le droit pose l'exigence d'un écrit à des fins de validité de l'acte (*ad validitatem*). Par exemple, si l'on archive un document électronique qui ne répondrait pas aux prescriptions légales (ses fonctions d'identification et d'intégrité, sa lisibilité), il sera considéré par le juge comme n'ayant jamais existé. Les conséquences juridiques peuvent être véritablement désastreuses puisque les parties devraient alors être rétablies dans leur situation d'origine. Il convient également de distinguer selon que l'écrit sous forme électronique doit être considéré comme un « original électronique » ou comme une copie. Les régimes juridiques sont différents.

Le titre original se définit comme un écrit dressé, en un ou plusieurs exemplaires, afin de constater un acte juridique signé par les parties à l'acte (ou par le représentant) à la différence d'une copie.

L'original sous forme électronique a reçu dernièrement une consécration juridique. Introduit par l'ordonnance du 16 juin 2005 prise en application de l'article 26 de la LCEN [114], l'article 1325, alinéa 4, du Code civil dispose : « L'exigence d'une pluralité d'originaux est réputée satisfaite pour les contrats sous forme électronique lorsque l'acte est établi et conservé conformément aux articles 1316-1 et 1316-4 et que le procédé permet à chaque partie de disposer d'un exemplaire ou d'y avoir accès. » Outre la mise à disposition ou l'accessibilité, le caractère original d'un écrit dépend donc du respect des articles 1316-1 et 1316-4 du Code civil qui régissent la valeur probatoire de l'écrit sous forme électronique et sa validité (l'article 1108-1 renvoie aux conditions posées par ces deux articles).

114. *JO* 17 juin 2005.

La copie se définit comme toute reproduction littérale d'un original qui, n'étant pas revêtue des signatures qui en feraient un second original, ne fait foi que lorsque l'original ne subsiste plus et sous les distinctions établies par l'article 1335 du Code civil. En matière d'archivage, il pourra s'agir d'un document scannérisé ou tout simplement de tout document électronique non signé. L'article 1348, alinéa 2, du Code civil dispose qu'à défaut d'original, la copie, pour pouvoir être retenue, doit être la « reproduction non seulement fidèle mais aussi durable » du titre original[115]. Ainsi, les copies peuvent valoir comme commencement de preuve par écrit[116]. La durabilité se conçoit, au sens de l'article 1348, alinéa 2, du Code civil comme « toute reproduction indélébile de l'original qui entraîne une modification irréversible du support ». La fidélité est une autre garantie demandée et qui n'est pas définie juridiquement. La norme AFNOR Z 42-013 en donne l'acception suivante : « un document est considéré comme fidèle au document d'origine s'il permet de reconstituer toute l'information nécessaire aux usages auxquels le document d'origine est destiné ». Si la fidélité de la copie s'apprécie par rapport au document original (papier), cette qualité se distingue de l'intégrité (reprise pour l'original) en ce sens que l'intégrité résulte de la confrontation du document original électronique par rapport à lui-même (un autre exemplaire original), c'est-à-dire depuis son enregistrement d'origine. Aucune modification ne doit être détectée.

En définitive, seule la signature électronique reste l'élément distinctif pour différencier un acte sous forme électronique original d'une copie[117].

Par ailleurs, l'archivage portera également sur les données de log, de connexion, et tout autre élément de traçabilité, sur les courriers électroniques, la gestion des accès aux postes informatiques et aux réseaux et services.

B. – Les outils de la SSI

La sécurité des Systèmes d'information repose sur des moyens techniques et sur des instruments juridiques.

1) Les moyens techniques

a) Gestion des risques informatiques

Un dysfonctionnement du système d'information peut déclencher de graves conséquences pour une entreprise ou une organisation. La perte d'informations telle que la perte des adresses e-mails des clients ou de l'ensemble des données commerciales

115. V. G. CORNU, *Vocabulaire juridique*, Association H. Capitant, mai 2000 : « 2. Écrit en vue de constater un acte juridique ou un acte matériel pouvant produire des effets juridiques. »

116. Cass. 1re civ., 14 févr. 1995 : *D.* 1995, 340, note S. PIEDELIÈVRE.

117. Pour plus de détails à ce sujet, v. E. A. CAPRIOLI, *Variations sur le thème du droit de l'archivage dans le commerce électronique* : *LPA* 18 et 19 août 1999, p. 4 et s. Pour de plus amples informations sur l'archivage, v. J.-M. RIETSCH, M.-A. CHABIN et E. A. CAPRIOLI, *Dématérialisation et archivage électronique*, Dunod, 2006.

constitue un risque potentiel et souvent peu pris en compte dans le cadre des systèmes d'information.

Le droit cherche à protéger l'information et les systèmes qui les créent, les communiquent et les conservent. Les systèmes d'information peuvent se voir corrompus par une attaque informatique – ce qui sous-entend un sinistre, une menace ou un risque. On comprend par « sinistre » l'incident dont la survenance entraîne des dommages pour le système touché. Un « risque » est un événement pouvant causer des dégâts et son occurrence est plus au moins probable. Une « menace » est un sinistre dont la probabilité d'occurrence est élevée pour une cible donnée. Une attaque est la concrétisation de cette menace par l'exploitation d'une vulnérabilité du système. On peut citer, comme exemple d'attaque, les intrusions, la diffusion de virus...

Les entreprises font souvent auditer leur système d'information et procèdent à une évaluation des risques. Cet « audit des risques informatiques » doit permettre au dirigeant de décider des modes de prévention des risques et menaces et de résolution en cas de survenance. La méthode la plus couramment utilisée consiste à établir une cartographie à laquelle sont associées certaines directions (risque, assurance, juridique et sécurité de l'information) sous le contrôle de la direction générale. Elle comprend à la fois l'évaluation du risque (c'est-à-dire la mesure des conséquences de leur réalisation), la fréquence (la probabilité de survenance) et la gravité de leur réalisation pour l'organisation.

Après cette phase d'analyse, un plan de prévention est souvent mis en place. Il définit les améliorations à apporter en terme de sécurité et comprend un calendrier prévisionnel de réalisation. Il s'agit de définir les traitements des risques et éventuellement les modalités de continuité de l'activité, c'est-à-dire la mise en place d'un plan de continuité d'activité (PCA) ou de reprise d'activité (PRA). Ces plans ne correspondent pas à un simple plan de secours ou de sauvegarde. Dans certains secteurs comme le secteur bancaire, le PCA est une obligation imposée par le règlement CRBF 97-02 [118].

b) Les protections techniques

Le développement des différents outils de communication à distance tels que le wi-fi, bluetooth ou des outils portables (ordinateur, téléphone, PDA,...)[119] multiplient les risques potentiels d'attaques des systèmes d'information de par une accessibilité étendue du système d'information. Une des premières mesures de protection des systèmes d'information – la plus basique – serait la mise en place

118. V. E. A. CAPRIOLI, *Plan de continuité d'activité des systèmes d'information : aspects juridiques*, oct. 2005, disponible sur *www.caprioli-avocats.com* ; *Commentaire de l'arrêté du 31 mars 2005 modifiant le règlement du comité de la réglementation bancaire et financière n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement : Comm. com. électr.* oct. 2005, p. 49 et s.

119. E. A. CAPRIOLI, *Aspects juridiques de la mobilité : Revue des ingénieurs (des Mines)* janv.-févr. 2006, p. 36 et s.

des mesures de protection technique comme les pare-feux, routeurs, VPN, certificats SSL, Single Sign On (SSO)[120]...

A côté des login/mots de passe, la cryptologie constitue également le moyen par excellence pour sécuriser les systèmes d'information plus complexes, ainsi que les transactions commerciales et l'accès et l'utilisation des données et des informations qui en résultent. Développée originairement à des fins militaires, elle trouve de nos jours de multiples usages, notamment dans un but **d'authentification** et de **contrôle d'intégrité**.

Les entreprises et les administrations mettent souvent en place deux autres types de protection : contractuel et organisationnel.

2) Les instruments juridiques

a) Les documents de nature contractuelle

α) Le guide juridique du RSSI (ou du DSI)

Le RSSI (ou le Responsable Sécurité de l'Information) « incarne » la sécurité de l'information au sein de l'entreprise (ou dans un groupe d'entreprises) ou de l'autorité administrative. Le périmètre de son intervention est essentiel, mais la position hiérarchique nécessairement transversale du RSSI est également très importante dans la mesure où elle influe directement sur les pouvoirs et responsabilités de celui-ci. L'efficacité de la sécurité des systèmes d'information est ainsi conditionnée par son positionnement interne et les délégations de pouvoirs qui leur sont confiées. La sécurité des systèmes d'information s'entend de la sécurité physique et logique des matériels et systèmes (ordinateurs, réseaux, etc.) mais aussi d'une approche proactive et réactive en termes stratégiques et organisationnels.

Pour appréhender l'incidence du droit sur le RSSI, il est capital de partir de l'organisation de l'entité en cause (organigramme et périmètre des fonctions attribuées). Cette démarche est nécessaire puisqu'elle permet d'analyser les contraintes propres à l'entité et de prévoir les règles de sécurité qui lui seront applicables. À ce titre, il conviendra de mettre en place une politique de sécurité de l'information mais aussi une formalisation des obligations et responsabilités du RSSI : le Guide juridique du RSSI. Cela permet de mieux évaluer les risques juridiques qui relèvent de la fonction et le périmètre de ses attributions[121].

β) La chaîne documentaire de la Sécurité des systèmes d'informations

• La Politique de sécurité des systèmes d'informations

L'entreprise et les administrations doivent prévoir le rôle et les responsabilités de tous les acteurs concernés par la sécurité des systèmes d'information (utilisateurs, DSI, RSSI, prestataires externes, stagiaires, etc.). Le facteur humain est d'ailleurs

120. V. notamment les différentes études du CIGREF sur le site *www.cigref.fr*.

121. E. A. CAPRIOLI, *Régime juridique du Responsable Sécurité des Systèmes d'Information*, Livre bleu, t. III, oct. 2006, disponible sur le site *www.caprioli-avocats.com*; B. FORAY, *La fonction RSSI*, Dunod, 2007.

le premier facteur de risque, ce dernier étant souvent à l'origine de vols, de pannes, d'erreurs d'utilisation, de délits divers ou de malveillance. Le préalable à toute démarche de sécurité consiste à élaborer une Politique de sécurité des systèmes d'information (PSSI) fondée sur l'édiction de règles clairement définies. Toutefois, il est indispensable que les comportements illicites ou à risque puissent être sanctionnés (charte, contrat de travail et règlement intérieur). Mais la sécurité repose aussi sur la sensibilisation, l'information et la formation des salariés. La confidentialité est un autre facteur à prendre en compte et des règles de mise en œuvre de la politique suivie par l'organisation peuvent figurer au sein de la PSSI. Il s'agira notamment de procéder à la classification des informations générées, traitées et archivées sur le ou les système(s) d'information de l'entité et de déterminer les niveaux de confidentialité que les salariés et prestataires doivent respecter en fonction de leur rôle au sein de l'entreprise.

L'entreprise peut prévoir une politique de délégation de pouvoir en ce qui concerne la sécurité et l'administration des technologies de l'information. Ainsi, la responsabilité pénale correspondant aux fonctions déléguées ne sera plus supportée par le dirigeant mais par le délégataire. Ce dernier devra avoir eu connaissance de la délégation, l'avoir acceptée et l'entreprise délégante ne doit pas avoir participé à la commission de l'infraction [122]. Bien évidemment, les conditions de validité de la délégation devront être remplies (compétences du délégataire, appartenance de ce dernier au même groupe ou à la même société, délégation sans ambiguïté, certaine et opportune, moyens humains et financiers d'exercer la mission).

• Charte d'utilisation des communications électroniques

La charte d'utilisation des communications électroniques [123] constitue un recueil fonctionnel des règles applicables aux salariés et prestataires lorsqu'ils utilisent des moyens informatiques et des réseaux (matériels et logiciels) mis à disposition au sein de l'entreprise. Sans prétendre à l'exhaustivité, et en fonction de l'environnement technique de l'entreprise, cette charte devra intégrer une clause prévoyant l'interdiction du téléchargement ou de l'introduction d'œuvres protégées par le droit d'auteur sur les postes informatiques mis à la disposition des salariés, ou encore l'interdiction d'utiliser des outils cryptographiques autres que ceux définis par l'entreprise [124]. Cette précaution permettra d'évacuer tout risque de complicité encouru par l'entreprise en cas de téléchargement ou copie illicite effectué par un salarié pendant ses heures de travail. De plus, cette charte devrait inclure des éléments permettant l'administration des preuves et des traces informatiques qui conditionnent, en grande partie, la pertinence et l'efficacité des recours judiciaires

122. Cass. crim., 20 mai 2003 : *Bull. crim.*, p. 404.

123. L'opposabilité de la charte au salarié et les aspects de droit social ne sont pas abordés ici. V. E. A. CAPRIOLI, *Cybersurveillance des salariés : du droit à la pratique des chartes informatiques : LPA* 29 sept. 2004. V. également la table ronde intitulée *Cybersurveillance – Plaidoyer pour un humanisme numérique*, avec A. LEPAGE, E. A. CAPRIOLI, N. FORT : *Cah. dr. entrepr.*, n° 4, juill.-août 2005, p. 11 et s.

124. E. A. CAPRIOLI, note sous Cass. soc., 18 oct. 2006 : *Comm. com. électr.* janv. 2007, p. 40 et s.

de l'entreprise[125], voire à des fins de preuve pour dégager sa responsabilité. Les questions de la conservation des données de connexion et de la gestion des accès aux postes de travail et aux réseaux trouvent leur place dans un tel document. La simple adoption d'une charte sera insuffisante si l'entreprise ne prend pas le parti d'accompagner le changement par des actions de sensibilisation et de formation. La sécurité des systèmes d'information doit entrer dans la culture de l'entreprise, car le facteur humain est essentiel. Il va sans le dire que ce document doit évoluer dans le temps en fonction des changements de l'organisation, des technologies ou des évolutions des règles applicables et de la jurisprudence.

• Contrat de travail et règlement intérieur

L'élaboration d'une charte d'utilisation des communications électroniques ne se suffit pas à elle-même. Elle doit pouvoir être opposable à l'ensemble des salariés en l'intégrant comme annexe du contrat de travail des salariés ou, plus généralement, du règlement intérieur de l'entreprise. Le formalisme entourant cette opposabilité est spécifié :

- les instances représentatives du personnel doivent être consultées et informées de tout ce qui concerne les décisions de mise en œuvre dans l'entreprise de moyens techniques permettant un contrôle de l'activité des salariés (cybersurveillance) conformément à l'article L. 432-2, alinéa 1, du Code du travail ;

- les salariés doivent être informés de la mise en place de cette charte (art. L. 121-8 du Code du travail).

Tous les dispositifs techniques qui collectent et traitent des données à caractère personnel doivent être déclarés ou autorisés (biométrie) à la CNIL.

• Contrats avec les tiers

Il arrive souvent que des prestataires externes, des sous-traitants ou des stagiaires utilisent les systèmes d'information de l'entreprise. Cette utilisation doit être encadrée et contrôlée. Rappelons en cet endroit qu'en 2005, une stagiaire chinoise chez un équipementier automobile est accusée d'avoir copié des données (*a priori* confidentielles) sur son disque dur avant de les emporter chez elle. Le téléchargement anormal de fichiers alerte l'administrateur informatique. L'entreprise porte plainte en se fondant sur un « accès frauduleux dans un système automatisé de données et abus de confiance ». La jeune femme justifie l'« appropriation » de ces données par la rédaction de son rapport de stage ainsi que par le fait que ces données étaient parfaitement accessibles sur l'intranet de l'entreprise.

Ainsi, il conviendra de prévoir des clauses de confidentialité, de propriété intellectuelle, et de rendre opposable la Charte d'utilisation dans les différents contrats ayant trait à la sécurité des systèmes d'information de l'entreprise et qui sont conclus avec des tiers à l'entreprise.

125 V. E. A. CAPRIOLI, *La qualification d'une entreprise de « fournisseur d'accès »*, sous CA Paris, 4 févr. 2005 : *Dr. et patrimoine* sept. 2005, 3734, p. 108 et s.

b) L'assurance du patrimoine informationnel

Le professeur Linant de Bellefonds énonçait que « d'autres secteurs du droit évoluent sous la pression de ce phénomène nouveau (l'internet) : le droit des assurances, car la question de la sécurité des systèmes d'information est cruciale » [126]. Cette affirmation avant-gardiste rappelle à quel point l'assurance est devenue essentielle dans le domaine informatique. En effet, l'entreprise doit pouvoir compter sur la sécurité de son système d'information. Celle-ci transférera alors la couverture de la survenance d'un ou plusieurs risques sur un tiers : la compagnie d'assurances, ce qui se traduira par la souscription de plusieurs assurances couvrant les dommages et la responsabilité. L'exercice d'une activité nécessite forcément de se prémunir contre certains dommages pouvant la ralentir, voire la stopper. La négociation du contrat d'assurance devra être particulièrement surveillée. Il devra énumérer et définir les causes de dommages assurés. Il conviendra de vérifier que le niveau du montant des capitaux assurés est adapté à la situation de l'entreprise (pour éviter toute sous ou sur-assurance) ainsi que l'articulation et la définition des garanties souscrites. En matière de systèmes d'information, la garantie va retenir différents éléments. Ainsi, pour les supports informatiques, elle tiendra compte du remplacement des supports matériels (disques, disquettes, bandes,...) ainsi que des frais de report sur un matériel identique ou équivalent à celui qui a été endommagé ou détruit. Un contrat d'assurance spécifique pourra être prévu pour assurer la couverture des frais de reconstitution de l'information.

Au final, il apparaît que la dimension juridique occupe une place centrale au sein de la sécurité des systèmes d'information. Sa prise en considération tant par le législateur et le pouvoir réglementaire que par les décideurs d'entreprise prend de plus en plus de consistance dans la réalité opérationnelle. Goethe n'écrivait-il pas « l'enfer même a ses lois » !

Paris le 20 février 2007

126. X. LINANT DE BELLEFONDS, *L'informatique et le droit*, Paris, PUF, *op. cit.*, 1998, p. 8.