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 XX^e 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.