« *De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales ?* »

© Eric A. CAPRIOLI, Avocat à la Cour de Paris, Docteur en droit, chargé de cours à l'Université de Paris II, (Panthéon-Assas), Membre de la délégation française auprès de la C.N.U.D.C.I.[1]
e.caprioli@caprioli-avocats.com
www.caprioli-avocats.com

Sommaire

[1] L'auteur, bien qu'impliqué à des titres divers dans les travaux de la C.N.U.D.C.I., n'exprime dans le présent article que ses opinions personnelles. Celles-ci ne sauraient d'aucune façon engager la délégation française.

Introduction : Enjeux juridiques et sociaux

A l'heure des communications électroniques et des technologies de l'information, la criminalité et la fraude empruntent d'autres formes que celles traditionnellement rencontrées et ce, avec un essor décuplé. Avec les réseaux numériques, leur spectre d'intervention ne se limite plus à un pays ou une région, voire à un réseau international géographiquement localisé, il est planétaire et affecte le fameux « *village global* ». Cette sphère doit être entendue comme la zone mondiale interconnectée, celle qui est « *enrobée* » de réseaux de communications électroniques : filaires, hertziens, satellitaires, numériques[2].

L'accès aux réseaux est parfois considéré comme un droit fondamental ; en tous les cas, cet accès constitue un prérequis incontournable pour l'économie numérique. Cela signifie que plusieurs milliards d'individus[3] naviguent, communiquent, échangent, partagent, commercent, téléchargent, en leur nom propre comme au nom de leurs entreprises, associations ou organismes publics (Etats, collectivités locales, …). De plus, les technologies de l'information et de la communication (TIC) connaissent un développement sur tous les continents et dans tous les pays quel que soit leur niveau de développement économique[4]. Néanmoins, au regard des moyens technologiques utilisés, des spécificités locales ou régionales existent (ex : le mobile au Japon, en Afrique ou en Amérique latine).

D'une part, les communications électroniques se caractérisent par l'abrogation de l'espace géographique (distances, frontières) et du temps (tout est quasi-instantané, en temps réel). D'autre part, avec le web 2.0, elles sont interactives entre personnes et entre ces dernières et des contenus ou services hébergés et diffusés sur le web. En outre, le monde numérique, contrairement au monde physique, est par nature international : tout ce qui est diffusé sur les réseaux numériques est accessible de n'importe quel point du globe. Or, le réseau des réseaux constitue une mémoire collective de toutes les informations diffusées ; le droit à l'oubli n'existe pas en raison des reproductions et des stockages des informations réalisés dès la première publication sur l'internet, en des lieux soumis à des lois différentes.
De plus, les internautes sont amenés à avoir des relations avec des objets immatériels ou virtuels comme des serveurs ou des sites, ou à utiliser des biens incorporels comme les logiciels ou les bases de données[5]. Là aussi, il faut être certain que l'on est en relation avec la bonne personne morale qui détient les droits patrimoniaux sur ces objets complexes composés de droits intellectuels (noms de domaine, droit d'auteur, …) et de droits de propriété industrielle. Confronté à ce contexte, le besoin de confiance s'impose aux acteurs

[2] René-Jean Dupuy, *L'humanité dans l'imaginaire des nations*, Paris, Juilliard, Conférences, Essais et leçons du Collège de France, 1991.
[3] 1.966.514.816 connectés au 30 juin 2010, à l'adresse : http://www.internetworldstats.com/stats.htm.
[4] Pour un état de la situation des TIC dans les pays les plus pauvres, v. UNCTAD, *Information economy report 2010*, United Nations, New York and Geneva, 2010.
[5] Pierre Catala, *Le droit à l'épreuve du numérique, Jus ex machina*, Paris, P.U.F., 1998, voir le chapitre sur les bases de données.

de l'économie numérique dans la mesure où il est essentiel de pouvoir imputer une action ou une opération donnée à une personne déterminée[6]. Le développement de l'économie numérique auquel on assiste présentement ne va pas sans risques. Les questions de l'authentification et de la signature électronique des personnes doivent être traitées et résolues afin d'assurer au mieux la confiance dans les communications électroniques dans la mesure où ces méthodes ont des incidences juridiques importantes en terme de preuve des engagements et des faits juridiques[7]. Elles conduisent à s'interroger sur les manifestations de l'identité numérique, soit les données identifiantes qui constituent la personne juridique (en France, celles de l'Etat civil), et les identifiants qui peuvent se traduire par l'usage d'un simple login/mot de passe pour se logger, d'un certificat d'identification électronique, mais aussi : adresses électroniques, pseudonymes, noms de domaine, Url, adresses IP, traces informatiques, empreintes biométriques (doigt, iris, oreille)[8]. Parmi les nombreuses interrogations, certaines peuvent être relevées à ce stade, sans toutefois avoir vocation à l'exhaustivité.

Outre les questions de qui doit-on identifier et comment, doit-on s'identifier ou s'authentifier ?

- Pour une transaction en ligne ?
- Pour accéder à des données en ligne dont l'accès est réservé ?
- Comment gérer les droits d'accès des personnes habilitées ?
- Quels mécanismes sont mis en œuvre par ces deux modes de connexion[9] et comment répondent-ils aux différentes attentes du marché ?
- Quelles transactions requièrent une signature et comment cette signature se distingue-t-elle de l'authentification ?
- Peut-on signer avec un certificat émis à la volée et qui peut être utilisé pendant une durée très courte et pour une seule et unique transaction ?
- Quels types de signatures sont attendus par les acteurs de l'économie en ligne ?

---

[6] Eric A. Caprioli, *Sécurité et confiance dans le commerce électronique*, JCP éd G, n°14, 1 avril 1998, I, 123.

[7] Pierre-Yves. Gautier et Pierre Catala, *L'audace technologique à la cour de cassation : vers la libération de la preuve contractuelle*, JCP éd. G, 1998, p. 905 et s. ; Eric A. Caprioli, *Preuve et signature dans le commerce électronique*, Droit et Patrimoine, n°55, Décembre 1997, p. 56-61.

[8] Eric A. Caprioli, *Traitement utilisant des données biométriques*, Comm. Com. Electr. n°3, 1 mars 2007, comm. 48 ; Eric A. Caprioli, *Généralisation du passeport* biométrique, Comm. Com. Electr. n°7, juillet 2008, comm. 98.

[9] Le service d'authentification permet de garantir l'intégrité et l'origine du message des données authentifiées mais, contrairement au service de signature électronique, il ne signifie pas que l'émetteur manifeste son consentement au contenu du message des données. Voir en ce sens, le RGS (Référentiel Général de Sécurité), rédigé par l'Agence Nationale de la Sécurité des Système d'Information (ANSSI) et par la Direction Générale de la Modernisation de l'Etat (DGME), a été pris en application de l'article 9 de l'ordonnance du 8 décembre 2005 (Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, JO n°286 du 9 décembre 2005, p. 18896 et s. ; Eric A. Caprioli, *Des échanges électroniques entre les usagers et les autorités administratives d'une part, et entre ces dernières d'autre pa*rt, JCP éd. A et CT, 2006, n°1079, p. 432 et Comm. Com. Electr. avril 2006, n°4, comm. 75). Le RGS définit un ensemble de règles de sécurité s'imposant aux autorités administratives dans le but de sécuriser leur système d'information dans le cadre d'échange des informations par voie électronique et notamment l'authentification. Son décret d'application a été publié au Journal Officiel du 4 février 2010 (Décret n°2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, JO 4 février 2010, p. 2072) suivi d'un arrêté ministériel en date du 6 mai 2010 (JO du 18 mai 2010), qui approuve la version 1.0 du RGS.

- Enfin, quel cadre juridique envisager pour la reconnaissance juridique internationale des moyens d'authentification et de signature électroniques ?

Par ailleurs, l'émergence de l'informatique dans les nuages ou « Cloud computing », associée aux services proposés en mode SaaS, doit permettre de garantir la conformité juridique des opérations, spécialement le contrôle et le suivi des identités des utilisateurs de ces services, ainsi que leurs activités sur les données et les infrastructures. En ce domaine encore, la confiance passe par la mise en place de méthodes d'authentification et de signature électroniques fiables (ex : SSO, OTP, certificats, …). La sécurité et la confidentialité des informations, ainsi que leur lieu d'hébergement sont des questions clés notamment en termes contractuels et de conformité aux règlementations sur la protection des données à caractère personnel.

A l'accès aux informations et aux services, on peut étroitement associer l'authentification qui le permet. Les règles de sécurité associées aux diverses méthodes sont plus ou moins fiables et leur utilisation dépendra de la sécurité juridique recherchée.… Nonobstant les lois et règlements relatifs à la conformité qui s'imposent, une analyse de risques sera déterminante (ex : la norme internationale ISO 27005 ou en France, la méthode EBIOS).

Le développement des technologies de l'information a fait émerger différentes méthodes pour relier une donnée sous forme numérique à une personne ou une entité définie et ceci afin d'assurer l'intégrité de l'information ainsi que de permettre à cette personne ou entité de démontrer qu'elle a le droit ou l'autorisation d'accéder à un certain service ou à une certaine source d'information. Sur le plan juridique, les acteurs doivent pouvoir se fier à l'identité numérique d'une personne, afin d'être en position de lui imputer un acte ou un fait juridique. Pour assurer une bonne gestion des risques juridiques, chaque partie doit être en mesure d'avoir une confiance raisonnable en l'identité numérique déclarée ou vérifiée, selon le besoin et la nature de l'opération en cause. Ces besoins d'authentification et de signature électronique existent tant au sein d'une entreprise ou d'un groupe, que dans les relations commerciales, tant en droit interne, qu'en droit international. En cas de différend, l'identité d'une personne reste incontournable pour introduire une action en justice contre celle-ci, devant un tribunal territorialement compétent.

Cette prise de conscience impose de soumettre les acteurs économiques aux nouvelles exigences liées à la sécurisation de leurs activités, notamment via les méthodes d'authentification et d'identification. Ainsi, l'étude du cadre juridique des méthodes d'authentification, d'identification et de signature électronique s'avère essentielle pour déterminer les enjeux sociétaux, économiques et politiques des communications électroniques internationales.

L'œuvre normative de la C.N.U.D.C.I. a été continue et fournie depuis sa fameuse loi-type sur le commerce électronique de 1996 sur laquelle les fondations de la confiance se sont progressivement construites au niveau international[10]. Pourtant, lors de sa recommandation

[10] Eric A. Caprioli et Renaud Sorieul, *Le commerce électronique international : vers l'émergence de règles juridiques transnationales*, Journal du Droit international (Clunet) 1997, p.323 s ; Olivier Cachard, *La régulation internationale du marché électronique*, L.G.D.J., Bibl. de dr. privé, 2002 ; Ugo Draetta, *Internet et commerce électronique en droit international des affaires*, Paris et Bruxelles, F.E.C. et Bruylant, Collection feduci, 2003, p.

de 1985, reprise par une résolution de l'Assemblée générale des Nations Unies du 11 novembre 1985 concernant l'utilisation des traitements automatiques de l'information[11], la C.N.U.D.C.I. recommandait déjà aux Gouvernements :
« *c) de réexaminer l'exigence légale d'une signature manuscrite ou de toute autre méthode d'authentification sur papier pour les documents commerciaux afin de permettre, le cas échéant,* ***l'utilisation de moyens électroniques d'authentification*** *;* ».

Par la suite, les travaux de la C.N.U.D.C.I. ont conduit à l'adoption de la loi-type sur le commerce électronique en 1996[12], de la loi-type sur les signatures électroniques en 2001[13] et de la Convention des Nations Unies sur l'utilisation des communications électroniques dans les contrats internationaux en 2005[14]. Ces instruments juridiques ont largement contribué à l'harmonisation des dispositions législatives nationales applicables aux signatures électroniques[15].

Outre les aspects juridiques de chaque système juridique sur l'authentification et la signature électronique, les principales questions juridiques liées à leur utilisation et à leur reconnaissance transfrontières lors d'opérations internationales ont été identifiées à l'occasion de la publication indépendante du secrétariat de la CNUDCI remarquée lors de la

---

101 s. ; Eric A. Caprioli, *Droit international de l'économique numérique*, préface de Renaud Sorieul, Paris, Litec, 2ème éd., 2007 ; Amelia H. Boss, *The United Nations Convention on the Use of Electronic Communications in International Contracts,* Kluwer Law International, 2008 ; José Angelo Estrella Faria, *Convention des Nations Unies sur l'utilisation des communications électroniques dans les contrats internationaux*, Journal du Droit international (Clunet), 2006, p. 393 et s*. ;* Corinne Montineri, *Un droit moderne pour le commerce mondial,* Journal du Droit international (Clunet), n°4, octobre 2007, biblio. 24.

[11] CNUDCI, Doc. A/CN.9/265, du 21 février 1985, v. §82. En outre, la Commission avait recommandé aux Etats :
« *a) de réexaminer les règles juridiques touchant l'utilisation des enregistrements informatiques comme moyens de preuve en justice afin d'éliminer les obstacles superflus à leur recevabilité, de s'assurer que ces règles sont compatibles avec les progrès techniques et de donner aux tribunaux les moyens leur permettant d'apprécier la fiabilité des données contenues dans ces enregistrements ;*
b) de réexaminer les règles juridiques en vertu desquelles certaines transactions commerciales ou certains documents ayant trait au commerce doivent être sous forme écrite, que cette forme écrite soit ou non une condition requise pour que la transaction ou le document soit valide ou s'impose aux parties, afin de faire en sorte que, le cas échéant, la transaction ou le document puissent être enregistrés et transmis sur support informatique;
(…)
d) de réexaminer les règles juridiques selon lesquelles les documents à soumettre à l'administration doivent être présentés par écrit et doivent porter une signature manuscrite en vue d'autoriser leur présentation sur support informatique aux services administratifs qui ont acquis les équipements nécessaires et mis en place les procédures requises ; ».

[12] E. Caprioli, *Un texte précurseur en matière de commerce électronique : la loi type de la Commission des Nations Unies pour le commerce international (CNUDCI)*, Droit de l'Informatique et des Télécoms 96/3, p. 88.

[13] E. Caprioli, *Le projet de règles uniformes de la C.N.U.D.C.I. sur les signatures électroniques : ébauche d'une harmonisation internationale*, in *Droit et économie du savoir, Journées Maximilien-Caron 2000*, Montréal, éd. Thémis, 2001, p.103 s. ; E. Caprioli, *La loi type de la CNUDCI sur les signatures électroniques (Vienne 23 juin - 13 juillet 2001)*, Comm. Com. Electr. 2001, n°12, p.9 ; *Commentaire sur Loi type de la CNUDCI sur les signatures électroniques réalisé par le CRI*D, sous la coordination de H. Jacquemin, consultable à l'adresse : http://mineco.fgov.be/internet_observatory/pdf/legislation/cmt/law_un_2001-07-05_cmt_fr.pdf.

[14] Cette convention n'était pas en vigueur au 11 février 2011. Au 1er mars 2011, les Etats ayant ratifié l'instrument sont au nombre de 2, le Honduras et Singapour. V. sur le site : www.uncitral.org.

[15] Loi-type de la CNUDCI sur le commerce électronique, 1996, v. l'article 7 ; Loi-type de la CNUDCI sur les signatures électroniques, 2001, v. les articles 1, 8, 9, 11 ; Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux, 2005, v. l'article 9.

quarantième session de la Commission en 2007[16]. L'intervention de tiers, prestataires de services de confiance, présente des difficultés spécifiques, notamment pour ceux qui, dans le cadre d'une infrastructure à clé publique (ICP), émettent et gèrent des certificats d'authentification, de signature électronique ou permettant le chiffrement de données.

En effet, chaque application appellera un flux spécifique de données – identification, authentification, signature ou chiffrement – qui dépend du niveau de sécurité des informations échangées sur le web, mais également de son cadre juridique. Certains Etats se sont d'ores et déjà saisis de la question de l'identification sur les réseaux, en incluant dans leur titre national d'identité plusieurs catégories de certificats, publics ou privés[17].

A titre d'exemple, la dématérialisation des moyens de paiement – virements, cartes de crédit, prélèvements - fait depuis longtemps appel à des mécanismes relativement robustes de confirmation d'identité et de solvabilité[18]; les moyens traditionnellement admis (usages) ne suffisent plus à garantir une identité dans le cadre de l'économie numérique. Ainsi, une simple adresse électronique suffit-elle à garantir l'identité d'un commerçant ? Avec le développement actuel de l'économie numérique, des règles fiables, traduites sous forme de normes juridiques internationales, doivent être instaurées pour prévenir les menaces de fraude et pour garantir un niveau de confiance suffisant. L'utilisation des communications électroniques dans les contrats commerciaux internationaux ne peuvent plus reposer uniquement sur les moyens classiques de reconnaissance mutuelle des parties (valables si les parties sont dans une relation courante d'affaires, … car une fraude ou une usurpation d'identité peut affecter les communications électroniques)[19], mais sur les nouvelles méthodes d'authentification et de signature électronique (3D Secure[20], PCI-DSS)[21].

En outre, bien que se situant hors du domaine d'intervention de la C.N.U.D.C.I., il convient de souligner que sur le plan de la cybercriminalité, la gestion de l'identité numérique a de multiples incidences juridiques. Des travaux ont été initiés récemment dans le cadre de

---

[16] V. *Documents officiels de l'Assemblée générale, soixantième et unième session, supplément no 17* (A/61/17), paragraphe 21 ; v. aussi *Promouvoir la confiance dans le commerce électronique : questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signatures électroniques,* CNUDCI, Vienne 2009. Disponible sur http://www.uncitral.org/pdf/french/texts/electcom/08-55699_Ebook.pdf.

[17] Voir notamment la carte d'identité électronique en Belgique (eid) à l'adresse : http://welcome-to-e-belgium.be/fr/ ; en Estonie (Card id, disponible à l'adresse www.id.ee) ; en Italie (http://www.cnipa.gov.it).

[18] A titre d'exemple, le réseau des cartes de paiement certifie – quasiment en temps réel – la solvabilité de l'acheteur mais également la possession légitime du titre par la génération du code PIN et son contrôle lors des transactions.

[19] L'envoi de documents bancaires et de pièces d'identité à des inconnus peuvent servir à de nombreuses fraudes non seulement à l'encontre des personnes physiques, mais aussi des entreprises.

[20] Rappelons ici que 3D Secure est un protocole sécurisé de paiement sur l'Internet. Il consiste à s'assurer, lors de chaque paiement en ligne, que la carte est bien utilisée par son titulaire. Ainsi, en plus du numéro de carte bancaire, de la date d'expiration de la carte et des trois chiffres du code de sécurité (imprimés au dos de la carte), l'internaute doit saisir un mot de passe, tel que sa date de naissance ou un code dynamique à usage unique. Voir notamment le site : http://visa-europe.fr/fr.

[21] Le *Payment Card Industry Data Security Standard* (PCI DSS) est un standard de sécurité des données pour l' industrie des cartes de paiement créé par le comité PCI SSC pour les plus importantes entreprises de carte de débit et crédit (Visa, MasterCard, American Express, Discover, JCB). Cette norme comporte 12 exigences applicables aux commerçants en ligne et aux fournisseurs de services de paiement en vue de protéger leurs données et de prévenir les fraudes. Voir notamment http://fr.pcisecuritystandards.org/_onelink_/pcisecurity/en2frfr/doc/pci_dss_v1-2.pdf.

l'UNODC à Vienne (United Nations Office on Drugs and Crime[22]) et pourraient aboutir à une convention internationale sur la cybercriminalité dans la lignée de la Convention du Conseil de l'Europe du 23 novembre 2001[23].

S'agissant des règles juridiques internationales, elles constitueraient une avancée significative dans un domaine où l'authentification est souvent encadrée de manière purement contractuelle. Dans la plupart des systèmes juridiques, seule la signature électronique à laquelle une valeur juridique est associée et l'écrit électronique qui en résulte, font l'objet de dispositions législatives[24].

Si l'identité est un concept complexe, elle peut cependant se manifester sous des formes très diverses dans l'univers numérique, en fonction des utilisations. C'est pourquoi, il faut à ce stade bien distinguer l'identité sous forme numérique qui relève de la puissance régalienne de certains Etats comme la France et les identifiants numériques qui peuvent aller de la simple adresse de messagerie électronique, à un login/mot de passe, en passant par une adresse IP ou une signature manuscrite scannée[25]. Les effets juridiques de ces dispositifs techniques doivent être différenciés étant donné qu'ils varient en fonction de l'importance accordée à l'opération en cause.

La présente étude a pour objectif de présenter les données de base de la gestion de l'identité numérique (ou des identités) et de tracer quelques pistes de réflexion en vue d'assurer la mise en œuvre de règles juridiques internationales par une autorité légitime (la C.N.U.D.C.I.) afin de combler des carences importantes en la matière. Il en va de la confiance dans l'économie numérique.

---

[22] Pour les travaux de l'Office des Nations Unies contre la drogue et le crime, v. le site : www.unodc.org/.

[23] Myriam Quéméner, *Lutte contre la cybercriminalité. Où en est-on des instruments internationaux?*, Expertises, Mars 2011, spéc. p.98-99. V. égal., Gilberto Martins de Almeida, *Typology and criminalization approaches to identity-related crime: Compendium of examples of relevant legislation*, à paraître sur le site de l'UNODC. Sur la Convention du Conseil de l'Europe, v. Eve Tourny, *La lutte contre la criminalité informatique en matière bancaire : approches de droit comparé et de droit international*, Thèse pour le Doctorat en droit, Université de Nice Sophia Antipolis, 27 Mai 2011, p.329 s.

[24] V. pour la France : 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 (JO n° 62 du 14/05/2000 p. 3968), Décret d'application n° 2001-272 du 30 mars 2001 (JO n° 77 du 31 mars 2001), 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 (JO n° 92 du 19 avril 2002) ; pour la Belgique : Loi n° 2000/10017 du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire (Moniteur Belge du 22/12/2000, p.42698), Arrêté royal du 6 décembre 2002 organisant le contrôle et l'accréditation des prestataires de service de certification qui délivrent des certificats qualifiés (Moniteur belge du 17/01/2003) ; pour le Luxembourg : Loi du 14 août 2000 relative au commerce électronique (JO n° 96 du 8/09/2000 p. 2176), le règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du comité commerce électronique (JO n° 71 du 22 juin 2001 p. 1429), le règlement grand-ducal du 21 décembre 2004 portant organisation de la notification des prestataires de services délivrant des certificats qualifiés, mettant en place un système d'accréditation des prestataires de services de certification, créant un comité signature électronique et déterminant la procédure d'agrément des auditeurs externes (JO n° 21 du 14/02/2005 p. 418).

[25] La représentation graphique de la signature manuscrite peut être contrôlée par le signataire (ex : avec un mot de passe) ou non. Juridiquement, la fiabilité du procédé et sa sécurité sont essentielles étant donné les conséquences qui peuvent être associées à une signature.

Ainsi, après avoir procédé à l'analyse de l'environnement juridique et normatif de la gestion d'identité (I), les diverses possibilités de leur mise en œuvre juridique internationale seront envisagées (II).

I. Cadre juridique et normatif de la gestion de l'identité

Afin d'analyser les principaux concepts associés à la gestion de l'identité numérique, la démarche retenue nous conduira à exposer les éléments de définition des principaux concepts relatifs aux méthodes d'authentification et de signature électronique (A) avant de préciser les exigences techniques et juridiques (conformité légale et règlementaire) nécessaires à la mise en œuvre de l'identité numérique (B).

A. Eléments de définitions

Avant de pouvoir, tracer les contours juridiques que pourrait emprunter la gestion de l'identité numérique, il s'agira de poser plusieurs définitions dans un domaine où la complexité est de mise et où la dimension technique a fortement influencer les pratiques et les usages. Mais certaines normes juridiques impératives s'applique ; il en va ainsi des dispositions relatives à la protection des données personnelles étant donné que la gestion des identités numériques implique la collecte, le traitement voire la conservation de données permettant d'identifier directement ou indirectement une personne physique[26].

Ce préalable nécessaire passe par l'examen des termes utilisés comme l'authentification, la signature électronique, ce qui nous amènera à présenter les principales techniques utilisées dans le cadre des échanges électroniques.

1. Authentification[27]

La sécurité dans les communications électroniques induit un besoin accru en matière d'identification des personnes, de sorte que l'authentification prend alors le relais sur l'identification physique traditionnelle avec, pour finalité, de vérifier l'identité dont une entité (personne ou machine) se réclame.

Dans les pays européens de tradition civiliste, le concept d'authentification est interprété de façon assez étroite. Il signifie que l'authenticité d'un document a été vérifiée et certifiée par une autorité publique compétente (juridiction ou Etat civil) ou un officier public et ministériel dont les pouvoirs ont été délégués par une autorité publique (notaires, huissiers de justice). En procédure civile, il est courant de se référer plutôt à la notion de « *document original* ». Dans cette logique, le caractère authentique d'un document renvoie à sa nature

[26] Le sujet de la protection des données à caractère personnel mériterait de plus amples développements que ceux contenus dans la présente étude qui se contente d'évoquer les questions y afférentes comme par exemple en matière de données biométriques, v. infra I.A.6.

[27] *« Mécanisme de sécurité qui permet de s'assurer de l'authenticité de l'émetteur ou du récepteur d'un message. L'authentification peut être simple (utilisation d'un mot de passe) ou complexe (recours au chiffrement). Authentification de l'origine des données : confirmation que la source des données est telle que déclarée »*, in *Dictionnaire de l'informatique,* sous la direction de Pierre Morvan, Larousse, 1996, V°Authentification (en anglais : authentication).

sincère[28], c'est-à-dire qu'il émane bien des signataires, qu'il constitue l'*instrumentum* « original » des informations qu'il contient, sans altération ni modification depuis son établissement.

Pendant longtemps, en l'absence de définition juridique[29] précise de l'authentification au niveau européen, il a fallu se référer aux dispositions relatives à la signature électronique en tant que méthode d'authentification. En effet, l'article 2 de la directive 1999/93/CE[30] du 13 décembre 1999 du Parlement européen et du Conseil, sur un cadre communautaire pour les signatures électroniques définit la signature électronique comme « *une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui* ***sert de méthode d'authentification*** ». En outre, un certificat constitue un dispositif de vérification d'une signature électronique ; il est défini par l'article 2-9 de la directive comme « *une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne* ». S'agissant d'un « certificat qualifié », selon l'article 2-10, c'est : « *un certificat qui satisfait aux exigences visées à l'annexe I et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II* ».

La première véritable définition juridique de l'authentification a été introduite dans le Règlement communautaire n° 460/2004 du 10 mars 2004[31] instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA). Selon son article 4-e, l'authentification doit être entendue comme « *la confirmation de l'identité prétendue d'entités ou d'utilisateurs* ». Cette définition est assez large puisqu'elle intègre les personnes morales.

Dans le contexte international, ni la Loi type de la CNUDCI sur le commerce électronique[32] ni la Loi type de la CNUDCI sur les signatures électroniques[33] n'emploient le terme « *authentification électronique* », en raison du sens différent attribué au mot « authentification » dans divers systèmes juridiques et de la confusion possible avec des procédures ou des exigences de forme particulières. Par ailleurs, s'il est fait état de

---

[28] Eric A. Caprioli, *La sincérité de la signature électronique*, in *La sincérité en droit*, (sous la coordination de Olivier Le Bot), Bruxelles, Larcier, 2011, v. p.111-127 ; disponible à l'adresse : http://www.caprioli-avocats.com.

[29] Il existe des définitions purement techniques de l'authentification, elles ne sont pas prises en compte dans le cadre de la présente analyse qui se situe sur un plan juridique.

[30] J.O.C.E., L 13 du 19 janvier 2000, p. 12 et s. V. notamment : Pierre Catala, *Le formalisme et les nouvelles technologies,* Defrénois 2000, p.897 s. ; Eric A. Caprioli, *La loi française sur la preuve et la signature électroniques dans la perspective européenne*, J.C.P. éd. 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 octobre 2000, p. 5 et s. ; *Eric A. Caprioli, Sécurité et confiance dans les communications électroniques en droits français et européen, in Libre droit, Mélanges Ph. Le Tourneau, Dalloz, 2008, p. 155 et s*., disponible à l'adresse : http://www.caprioli-avocats.com/pdf/securite-informatique-electronique.pdf. ; Pierre Yves Gautier et Xavier Linant de Bellefonds, *De l'écrit électronique et des signatures qui s'y attachent*, JCP éd. G, I, 236, 2000, p. 1113 et s ; Pierre Leclercq *Le nouveau droit civil et commercial de la preuve et le rôle du juge, Le droit des preuves au défi de la modernité*, Actes du colloque du 24 mars 2000, éd. La documentation française, 2000.

[31] J.O.C.E L 077, 13 mars 2004, p.1 et s.

[32] Loi-type de la CNUDCI sue le commerce électronique et Guide pour son incorporation, 1996 avec article 5bis tel qu'ajouté en 1998, Publication des Nations Unies, accessible sur le site Internet : http://www.uncitral.org/pdf/french/texts/electcom/ml-elecsign-f.pdf.

[33] Loi-type de la CNUDCI sur la signature électronique et Guide pour son incorporation, 2001, accessible sur le site Internet : http://www.uncitral.org/pdf/french/texts/electcom/ml-elecsign-f.pdf.

l'authentification dans le Guide d'incorporation de la loi type de la CNUDCI sur le commerce électronique[34], elle n'a trait qu'à l'authentification des messages ou des données.

La responsabilisation des acteurs sur l'Internet est encore en développement. Elle a reçu récemment quelques confirmations importantes de la part de la justice américaine. Notamment, dans une décision du Tribunal de l'Illinois, dans une affaire Shames Yeakel vs Citizen Financial Bank en date du 21 août 2009 (Case 07 C 5387)[35], les juges ont accueilli favorablement la plainte d'une victime d'une cyber-attaque sur son compte bancaire en ligne, déposée contre l'établissement bancaire. Ce jugement remettait en cause l'authentification à facteur unique (un seul canal d'identification comme l'identifiant/mot de passe) pour protéger l'accès aux comptes bancaires en ligne. Ainsi, dans le cadre de l'authentification au moment de l'accès aux comptes bancaires via l'Internet, l'établissement bancaire est tenu de satisfaire aux normes techniques et sécuritaires généralement admises et proportionnées aux risques liés à ses produits et services, qui sont considérées comme les seules suffisantes. Le jugement en question fournit par ailleurs, une liste des méthodes mises en place par ces institutions financières afin de procéder à l'authentification de leurs clients. Cette liste comprend notamment l'utilisation de mots de passe, de numéros personnels d'identification (PINs), de certificats électroniques, de supports physiques tels que les smart cards ou les clés USB, de mots de passe uniques (OTPs) ou d'autres types de « tokens », des procédés biométriques, etc.

En France, la Cour d'appel de Versailles le 18 novembre 2010[36] a eu à juger une question de sécurité connexe pour engager la responsabilité d'une banque. Dans cette affaire, on peut constater que l'authentification, plus qu'un simple moyen de vérification de l'identité d'une personne, doit être considérée comme une véritable mesure de sécurité pour la gestion des accès) à l'instar de ce que précise la norme ISO 27001[37].

En l'espèce, une femme, agent de la RATP, a saisi la justice à l'encontre de la banque dans laquelle elle avait constitué une épargne salariale d'entreprise. Elle demandait le remboursement de la somme de 13.244,85 euros prélevée de son compte bancaire par son époux avec lequel elle était en instance de divorce.

Les magistrats observent que « *dans un premier temps, l'épargnant qui souhaitait consulter en ligne ses comptes sur le site internet de la société intimée pouvait accéder à son espace sécurisé en saisissant ses identifiants tels que le numéro d'entreprise et le code serveur qui étaient mentionnés sur les relevés adressés à titre personnel au titulaire ; qu'ensuite, l'utilisateur devait nécessairement, s'il voulait effectuer une opération, utiliser un mot de passe ; qu'ainsi la réalisation de toute opération telle que demande de remboursement d'avoirs disponibles ou demandes de transfert, requéraient l'utilisation par l'épargnant du mot de passe, qu'on lui laissait créer lui-même lors de sa première connexion* ».

[34]Guide pour l'incorporation de la loi type CNUDCI sur le commerce électronique, n° 39 et s., http://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf.
[35]Commentaire par Eric Caprioli, *Première décision américaine concernant l'authentification par voie électronique d'un client bancaire*, Communication Commerce Electronique (LexisNexis) n° 4, Avril 2010, comm. 41.
[36] Décision N° 09/06634, Marie-Maure C. épouse A. c/ SA Natixis Interepargne.
[37] ISO/IEC 27001 :2005 v. le § 16.

Ainsi, pour les juges « *l'utilisation du compte épargne entreprise à l'insu de la titulaire, notamment par son époux, avec lequel elle était alors en instance de divorce, restait alors possible, tout tiers suffisamment proche de Mme X pour entrer en possession de ses relevés de compte n'ayant qu'à créer lui-même un premier mot de passe pour se rendre maître des sommes non bloquées qui étaient déposées sur ce dernier* ».

Au surplus, une modification ultérieure de son système de sécurisation des comptes, consistant en l'émission du mot de passe par la banque et sa communication par courrier séparé de celui portant le code identifiant démontrait que la banque « *avait bien conscience de ce que dans une première période de gestion en ligne des comptes individuels de ses clients, elle ne remplissait pas totalement son obligation de sécurité et donc de sécurisation des opérations de gestion informatique de ces comptes.* ». La banque se voit donc condamnée à rembourser à la titulaire du compte la moitié des sommes débitées frauduleusement par son époux (correspondant à la hauteur des sommes lui revenant à l'issue de la procédure de divorce) sur le fondement de son manquement à l'obligation de sécurité. Cependant, la Cour d'appel a également reconnu que la banque était fondée à agir en garantie contre le conjoint indélicat.

A la suite de demandes répétées de la Banque de France concernant la hausse du niveau de sécurisation des activités de banque en ligne, le Groupe d'expertise FBF-BDF a travaillé jusqu'en mars 2009 sur l'authentification et la sécurité des paiements sur l'Internet (Rapport du 2 mars 2009 au COMP). La principale recommandation consiste en l'usage d'un mot de passe aléatoire pour l'authentification lors de virements sur l'Internet ou d'autres opérations sensibles (services d'émission de chèque dématérialisé, commandes de moyens de paiement, services de mise à jour de toute donnée client permettant une prise de contrôle, même partielle, du compte - changement d'adresse courrier, etc. - ou des données pouvant être utilisées par la banque pour authentifier son client - selon les cas : numéro de portable, adresse email, etc. -, services de coffre-fort électronique).
L'objet de cette recommandation est de garantir ainsi un niveau de sécurité considéré comme élémentaire à l'aide d'une solution dynamique non rejouable.

Par ailleurs, la Banque de France considère que certaines données (identifiants de compte type BIC/IBAN, numéros de carte) affichées ou utilisées via la banque en ligne revêtent une certaine sensibilité en raison de leur possible réutilisation frauduleuse via le canal de l'Internet ou sur d'autres canaux (paiement par prélèvement ou paiement par carte sur certains sites sur l'Internet).

C'est la raison pour laquelle la Banque de France appelle les établissements bancaires à être vigilants vis-à-vis de l'affichage de ces identifiants de compte ou de carte en clair sur leurs sites de banque en ligne, lorsque ceux-ci ne sont pas sécurisés dès la connexion par une authentification non rejouable.

De même, la Banque de France considère que la saisie des numéros de compte comme identifiants lors de la connexion ne constitue pas une bonne pratique en termes de sécurité. Elle recommande aux établissements d'employer un autre type d'identifiant pour la connexion de ses clients, ou à défaut d'étudier la mise en œuvre de mesures palliatives afin de dissimuler totalement ou partiellement ces données à la saisie.

Ainsi, les méthodes d'authentification fortes sont plus fiables et permettent de prévenir des cas de fraude plus efficacement. Par exemple, la protection assurée par l'utilisation d'un mot de passe et d'un identifiant est une authentification à un facteur (l'utilisateur fournit uniquement une information qu'il possède) tandis qu'une méthode d'authentification forte impose une combinaison de deux canaux distincts et de deux facteurs : un en ligne, l'autre généré de façon aléatoire (non rejouable) via le téléphone mobile ou un One time Password (OTP).

2. Identification

L'identification peut être définie comme une opération permettant à un individu de faire état de son origine sur la base d'un élément externe, d'exprimer son identité. Elle peut être réalisée par le biais de tout document pouvant attester de l'origine d'une personne (extrait de naissance, carte d'identité, permis de conduire, passeport), mais également sur la base du témoignage de tiers. En revanche, cette procédure n'exige pas que soit constitué un lien physique entre la personne et l'élément externe qui atteste de son origine. S'identifier c'est donc communiquer une identité préalablement enregistrée, s'authentifier, c'est apporter la preuve de son identité. Cette dernière recouvre «*l'ensemble des composantes grâce auxquelles il est établi qu'une personne est bien celle qui se dit ou que l'on présume telle (nom, prénoms, nationalités, filiation...)*»[38], ainsi que tous « *les traits juridiquement pertinents qui se retrouvent aussi bien dans le numéro national d'identification attribué par l'INSEE que sur la carte nationale d'identité délivrée par le ministre de l'intérieur ou sur les actes de l'état civil.*»[39].

L'identification des personnes constitue la condition sine qua none de la sécurité des échanges sur les réseaux numériques, qu'il s'agisse de transactions commerciales ou administratives (télé-services) ou de simples correspondances privées. Ainsi, dès le moment où l'on considère que le droit à l'anonymat[40], sous réserve notamment de l'article 6-III-2 de la Loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004[41] ne trouve pas à s'appliquer dans l'univers des réseaux numériques comme l'internet, plusieurs risques juridiques devront être pris en compte, notamment :

- Les risques liés à la **dénégation d'un acte juridique conclu par voie électronique** (remise en cause d'un engagement/contrat sur les réseaux) ;

---

[38] *Lexique des termes juridiques*, éd. Dalloz, 1999, p. 280, V° Identité. Selon Gérard Cornu : « *Pour une personne physique* : *ce qui fait qu'une personne est elle-même et non une autre ; par ext., ce qui permet de la reconnaître et de la distinguer des autres ; l'individualité de chacun, par ext. L'ensemble des caractères qui permettent de l'identifier* », *Vocabulaire juridique,* Quadrige/PUF, 2000, p. 431, V° Identité.

[39] Alain Supiot, *L'identité professionnelle*, in *Les orientations sociales du droit contemporain. Ecrits en l'honneur du Professeur J. Savatier*, P.U.F., 1992, p. 409 et s.

[40] Jacqueline Pousson-Petit, *Le droit à l'anonymat,* in *Mélanges dédiés à Louis Boyer,* Presse de l'Université des Sciences sociales de Toulouse, 1996, p. 595 s. ; Eric A. Caprioli, *Anonymat et commerce électronique,* in *Les premières journées internationales du droit du commerce électronique, Actes du colloque de Nice des 23, 24 et 25 octobre 2000 organisé par le Département Sciences Juridiques de l'EDHEC et l'Ecole du Droit de l'Entreprise de la Faculté de Droit de l'Université de Montpellier, sous la responsabilité scientifique de Eric A. Caprioli,* Litec, 2002, v. p. 149 s.

[41] « *2. Les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné au 2 du I, sous réserve de lui avoir communiqué les éléments d'identification personnelle prévus au 1.* »

- Les risques liés à une **utilisation délictuelle des données personnelles et des réseaux** (par exemple, infractions liées aux actes de paiement, aux dénis de service (saturation), ou infractions facilitées ou liées à l'utilisation des technologies de l'information : diffusion de contenus illicites (pédopornographie, racisme, antisémitisme, etc.), escroqueries par utilisation frauduleuse de numéros de carte bancaire pour une transaction en ligne (phishing[42]) ou de données sociales, les escroqueries par fausses ventes sur un site d'enchères en ligne, les contrefaçons de logiciels ou d'œuvres audiovisuelles, que ces actes soient effectués à partir d'un ordinateur situé au domicile d'une personne ou dans une entreprise[43].

En France, par exemple, en vertu de l'article 6-II de la LCEN, les fournisseurs d'accès et les hébergeurs de contenus sont soumis à une obligation de détenir et de conserver les données de nature à permettre l'identification des personnes qui ont contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires[44]. Cependant, ces « identifications » ne touchent que les contenus diffusés sur l'internet et non pas les transactions ou les accès en ligne à des données ou à des services[45]. D'où, nonobstant la

[42] Eric A. Caprioli, *Le phishing saisi par le droit* (TGI Paris, 31ème chambre, 21 sept. 2005, Microsoft Corporation / Robin B), Comm. Com. Electr. Février 2006, p. 48, n°37.

[43] Myriam Quéméner et Yves Charpenel, *Cybercriminalité, Droit pénal appliqué*, Economica, 2010 ; Abbas Jaber, *Les infractions commises sur Internet*, Paris, L'Harmattan, Préface de Hervé Bonnard, 2009 ; Eric A. Caprioli, *Le risque pénal dans l'entreprise et les technologies de l'information*, JCP E, 2006, Cah. Dr. Entrep., janvier-février 2006, n°10.

[44] II. (…) *« Elles fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues au III.*
L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa.
Les dispositions des articles 226-17, 226-21 et 226-22 du code pénal sont applicables au traitement de ces données.
Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation.
III. - 1. Les personnes dont l'activité est d'éditer un service de communication au public en ligne mettent à disposition du public, dans un standard ouvert :
a) S'il s'agit de personnes physiques, leurs nom, prénoms, domicile et numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription ;
b) S'il s'agit de personnes morales, leur dénomination ou leur raison sociale et leur siège social, leur numéro de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription, leur capital social, l'adresse de leur siège social ;
c) Le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction au sens de l'article 93-2 de la loi n° 82-652 du 29 juillet 1982 précitée ;
d) Le nom, la dénomination ou la raison sociale et l'adresse et le numéro de téléphone du prestataire mentionné au 2 du I.
2. Les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné au 2 du I, sous réserve de lui avoir communiqué les éléments d'identification personnelle prévus au 1.
Les personnes mentionnées au 2 du I sont assujetties au secret professionnel dans les conditions prévues aux articles 226-13 et 226-14 du code pénal, pour tout ce qui concerne la divulgation de ces éléments d'identification personnelle ou de toute information permettant d'identifier la personne concernée. Ce secret professionnel n'est pas opposable à l'autorité judiciaire. »

[45] Dans une affaire récente, après notification par lettre recommandée à Facebook afin d'obtenir le retrait intégral de la page incriminée et face à l'inaction de la plate-forme, le tribunal saisi a indiqué dans sa décision que Facebook *« n'est pas l'éditeur des contenus publiés sur son site mais un prestataire technique dont l'activité*

sécurité, l'importance juridique des diverses méthodes d'authentification et de signatures électroniques.

3. Identité sous forme numérique

L'explosion rapide des espaces de communication et d'expression sur l'Internet pose avec acuité la question de l'identité sous forme numérique, notion encore complexe que les travaux les plus récents en sciences humaines et sociales tentent de circonscrire. D'après le Rapport Truche[46], « *Le concept même d'identité numérique n'est pas, et pas plus que l'identité « traditionnelle » univoque et uniforme : l'identité numérique se compose d'un ensemble d'identifiants partiels, finalisés, et des relations qu'entretiennent ces identifiants. L'essor de l'administration électronique, et plus largement de la société de l'information, multiplie et complexifie ces identités partielles et ces relations, sans pour autant conduire à les fusionner : cela pose la question de l'interopérabilité des identités numériques.* ».

En effet, les procédés d'identité sous forme numérique ne doivent nullement être considérés comme la transposition de règles de fonctionnement du monde physique mais comme des dispositifs qui, grâce aux technologies mises en œuvre, permettent d'anticiper des gains de productivité importants et favorisent l'apparition de nouveaux métiers d'intermédiation. Cependant, il n'en demeure pas moins que l'identité doit apporter sa pierre à l'édification de la sécurité des usages numériques.

L'usage courant du pseudonyme (qui est un moyen d'identification d'un individu sous couvert d'anonymat[47]) constitue un obstacle à la recherche de certitude d'une véritable

---

est d'offrir des services de communication au public en ligne ». Après avoir retenu, sur le fondement de la LCEN, la qualification d'hébergeur, le juge des référés a ordonné sous astreinte, à Facebook le retrait des contenus litigieux ainsi que **la communication des éléments permettant l'identification de leurs auteurs**. TGI Paris, ord. réf. du 13 avril 2010, H. Giraud c/ Facebook France, RG : n° 10/53340 ; V. égal. : Cass. civ. 1ère, 14 janvier 2010, Tiscali Média / Dargaud Lombard, Lucky Comics, RG n° 06/18855, v. Jérôme Huet, *Tiscali n'est pas un hébergeur*, Legipresse n° 270, 1 mars 2010, p.39-42 ; Lionel de Souza, *Statut de l'hébergeur : la Cour de cassation adopte une analyse stricte*, Expertises des systemes d'information n°345, 1 mars 2010, p. 100-101 ; Philippe Stoffel-Munck, *Avis de tempête sur le Web 2.0 : la Cour de cassation juge que Tiscali n'est pas un hébergeur*, Comm. Com. Electr. n°3, 1 mars 2010, comm. 25 ; Frederic Pollaud-Dulian, *Note sous Cour de cassation, première Chambre civile, 14 janvier 2010, Société Telecom Italia (anciennement Tiscali media) contre Société Dargaud Lombard, pourvoi numéro 06-18.855*, RTD com n°2, 1 avril 2010, p. 307-310.

[46] Rapport Truche, *Administration électronique et protection des données personnelles*. Synthèse, Paris 2002, disponible sur http://www.foruminternet.org/telechargement/documents/rapp-truche-20020226.pdf.

[47] L'usage du pseudonyme est prévu dans la directive n° 1999/93/CE du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques (JOCE n° L 013 du 19 janvier 2000 p. 0012 à 0020) *:* considérant 25 : *(…)* ***les dispositions relatives à l'utilisation de pseudonymes dans des certificats n'empêchent pas les États membres de réclamer l'identification des personnes conformément au droit communautaire ou national*** *;* Article 8.3 : *Sans préjudice des effets juridiques donnés aux pseudonymes par la législation nationale, les États membres ne peuvent empêcher le prestataire de service de certification d'indiquer dans le certificat un pseudonyme au lieu du nom du signataire ;* Annexe I c) : *Tout certificat qualifié doit comporter (…)* ***le nom du signataire ou un pseudonyme qui est identifié comme tel*** *;* Annexe IV f) : *Durant le processus de vérification de la signature, il convient de veiller, avec une marge de sécurité suffisante, à ce que (…)* ***l'utilisation d'un pseudonyme soit clairement indiquée*** *(…) ;* et en France, dans le 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 (JO n° 77 du 31 mars 2001 p. 05070) : Article 5 f) : *Un dispositif de vérification de signature électronique peut faire, après évaluation, l'objet d'une certification, selon les procédures définies par le décret mentionné à l'article 4, s'il répond aux exigences suivantes :* ***Lorsqu'il est fait usage d'un pseudonyme****, son utilisation doit être clairement portée à la*

identification numérique. Ainsi, l'identité sous forme numérique échappe pour l'heure à toute attribution par une autorité publique ; en ce sens, on peut estimer que les éléments qui la composent ne relèvent pas de l'identité juridique de la personne. Pourtant, dans la mesure où elle se trouve au cœur d'une réflexion nationale voire européenne dans le cadre du renforcement de la confiance numérique, touchant des problèmes tels que l'e-reputation, la protection des données personnelles ou encore le respect de la vie privée sur l'Internet, différents textes législatifs et réglementaires s'y réfèrent.

Actuellement, parmi les textes français qui peuvent s'appliquer à la protection de l'identité et du nom d'une personne (donc dans des cas très spécifiques), on trouve notamment :

- L'article 433-19 du code pénal qui concerne l'utilisation d'une fausse identité (au sens de l'Etat civil) ;
- L'article 434-23 du code pénal qui concerne la prise du nom d'un tiers dans des circonstances qui pourraient engendrer à son encontre des poursuites pénales ;
- L'article 781 du code procédure pénale qui incrimine la prise d'un faux nom ou d'une fausse qualité ;
- Enfin, l'article 441-6 du code pénal, incriminant le fait de se faire indûment délivrer par administration un document destiné à constater un droit, une identité.

Cependant, il convient de noter qu'ici, ce n'est pas l'usurpation de l'un ou plusieurs des identifiants numériques de la personne (ex : adresse de messagerie, nom de domaine, pseudonyme virtuel etc.), qui est réprimée, mais seulement l'usage des données d'identification figurant à l'Etat civil dont le nom de famille, prénoms, domicile, ce qui ne permet pas d'appréhender des comportements liés à la cybercriminalité, tels que le « phishing » ou le « spoofing ».

Par conséquent, l'idée d'insérer un nouvel article dans le code pénal qui introduirait une pénalisation de l'usurpation d'identité numérique a fait l'objet de plusieurs initiatives législatives, notamment le projet de la Loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI), en deuxième lecture devant l'Assemblée nationale, ou encore le projet déposé le 27 juillet 2010 devant le Sénat visant à moderniser la carte nationale d'identité, en l'équipant de puce électronique sécurisée contenant des données biométriques ainsi que, facultativement, d'un système d'authentification à distance de la signature électronique. Il faut cependant noter que là aussi, ce n'est pas l'usurpation de l'identité-même qui se voit sanctionnée, mais plutôt un accès frauduleux dans une base, l'entrave ou l'altération du fonctionnement de la base ou l'introduction, la modification ou la suppression frauduleuse de données.

Désormais, le nouvel article 226-4-1 du Code pénal introduit par la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure[48] dispose « *Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.*

---

connaissance du vérificateur ; Article 6-I. c) : *Un certificat électronique qualifié doit comporter (…)* ***le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel****.* »

[48] J.O du 15 mars 2011 p. 4582.

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. ».

Aucun domaine de la société (organismes publics, entreprises, associations et individus) n'étant à l'abri des atteintes apportées à l'identité sous forme numérique notamment en matière d'accès à des informations sensibles (médicales, sociales, bancaires, etc.), de recrutement et d'image véhiculée, les premiers problèmes d'ordre juridique viennent souligner le caractère fondamental de ces questions et mettent en évidence leur complexité[49].

Le programme d'identité électronique français ambitionne la mise en service d'une carte nationale d'identité (électronique) spécifique, avec un objectif « *d'identification générale et non des usages spécifiques, comme le permis de conduire ou le passeport* »[50]. Comme le rappelait le Rapport Truche, les mécanismes inhérents aux certificats électroniques constituent une véritable mine de renseignements si, à l'avenir, les fichiers devaient être croisés par les détenteurs des traces[51]. Les certificats de cette Carte Nationale d'Identité Electronique pourraient alors servir dans le cadre des formalités administratives (signature de mandataires sociaux, réponses aux appels d'offres ou TéléTVA, etc.)[52]. Parallèlement, ils pourraient être utilisés par les grandes entreprises dans le cadre de délégations de pouvoirs, entre autres, grâce à des outils de workflow ou de paraphe électronique.

4. Sceaux électroniques

[49] A titre d'exemple, on peut citer le projet de loi allemande du 25 août 2010 concernant la protection des données à caractère personnel des salariés et qui vise, notamment, à interdire aux employeurs de consulter le profil Facebook et les messages publiés par les candidats à l'embauche. En France, même si l'obligation de s'informer s'impose à celui qui recrute (Cour d'Appel de Nancy 27 mars 2002 SARL Comabois c./Dacquembronne, n°00/01923 ; Cour d'Appel de Montpellier 5 février 2002), il est important de veiller au respect de l'article L. 1132-1 du code de travail). Ordonnance de référé du 24 novembre 2010 du TGI de Paris, 17e ch., Omar S. / Alexandre, P., Agathe Lepage, *Faux profil sur Facebook,* Comm. Com. Electr. n°3, mars 2011, comm. 28.

[50] La carte d'identité se distingue des autres pièces d'identité par la réunion de trois conditions :
– elle est délivrée par l'État ;
– elle vise des fins d'identification générale et non des usages spécifiques (comme le permis de conduire ou le passeport) ;
– elle contient des renseignements qui en font, en comparaison des autres pièces d'identité, un document privilégié pour identifier les personnes. Rapport Truche, *Administration électronique et protection des données personnelles*, Paris, 2002. Sur le passeport, v. Règlement (CE) n°2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres, JOUE du 20 décembre 2004, L. 385/1.

[51] « *Les risques et les perceptions en matière de vie privée se sont déplacés de la constitution de «grands fichiers » vers la problématique de la gestion des « traces » que l'on laisse dans les systèmes que l'on utilise ; Les risques et les perceptions en matière de vie privée se sont déplacés des fichiers publics, principaux créateurs et gestionnaires de fichiers, vers les opérateurs privés, spécialistes de marketing et de gestion « optimisée » (du point de vue de l'entreprise) de la relation client* ». Rapport Truche, *Administration électronique et protection des données personnelles*, Synthèse, Paris, 2002.

[52] V. le rapport du Forum des Droits sur Internet "*Projet de carte nationale d'identite numerique*", publie le 16 juin 2005 http://www.foruminternet.org/telechargement/documents/rapp-cnie-20050616.pdf ; Thierry Piette-Coudol, *L'identité des personnes, les certificats et la signature électronique*, Comm. Com. Electr. n° 1, 1 janvier 2005, p. 19-24.

Les télé-procédures au service des usagers - entreprises, professionnels ou particuliers - se sont développées tout au long de la dernière décennie (on pense ici aux déclarations de la TVA[53] ou à l'Impôt sur le revenu). Les procédures s'effectuent également dans les relations entre l'Etat et les collectivités locales, notamment dans le cadre du « *contrôle de légalité par voie électronique* »[54].

Les procédés de scellement électroniques ont pour objet de garantir l'intégrité des données auxquelles ils sont appliqués. Leurs manifestations s'opèrent par le biais des signatures dites techniques (certificat de serveur) et de l'horodatage.

C'est en France qu'est apparue la première loi permettant la dématérialisation des factures. En effet, la facture électronique par Echanges de Données Informatisés (EDI) existe en France depuis la loi de finances rectificative pour 1990[55]. En revanche, s'agissant de la facture électronique signée, elle a été introduite par l'article 17 de la loi de finances rectificative pour 2002[56], qui transpose la directive n°2001/115 du 20 décembre 2001 modifiant la directive n°77/388/CEE en vue de simplifier, moderniser et harmoniser les conditions imposées à la facturation en matière de taxe sur la valeur ajoutée et pose, à côté des factures EDI, le régime des factures électroniques, ayant recours aux dispositifs de signature électronique. Les modalités d'application de la facturation électronique ont été précisées dans l'instruction du 7 août 2003[57]. Il s'agit ici d'une signature électronique utilisant un certificat de serveur (certificat de personne morale) et non d'une signature électronique (certificat de personne physique) au sens juridique de « *signer un acte* ». Il est à noter en cet endroit que la facturation électronique se développe en Europe, notamment en raison de la croissance de l'économie numérique. Or, la diversité des règles en vigueur au sein des Etats membres de l'Union européenne relative à la facturation électronique, issue des diverses transpositions de la directive dans les droits des Etats membres, est considérée comme un frein à l'expansion de ce type de facturation. De nombreux Etats ont introduit des règles spécifiques qui interdisent aux entreprises européennes d'utiliser le même service dans tous les Etats. Le droit est harmonisé, il n'est pas unifié, d'où les difficultés. Un Règlement européen eut été plus adapté à la situation.

---

[53] Loi n°2002-1576 du 30 décembre 2002, J.O. n° 304 du 31 décembre 2002, p. 22070.

[54] V. pour une analyse de la problématique, Anne Cantéro, *Des actes unilatéraux des communes dans le contexte électronique, Vers la dématérialisation des actes administratifs ?*, PUAM, Coll. Collectivités locales, 2002. Nicolas Fouilleul, *Le contrat administratif électronique*, (2 tomes), préface de Florian Linditch, Avant-propos Yves-René Guillou, P.U.A.M., 2007. V. également pour les textes adoptés : la loi n°2004-809 du 13 août 2004 relative aux libertés et aux responsabilités locales, J.O. du 17 août 2004, p. 14545 et s. ; le décret n° 2005-324 du 7 avril 2005 relatif à la transmission par voie électronique des actes des collectivités territoriales soumis au contrôle de légalité et modifiant la partie réglementaire du code général des collectivités territoriales, J.O. du 8 avril 2005, p. 6340 et s. ; l'arrêté du 26 octobre 2005 portant approbation d'un cahier des charges des dispositifs de télétransmission des actes soumis au contrôle de légalité et fixant une procédure d'homologation de ces dispositifs, J.O. du 3 novembre 2005, p. 17289 et s. ; Eric Caprioli et Anne Cantéro, *L'entreprise face à la dématérialisation des marchés publics*, JCP, éd. E, 3 novembre 2005, pp.1887-1891 ; Hervé de Gaudemar, *La preuve devant le juge administratif*, Droit Administratif n° 6, Juin 2009, étude 12.

[55] Eric A. Caprioli, *La dématérialisation de la facture commerciale au regard de sa polyvalence juridique*, JCP, éd. E, Cah. dr. entrep., 1993/1, p. 34 et s.

[56] Loi n°2002-1576 du 30 décembre 2002, JO du 31 décembre 2002.

[57] Instruction de la Direction générale des impôts n° 136 du 7 août 2003, 3CA. V. égal. *Dématérialisation et archivage électronique*, Eric A. Caprioli, Marie-Anne Chabin, Jean-Marc Rietsch, éd. Dunod, 2006, p.58 à 68.

Ceci explique pourquoi une nouvelle directive a été adoptée le 13 juillet 2010[58]. Elle a pour but d'accroître l'utilisation de la facturation électronique, de réduire les charges pour les entreprises, de soutenir les petites et moyennes entreprises (PME) et d'aider les États membres à lutter contre la fraude Pour atteindre ces objectifs, les autorités fiscales doivent accepter les factures électroniques dans les mêmes conditions que les factures sur support papier en vertu de l'application du principe de non-discrimination de l'écrit électronique. Elle vise également à supprimer de la Directive 2006/112/CE[59] les obstacles entravant le recours à la facturation électronique. En effet, il est nécessaire d'accroître le recours à la facturation électronique, en cessant de faire des signatures électroniques avancées ou de l'échange des données informatisées des conditions indispensables à l'établissement des factures électroniques ; sur le plan fiscal, l'authenticité de l'origine, l'intégrité du contenu et la lisibilité de la facture restent les conditions nécessaires à l'établissement et à la conservation des factures électroniques.

En outre, la loi dite de simplification et de clarification du droit et d'allègement des procédures[60] a autorisé les employeurs à dématérialiser la procédure de remise de bulletins de salaire à leurs salariés. Les modalités techniques de la loi permettant de garantir l'intégrité des données ne sont toutefois pas encore arrêtées, même si les solutions de dématérialisation des bulletins de salaire ne devraient guère différer de celles déjà disponibles pour les factures électroniques.

Sous l'angle juridique, l'article L. 3243-2 du Code du travail dispose que « *lors du paiement du salaire, l'employeur remet* […] *une pièce justificative dite bulletin de paie* ». Il précise qu' « *avec l'accord du salarié concerné, cette remise peut ętre effectuée sous forme électronique, dans des conditions de nature à garantir l'intégrité des données* ». Deux conditions distinctes ressortent ainsi de la remise du bulletin de salaire : l'accord du salarié et la garantie de l'intégrité des données. Nul besoin de signer les bulletins de salaire au sens juridique, car, de jurisprudence constante, ce sont des pièces justificatives et non des actes juridiques.

Par ailleurs, les articles L. 3243-4 et L. 3243-5 du Code du travail posent les obligations de conservation par l'employeur du bulletin de salaire par voie électronique.

La loi ne précise pas les moyens de garantir l'intégrité de ces données, conformément au principe de neutralité technologique. Les objectifs à atteindre sont exposés mais sans imposer une solution spécifique[61]. En pratique, il apparaît que le recours à une signature électronique « technique » (scellement) du document telle qu'elle est employée pour la facture électronique devrait être considéré comme une garantie suffisante. Des mécanismes

[58] Directive 2010/45/UE du Conseil du 13 juillet 2010 modifiant la directive 2006/112/CE relative au système commun de taxe sur la valeur ajoutée en ce qui concerne les règles de facturation, J.O.U.E L. 189 du 22 juillet 2010, p. 1 et s.

[59] Directive 2006/112/CE du 28 novembre 2006 relative au système commun de taxe sur la valeur ajoute, JOUE n° L 347 du 11/12/2006, p. 0001-0118.

[60] Loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures publiée au J.O. du 13 mai 2009.

[61] Eric A. Caprioli *Bulletins de paie dématérialisés,* Comm. Com. Electr. Juillet 2009, n°71 ; Eric A. Caprioli, *La dématérialisation des bulletins de paie,* Cahiers de droit de l'entreprise, Fiche pratique Juillet 2009, n°20 ; Thierry Piette-Coudol, *La remise électronique de bulletin de paie,* JCP éd. Sociale n°43, 26 Octobre 2010, n°1440.

de coffre-fort électronique permettant au salarié de conserver et de disposer de ses bulletins de paie peuvent également être mis en place.

5. Signature électronique

La signature électronique fait l'objet d'une réglementation précise et détaillée sur le territoire français. Transposant la directive 1999/93/CE du 13 décembre 1999 pour un cadre commun sur les signatures électroniques du Parlement et du Conseil européens, la loi française du 13 mars 2000[62] a posé le cadre juridique de la preuve et de la signature électroniques.

Elle a été complétée par les décrets n° 2001-272 du 30 mars 2001[63] et n° 2002-535 du 18 avril 2002[64] ainsi que l'arrêté du 31 mai 2002[65]. Ce dernier arrêté a d'ailleurs été abrogé par un arrêté du 26 juillet 2004[66]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. Enfin, la loi n°2004-575 pour la confiance dans l'économie numérique du 21 juin 2004 a consacré la validité juridique des écrits sous forme électronique (articles 1108-1 et 1108-2 du code civil)[67].

La première définition légale de la signature électronique, fondée sur une approche fonctionnelle du dispositif, a été donnée à l'article 1316-4, al. 2 du code civil : « *Lorsqu'elle est électronique, elle (la signature) consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d 'Etat.* ».

---

[62] V. Eric A. Caprioli, *La loi française sur la preuve et la signature électroniques dans la perspective européenne*, J.C.P. éd. G, 2000, I, 224 et *Ecrit et preuve électroniques dans la loi n°2000-230 du 13 mars 2000*, J.C.P. 2000, éd. E, cah. dr. entr. n°2, Suppl. au n°30, p.1- 11 ; Pierre Catala, *Le formalisme et les nouvelles technologies*, Rép. Defrénois, Art. 37210, 2000 ; P. Y. Gautier et X. Linant de Bellefonds, préc. ; Jérôme Huet, *Vers une consécration de la preuve et de la signature électroniques*, D. 2000, n°6, Chr., p. 95 et s. ; Pierre Leclercq, préc., Arnaud Raynouard, *Adaptation du droit de la preuve aux nouvelles technologies de l'information et à la signature électronique*, Rép. Defrénois n°10, 2000, Doct., p. 593 et s.

[63] Décret pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique, J.O. du 31 mars 2001, p. 5070. V. Eric A. Caprioli, *Commentaire du décret n°2001-272 du 30 mars 2001 relatif à la signature électronique*, Revue de Droit Bancaire et financier, Mai/juin 2001, p. 155 s., v. égal. Laurent Jacques, *Le décret n°2001-272 du 30 mars 2001 relatif à la signature électronique,* J.C.P. éd. E 2001, Aperçu rapide, p. 1601 ; François Coupez, C. Gailliègue, *Vers une signature électronique juridiquement maîtrisée. A propos de l'arrêté du 31 mai 2002*, C.C.E., novembre 2002, p. 8 et s ; Anne Penneau, *La certification des produits et systèmes permettant la réalisation des actes et signatures électroniques (à propos du décret 2002-535 du 18 avril 2002)*, D. 2002, n° 26, p. 2065.

[64] J.O. du 19 avril 2002, p. 6944. v. à cet égard, Droit & Patrimoine, février 2003, p. 116, obs. Eric A. Caprioli.

[65] J.O. du 8 juin 2002, p. 10223.

[66] J.O. du 7 août 2004, p. 14104.

[67] J.O. n° 143 du 22 juin 2004, p. 11182. V. à ce titre, Eric A. Caprioli et Pascal Agosti, *La confiance dans l'économie numérique*, Les Petites Affiches, 3 juin 2005 p 4 s. ; Numéro spécial consacré à la loi pour la confiance dans l'économie numérique, Comm. Com. Electr. n° 9, Septembre 2004, Repère 9 ; Numéro spécial Cahier Lamy droit de l'informatique et des réseaux n°171, juillet 2004 ; Le dossier « contrat électronique » Revue des contrats, 1 avril 2005 n°2 .Mustapha Mekki, *Le formalisme électronique : la « neutralité technique » n'emporte pas « neutralité auxiologique »,* Revue des contrats, 1 juillet 2007, n°3, p. 681 ; Arnaud Van Eeckhout, *La sécurité juridique dans le secteur des communications électroniques : un principe malmené ?,* Revue des contrats, 1 juillet 2007, n°3, p. 933.

La signature électronique peut donc être considérée comme un ***moyen d'authentification***, en ce sens qu'elle permet de vérifier l'identité du signataire et l'intégrité du document, mais sans toutefois se limiter à ce seul aspect dans la mesure où la signature permet également de manifester la volonté du signataire de consentir à un acte (l'aliéna 1er de l'article 1316-4 : « *Elle manifeste le consentement des parties aux obligations qui découlent de cet acte.* »)[68].

La définition établie par la loi type de la C.N.U.D.C.I. sur les signatures électroniques va dans le même sens puisqu'elle l'interprète comme des données sous forme électronique contenues dans un message de données ou logiquement associées audit message, pouvant être utilisées pour « *identifier le signataire* » dans le cadre du message de données et « *indiquer qu'il approuve l'information qui y est contenue* »[69].

Différentes méthodes d'authentification pour les signatures électroniques ont été mises au point au fil des années visant à satisfaire des besoins spécifiques, à conférer des niveaux de sécurité différents correspondant à des exigences techniques distinctes. Ces méthodes peuvent être classées en trois catégories : celles qui sont fondées sur la **connaissance de l'utilisateur** (mot de passe, numéro d'identification personnel etc.), **celles qui sont fondées sur les caractéristiques physiques de l'utilisateur** (comme la reconnaissance biométrique) et celles enfin qui sont fondées **sur la possession d'un objet par l'utilisateur** (carte, clé USB, token, etc.)[70]. Ces catégories qui peuvent se cumuler, reposent sur le triptyque classique de la sécurité : ce que je connais, ce que je suis et ce que je possède[71].

Il convient d'ajouter que les niveaux de sécurité des certificats électroniques permettant de vérifier signature sont également liés à leurs modalités de délivrance par un tiers de confiance (appelé Prestataire de services de certification électronique/P.S.C.E.), trois niveaux du plus fort au plus faible : enregistrement en face à face, enregistrement sur la base de documents justificatifs envoyés par La Poste ou par électronique et avec une simple adresse électronique.

Le procédé d'identification de la signature électronique doit être fiable, comme le rappelle la jurisprudence[72].

Reprenant la Directive européenne de 1999, le décret du 30 mars 2001 a trait à la signature électronique sécurisée présumée fiable, une catégorie particulière de signature électronique.

---

[68] Christiane Féral-Schul, *Cyberdroit, le droit à l'épreuve de l'internet*, Paris, Dalloz, 6ème éd., 2010, v. n°92.11.

[69] Article 2-a) de la Loi type de la CNUDCI sur les signatures électroniques.

[70] V. le rapport du Groupe de travail sur le commerce électronique sur les travaux de sa trente-deuxième session, tenue à Vienne du 19 au 30 janvier 1998 (A/CN.9/446, paragraphes 91 sq.).

[71] Seul un procédé biométrique permet d'être vraiment certain que c'est la personne qui signe électroniquement qui est derrière son écran d'ordinateur. Mais aucun moyen technique ne permettra d'établir qu'au moment de la signature, le contrat n'a pas été vicié : par exemple par la violence (contrainte physique ou morale).

[72] En ce sens, à propos d'une signature scannée (non admise) dans le cadre d'une procédure d'appel : CA Besançon, 20 octobre 2000, JCP éd. G. 2001, II, 10606, p. 1890 et s. note Eric A. Caprioli et Pascal Agosti ; confirmé par la Cour de cassation le 30 avril 2003, Bull. civ. 2003, n°118, p. 101 et s. (disponible sur le site www.legifrance.gouv.fr).

La signature électronique sécurisée (Signature électronique avancée dans la directive européenne de 1999) est définie à l'article 1.2 comme : «*une signature électronique qui satisfait, en outre, aux exigences suivantes :*
- être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable».

En outre, doivent être pris en compte le dispositif sécurisé de création de signature électronique et le certificat électronique qualifié[73] pour caractériser une signature électronique sécurisée disposant d'une présomption de fiabilité (si elle est «*établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié* »[74]). Cette dernière sera présumée fiable, contrairement aux autres formes de signature dont la fiabilité devra être démontrée par l'utilisateur.

Bien qu'il existe une distinction entre les signatures électroniques dites « simples », à savoir toutes celles qui ne bénéficient pas de la présomption de fiabilité, et la signature électronique sécurisée présumée fiable, les deux types de signature électronique ont la même valeur juridique dès lors qu'elles reposent sur l'utilisation d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elles s'attachent[75]. Il incombe donc au juge de décider si la signature et l'écrit sous forme électronique sont admissibles ou non, aussi bien pour la valeur probante que pour la validité de l'écrit qui lui est présenté dans le cadre d'un litige et seule la charge de la preuve sera renversée en fonction du bénéfice ou non de la présomption de fiabilité[76].

6. Procédés biométriques

Les applications biométriques ont tendance à se multiplier et à se banaliser dans de nombreuses applications, ce qui ne va pas sans poser de sérieux problèmes juridiques[77]. La

---

[73] Ce certificat d'identification délivrée par le P.S.C.E. devra préciser, pour être considéré comme qualifié : «*a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;*
b) L'identité du prestataire de services de certification électronique ainsi que l'Etat dans lequel il est établi ;
c) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;
d) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;
e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;
f) L'indication du début et de la fin de la période de validité du certificat électronique ;
g) Le code d'identité du certificat électronique ;
h) La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;
i) Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.».
[74] Art. 2 du décret du 30 mars 2001.
[75] V. art. 1316-4, al. 2 du code civil.
[76] Dans un cas, il appartient à l'utilisateur du procédé de signature de prouver cette fiabilité (signature électronique « simple »), dans l'autre, c'est celui qui la conteste qui devra prouver son absence de respect des exigences (signature électronique sécurisée).
[77] V. sur le sujet, le remarquable article de Pierre Leclercq, *A propos de la biométrie*, Comm. Com. Electr. Mars 2006, p.14-18.

biométrie se définit comme l'étude de caractéristiques physiques, uniques des personnes, susceptibles de les identifier dans leur individualité[78]. Désormais, avec des procédés biométriques la vérification d'identité se fait quasi-instantanément, notamment pour contrôler l'accès à certains locaux sécurisés, aux salles informatiques, pour gérer les entrées et sorties des salariés dans les entreprises ou pour protéger les accès à des ordinateurs et leurs données. Il s'agit d'un moyen d'identification ou d'authentification des plus sûrs qui permet de s'assurer que la personne qui est derrière le dispositif connecté est bien celle qu'elle prétend être. En revanche, un procédé biométrique ne permet pas de manifester la volonté nécessaire à la signature. Certains auteurs estiment qu'une signature utilisant ce type de reconnaissance biométrique est infalsifiable[79], mais ils omettent l'importance de la manifestation de consentement comme fonctionnalité juridique essentielle de la signature dans certains systèmes juridiques ou encore à l'article 7 de la loi-type de la CNUDCI sur le commerce électronique et à l'article 9-3-a) de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux. Ces méthodes[80] pourraient venir en complément de ce que la personne possède (la carte, la clé, le token) et de ce qu'elle connait (les données d'activation de la clé privée)[81] dans le cadre d'une identification renforcée à partir du moment où la particularité biométrique est liée à un individu et que le lien établi est sécurisé. Il existe une limite quant à la fiabilité de ces empreintes : certaines caractéristiques physiques peuvent être sujettes à des variations dues au stress comme la voix et empêchent une identification certaine. Le public est réticent concernant l'usage de certains procédés d'identification biométriques. De plus, ils sont encore relativement lourds et coûteux à mettre en œuvre. En outre, l'utilisation de ces procédés est strictement encadrée par les lois relatives à la protection des données à caractère personnel afin d'éviter tout débordement sécuritaire (bases centralisées et croisement de données : « *Big brother* »). Les données biométriques doivent faire l'objet d'une demande d'autorisation dans de nombreuses législations transposant la directive

[78] On peut citer, par exemple, l'examen des empreintes digitales (dactyloscopie) ou des vaisseaux sanguins de la rétine de l'œil (rétinoscopie), la reconnaissance vocale ou encore la reconnaissance dynamique de la signature (analyse de la manière dont elle est tracée : vitesse, mouvements, pression, …).

[79] «*Chimie, génétique et biologie offrent aujourd'hui à toute main d'écrire une signature inviolable, unique et inimitable*.» : Expression de J. Srazzula, citée par Ch. Gavalda sous Cass. civ. 8 novembre 1989, D.1990, Jp. p. 370.

[80] Pour l'empreinte digitale, utilisée comme moyen d'identification électronique, la procédure technique est la suivante. Dans un premier temps, un capteur va prendre une image de l'empreinte. Cette image sera analysée par un logiciel de traitement d'image, afin de repérer les sillons et crêtes de l'empreinte, puis elle sera transformée en code. Ces points caractéristiques de l'empreinte – appelés minuties – permettent d'obtenir une empreinte digitale réduite ; elle est stockée dans une base de données (ou sur le matériel du titulaire). Par la suite, l'empreinte présentée est comparée avec l'empreinte digitale réduite, en mesurant la proximité de deux nuages de minuties. Le résultat de cette comparaison confirmera l'appartenance ou non des empreintes digitales réduites à une même personne. Ensuite, lorsqu'une personne se présente à un contrôle d'identité, elle indique alors la référence de son empreinte digitale réduite en présentant le doigt approprié au lecteur d'empreinte. Si la personne est reconnue, elle accède aux droits qui lui sont reconnus et dans l'hypothèse inverse, le système la rejettera.

[81] Certaines techniques pourraient cumuler plusieurs types de signatures. Par exemple, un dispositif biométrique pourrait s'appuyer sur des signatures dynamiques. Avec un tel dispositif, le signataire apposerait sa signature manuscrite à l'aide d'un stylo spécial ou d'un stylet, soit sur l'écran d'un ordinateur, soit sur une tablette numérique. La signature manuscrite serait alors analysée par l'ordinateur et mise en mémoire comme une série de valeurs numériques qui pourrait être ajoutée à un message de données affiché par le destinataire aux fins d'authentification. Ce dispositif remplacerait le code personnel du signataire à quatre chiffres. V. en ce sens, Jean-François Blanchette, *Les technologies de l'écrit électronique : synthèse et évaluation critique,* in Mission de recherche «Droit et justice» sous la direction de Isabelle de Lamberterie, *Les actes authentiques électroniques*, La documentation française, 2002, p. 139 et s.

européenne 95/46 du 24 octobre 1995 (en cours de révision), par exemple en France, conformément aux articles 25-I-8° et 27-I-2° de la loi du 76 janvier 1978 modifiée[82].

Une délibération de la Commission Nationale Informatique et Liberté (CNIL) n°2011-074 a été adoptée le 10 mars 2011. Elle porte autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale et elle a pour finalité le contrôle de l'accès aux postes informatiques portables professionnels[83]. Les responsables de ces traitements devront adresser à la CNIL un engagement de conformité aux conditions fixées par l'autorisation unique n°AU-027. Cette délibération était très attendue des professionnels concernés.

Dans certains cas, l'application de la loi « Informatique et libertés » intervient de manière connexe. A titre d'illustration, une décision de la Cour d'appel de Paris en date du 23 février 2011 vient rappeler l'importance des formalités préalables (en l'état une demande autorisation) pour la mise en œuvre de dispositif biométrique. En l'état, la S.A. d'économie mixte pour la construction et l'exploitation du marché d'intérêt national d'Avignon-SMINA a conclu le 23 décembre 2004, trois contrats « de maintenance avec option de location de matériel », avec la société SafeTIC. Le 12 janvier 2005, la société SafeTIC SA a livré la solution de contrôle d'accès aux locaux de SMINA. Cependant, le procès-verbal de livraison indique que l'utilisation de ce matériel biométrique est soumise à l'autorisation de la Commission nationale de l'informatique et des libertés (CNIL). Or, le 19 juin 2005, la CNIL avait jugé l'utilisation de ce matériel non conforme à la réglementation applicable en matière de protection des données à caractère personnel et avait donc refusé l'autorisation demandée. Par un jugement en date du 30 novembre 2007, le Tribunal de commerce de Paris a prononcé la résiliation des contrats signés aux torts de SMINA et a donné acte à Easydentic (qui est devenue la société SafeTIC) de ce qu'elle était en mesure de fournir à SMINA un nouveau système de contrôle en totale conformité avec les nouvelles exigences de la CNIL.

Ce jugement a été infirmé par un arrêt en date du 23 février 2011 de la Cour d'appel de Paris. Cette dernière a condamné Easydentic en prononçant la résolution des trois contrats conclus aux motifs qu' « *il incombait à Easydentic, professionnelle en matériels de biométrie, de* […] *fournir des matériels conformes à la réglementation en vigueur* ».
Cette décision reconnaît donc la responsabilité contractuelle de SafeTIC SA pour manquement à son obligation d'information. Même s'il appartenait à SMINA (la société utilisatrice) de soumettre une demande d'autorisation préalable de l'utilisation du matériel biométrique à la CNIL, il semblerait que SafeTIC SA ait sciemment omis cette information lors de la conclusion des contrats.

[82] Article 25-I « *Sont mis en œuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27* » : *(…) 8°* : *« Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes* » et article 27-I : « *Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés : (…) 2° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.* »
[83] V. le site : www.cnil.fr.

B. Exigences liées à l'identité numérique

Si ces exigences sont de deux ordres, technique et juridique, leurs objectifs convergent vers la sécurité entendue au sens large, des biens et des personnes, mais aussi des intérêts de l'Etat et de la Société. L'importance des usages de l'identité dans le monde numérique justifie des mesures particulières en termes de fiabilité des procédés utilisés (1), et de règles juridiques à respecter dans certaines hypothèses de conformité, comme par exemple dans l'organisation des jeux en ligne ou de la lutte anti-blanchiment d'argent (2). Outre les aspects technico-juridiques et commerciaux, l'incidence des exigences juridiques attenantes aux aspects de protection de la vie privée, là encore, doit être soulignée, en ce y compris la dimension des flux transfrontières de données à caractère personnel en dehors de l'Union européenne. L'hypothèse peut exister dans le cadre d'une fédération d'identité regroupant des entités pluri-localisées et des personnes sur plusieurs continents ou de l'application d'une politique d'Identity and Access Management au sein d'un groupe international.

1. L'incontournable sécurité technique

En France, le basculement dans l'ère numérique a été consacré par plusieurs lois[84] et de nombreux textes règlementaires ; il s'appuie, en outre, sur des normes techniques permettant d'identifier avec un degré de confiance suffisant les personnes utilisant des systèmes d'information[85]. Les différentes formes de « signature numérique », les méthodes d'authentification et les protocoles de chiffrement des flux de données constituent autant de garanties techniques sur lesquelles reposent la régularité et la sécurité des transactions et partant leur valeur juridique.

En vertu de la jurisprudence de la Cour de cassation, une norme consiste en «*une codification écrite des règles de l'art*»[86]. Elle détermine et décrit un socle de règles techniques, voire organisationnelles, sur lequel les acteurs économiques peuvent s'appuyer. Une norme n'a donc pas **de pouvoirs directement contraignants**. En France, les normes sont obligatoires lorsqu'elles sont prévues dans un arrêté, par contrat ou qu'elles résultent d'un usage dans un secteur d'activité. En revanche, la norme offre un certain nombre de repères (modalités, conditions, moyens) pour arriver à la finalité qu'elle s'est fixée. On utilise

[84] Notamment : Loi n°2002-1094 du 29 août 2002 d'orientation et de programmation pour la performance de la sécurité intérieure dite LOPPSI, J.O. n°202 du 30 août 2002 ; Loi n°2004-575 sur la confiance en l'économie numérique du 21 juin 2004, J.O. n°143 du 22 juin 2004, p. 11168 et s ; Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle, J.O. n°159 du 10 juillet 2004 ; Loi n° 2008-776 du 4 août 2008 de modernisation de l'économie, J.O. n°181 du 5 août 2008 ; Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la Loi 2004-801 du 6 août 2004 (J.O. du 7 août 2004) ; Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, J.O. du 13 juin 2009, p. 9666 ; Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet, J.O. n°251 du 29 octobre 2009 p. 18290.

[85] Le code pénal, articles 323-1 et suivants, les qualifie de « systèmes de traitement automatisé de données » (STAD). La jurisprudence a donné une interprétation extensive des STAD. Par exemple, il a été jugé que le radiotéléphone était un système (CA Paris, 18 nov. 1992, JCP E 1994, I, 359, obs. M. Vivant et C. Le Stanc) ; la même chose a été jugée à propos du réseau cartes de France Télécom (T. corr. Paris, 26 juin 1995, Petites affiches 1er mars 1976, note Alvarez) et de l'annuaire électronique de France Télécom (T. corr. Brest, 14 mars 1995, Petites affiches 22 juin 1995, note M. Choisy). Naturellement, il a été jugé qu'un service télématique est un système (CA Paris, 5 avr. 1994, Petites affiches 5 juill. 1995, note Alvarez ; JCP E 1995, I, 461, obs. M. Vivant et C. Le Stanc).

[86] Cass. civ. 3ème, 4 février 1976 ; n° de pourvoi : 74-12643, disponible sur le site www.legifrance.gouv.fr.

d'autres appellations telles que « *spécification à caractère normatif* » ou « *standard* » pour tout autre document de référence.

Concernant les exigences techniques applicables à la signature électronique, les dispositions réglementaires portent notamment sur les éléments de sécurité (profils de protection) des différents composants des outils de création de certificats et des produits de signature électronique publiés par le Comité Européen de Normalisation[87].

Les références précises des textes indispensables à la signature électronique sont explicitées dans un mémento édité par la DCSSI (Direction centrale de la sécurité des systèmes d'information devenue l'ANSSI)[88].

Dans le cadre français, l'authentification est traitée dans le cadre du Référentiel Général de sécurité (RGS)[89], à côté de la signature, du chiffrement et de l'horodatage. Ce référentiel s'applique aux relations entre les citoyens et les autorités administratives et ces dernières entre elles.

En outre, les prestataires de services de certification électronique (PSCE) doivent « *utiliser des systèmes et des produits garantissant la sécurité technique et cryptographique des fonctions qu'ils assurent »*[90].

L'authentification constitue une exigence essentielle en matière de sécurité des systèmes d'information dans certaines normes. Ainsi, la norme ISO 27001 fixant les méthodes et pratiques en matière de système de management de la sécurité de l'information (SMSI) prévoit une partie relative à la gestion des droits des utilisateurs[91] et par conséquent à leur authentification.

2. Exemples français en matière conformité légale et règlementaire

La conformité légale et règlementaire impose aux entreprises de plus en plus d'obligations. La plupart du temps, ces obligations vont s'appliquer sur un territoire donné. Certaines obligations sont sectorielles, par exemple en France, dans le domaine bancaire, le Règlement 97-02 ou le blanchiment et le financement du terrorisme (a), ou encore dans le secteur des jeux en ligne (b). D'autres obligations sont plus générales et s'appliquent quel que soit le secteur d'activité de l'entreprise. Ainsi, pour les pays de l'Union européenne, l'une des principales obligations concerne la protection des données à caractère personnel. Dans le

[87] Références CWA 14167-1, CWA 14167-2 et CWA 14169. Décision de la Commission 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, notifiée sous le numéro C (2003) 2439, 2003/511/CE.

[88] L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n° 2009-834 du 7 juillet 2009 (JO du 8 juillet 2009).

[89] V. l'arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques, JO n°0113 du 18 mai 2010, p.9152.

[90] V. l'article 6-II-g du décret n°2001-272 du 30 mars 2001. Eric A. Caprioli, *Référentiel général de sécurité : adoption de l'arrêté,* Comm. Com. Electr. n°7, juillet 2010, comm. 81.

[91] Eric A. Caprioli, *Introduction au droit de la sécurité des systèmes d'information,* in *Droit et technique, Etudes à la mémoire du Professeur Xavier Linant de Bellefonds*, éd. Litec, novembre 2007, article disponible sur le site www.caprioli-avocats.com.

domaine de la gestion de l'identité numérique, il est évident que l'identification directe ou indirecte des personnes physique impliquera le respect des règles applicables aux données personnelles par le responsable du traitement[92]. A ce titre, des formalités devront être accomplies auprès des autorités de contrôles compétentes (en France, la CNIL).

a) Blanchiment de capitaux et financement du terrorisme

Aux termes de l'article L. 561-5 du Code monétaire et financier : « « *I.- Avant d'entrer en relation d'affaires avec leur client ou de l'assister dans la préparation ou la réalisation d'une transaction, les personnes mentionnées à l'article L. 561-2 identifient leur client et, le cas échéant, le bénéficiaire effectif de la relation d'affaires par des moyens adaptés et vérifient ces éléments d'identification sur présentation de tout document écrit probant.*

Elles identifient dans les mêmes conditions leurs clients occasionnels et, le cas échéant, le bénéficiaire effectif de la relation d'affaires, lorsqu'elles soupçonnent que l'opération pourrait participer au blanchiment des capitaux ou au financement du terrorisme ou, dans des conditions fixées par décret en Conseil d'Etat, lorsque les opérations sont d'une certaine nature ou dépassent un certain montant.

II.- Par dérogation au I, lorsque le risque de blanchiment des capitaux ou de financement du terrorisme paraît faible et dans des conditions fixées par décret en Conseil d'Etat, il peut être procédé uniquement pendant l'établissement de la relation d'affaires à la vérification de l'identité du client et, le cas échéant, du bénéficiaire effectif. (…)»[93]

Il est important que les moyens mis en œuvre répondent au souci de sécuriser l'accès à un compte et de faire face aux menaces de fraude. Ainsi, consulter son compte requiert un minimum de confidentialité et engager une transaction ou procéder à un virement nécessite un formalisme et un niveau de sécurisation plus élevés garantissant leur traçabilité en cas de litige.

Dans cette perspective, les établissements bancaires (physiques) commencent à proposer à leurs clients un téléchargement de certificats (standard ou à la volée) pour signer des contrats ou des avenants aux contrats en cours. Dans ce cas précis, les risques de fraude sont relativement faibles, le client **étant déjà connu** du banquier et ses données d'identification enregistrées dans son back-office. Le recours à la signature électronique est précieux en termes de sécurité juridique et technique. Cette procédure est également retenue par certains établissements pour proposer des contrats d'assurance ou faciliter un changement d'intitulé de compte.

Les banques en ligne, quant à elles, du fait de leur ambition de dématérialiser la gestion de comptes, constituent un champ privilégié d'authentification forte, à tout le moins lors de la première « *mise en relation* » avec leurs clients. C'est un secteur particulièrement

[92] Sur les risques liés à la vie privée et aux données à caractère personnel en raison de l'utilisations des nouvelles technologies, v. Alex Türk, *La vie privée en danger*, Paris, éd. Odile Jacob, 2011.

[93] Les articles R. 563-1 et s. du Code Monétaire et Financier prévoient les modalités propres à assurer cette identification. Cette disposition législative se résume en un sigle « KYC » (Know Your Customer) qui constitue désormais un véritable sésame pour tout déploiement d'un service financier à distance.

prometteur dans la mesure où la réglementation impose aux banques en ligne des contraintes très strictes qui peuvent être idéalement mises en œuvre par des moyens d'authentification forte. En effet, l'ouverture de comptes (authentification) et les transactions sur le web (avec signature ou authentification) nécessitent l'utilisation de méthodes techniques sécurisées ayant une valeur juridique ou probatoire en cas de litige.

Le blanchiment de capitaux constitue une préoccupation majeure dans le secteur bancaire. En effet, à la suite des attentats intervenus en 2001 aux Etats-Unis et en 2004 en Europe, la lutte contre le terrorisme et le blanchiment d'argent s'est intensifiée. Afin de combattre cette nouvelle forme de guerre, des règles permettant de lutter efficacement contre le développement de ces réseaux criminels sont élaborées. Elles portent notamment sur le contrôle des flux financiers entre les différents Etats. Les pays démocratiques ont largement pris conscience des liens étroits noués entre terrorisme et blanchiment d'argent. Bras armé des Etats, le GAFI (Groupe d'Action Financière)[94] a proposé le principe d'une coopération internationale étroite, tout en soulignant la nécessité de mettre à profit les technologies de l'information pour contrer les actes de malveillance[95]. Ainsi, l'origine des fonds est-elle systématiquement contrôlée, tout comme les virements pour des montants élevés.

La Directive Européenne 2005/60/CE du Parlement et du Conseil du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme[96] constitue la réponse de l'Union européenne. Elle fait largement place au contrôle d'identité « *Conformément à ses dispositions, chaque État membre est tenu d'interdire le blanchiment de capitaux et d'imposer à son secteur.*
Pour mieux vérifier l'identité des clients, une définition précise du bénéficiaire effectif est indispensable. Plus précisément, les mesures de vigilance à l'égard de la clientèle comprennent :

- *l'identification du client et la vérification de son identité, sur la base de documents, de données ou d'informations de source fiable et indépendante;*
- *le cas échéant, l'identification du bénéficiaire effectif et la prise de mesures adéquates et adaptées au risque, pour vérifier son identité, de telle manière que l'établissement ou la personne soumis à la présente directive ait l'assurance de connaître ledit bénéficiaire effectif* (Article 8) ».

Cette directive a été transposée en droit français par une ordonnance en date du 30 janvier 2009 relative à la prévention de l'utilisation du système financier aux fins de blanchiment de

[94] Anglais FATF (Financial Action Task Force).
[95] *" In recent years, several governments worldwide have instituted electronic commerce laws that directly or indirectly require companies to reduce their vulnerability to identity theft. The United States, the European Union, Korea, Brazil, Japan, Australia, Singapore and many other nations have drafted or implemented regulations to safeguard consumer privacy, protect corporate data integrity and enhance auditing accountability. Standards to combat money laundering and terrorist financing that include customer identification have been proposed by the Financial Action Task Force (FATF), an inter-governmental organization, and have been adopted by more than 150 jurisdictions. In large part, these rules call for companies to adopt stronger identity authentication measures to assure governmental authorities about the veracity of their electronic transactions. Current and prospective regulations have created a boom in the interest in and use of identity authentication technologies such as digital certificates, biometrics, one-time passwords (OTP) and tokens*." citation provenant du rapport *"Complying with rules of Identity management"* réalisé par Economist Intelligence unit, p. 4, disponible à l'adresse : http://www.eiu.com/report_dl.asp?mode=fi&fi=1911955376.PDF.
[96] JOCE n°309 du 25 novembre 2005, p. 15-36.

capitaux et de financement du terrorisme[97]. Dans la pratique, en vertu de cette ordonnance, il existe une obligation pour un grand nombre de professionnels notamment de la finance, de la comptabilité et du droit, à procéder à une déclaration de soupçons pour les infractions punissables d'une peine d'emprisonnement supérieure à un an, conformément à l'article L. 561-15 du CMF. L'ordonnance a été ratifiée par l'article 140 de la loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures[98].

Le Règlement (CE) n°1781/2006 du Parlement européen et du Conseil du 15 novembre 2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds a été adopté dans un contexte de lutte contre le blanchiment des capitaux et le financement du terrorisme. Le « *financement du terrorisme* » (défini à l'article 2-1) est le fait, par quelque moyen que ce soit, directement ou indirectement, de fournir ou de réunir des fonds au sens de l'article 1er §4 de la directive 2005/60/CE, c'est-à-dire dans l'intention de les voir utilisés ou en sachant qu'ils seront utilisés, en tout ou en partie, en vue de commettre l'une quelconque des infractions visées aux articles 1er à 4 de la décision cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme[99]. L'objectif de ce règlement est, selon l'article premier, d'établir « *les règles relatives aux informations sur le donneur d'ordre qui doivent accompagner les virements de fonds, aux fins de prévention, de l'enquête et de la détection des activités de blanchiment de capitaux et de financement du terrorisme* ».

C'est à travers ces obligations de tracer et d'identifier leurs clients, à la charge des établissements financiers, que s'opère la lutte contre le blanchiment d'argent et le financement du terrorisme[100].

[97] L'ordonnance n°2009-104 du 30 janvier 2009, JO du 31 janvier 2009.
[98] JO n°110 du 13 mai 2009.
[99] J.O.C.E. L. 164, du 22 juin 2002, p. 3.
[100] Ainsi l'article L. 563-1 du Code monétaire et financier dispose : « *Les organismes financiers ou les personnes visées à l'article L. 562-1 doivent, avant de nouer une relation contractuelle ou d'assister leur client dans la préparation ou la réalisation d'une transaction, s'assurer de l'identité de leur cocontractant par la présentation de tout document écrit probant. Ils s'assurent dans les mêmes conditions de l'identité de leur client occasionnel qui leur demande de faire des opérations dont la nature et le montant sont fixés par décret en Conseil d'Etat. Les personnes visées au 8 de l'article L. 562-1 satisfont à cette obligation en appliquant les mesures prévues à l'article L. 565-1. Ils se renseignent sur l'identité véritable des personnes avec lesquelles ils nouent une relation contractuelle ou qui demandent leur assistance dans la préparation ou la réalisation d'une transaction lorsqu'il leur apparaît que ces personnes pourraient ne pas agir pour leur propre compte. Les organismes financiers et les personnes mentionnés à l'article L. 562-1 prennent les dispositions spécifiques et adéquates, dans les conditions définies par un décret, nécessaires pour faire face au risque accru de blanchiment de capitaux qui existe lorsqu'elles nouent des relations contractuelles avec un client qui n'est pas physiquement présent aux fins de l'identification ou lorsqu'elles l'assistent dans la préparation ou la réalisation d'une transaction.* ».

b) Les jeux en ligne[101]

Quant au secteur des jeux en ligne, le législateur français a fixé dans la loi du 10 mai 2010 de nombreuses mesures de sécurité informatique en prévoyant notamment, à la charge de l'opérateur candidat (à la licence), de préciser « *les modalités d'accès et d'inscription à son site de tout joueur et les moyens lui permettant de s'assurer de l'identité de chaque nouveau joueur, de son âge, de son adresse et de l'identification du compte de paiement sur lequel sont versés ses avoirs* […] » (article 17). Les mesures de vérification d'identité constituent donc une exigence essentielle pour tout candidat. L'une des méthodes permettant d'assurer cette vérification est relative à l'approvisionnement du compte joueur. En effet, conformément à l'article 17, cet approvisionnement ne peut être réalisé « *qu'au moyen d'instruments de paiement mis à disposition par un prestataire de services de paiement établi dans un Etat membre de la Communauté européenne ou un Etat partie à l'accord sur l'Espace économique européen*[…] ». Dès lors, la vérification d'identité relève en partie du prestataire de services de paiement (établissement de paiement et établissement de crédit au sens de l'art. L. 521-1 du C.M.F suite à la transposition de la directive 2007/64 du 13 novembre 2007)[102]. Cela ne signifie pas pour autant que l'opérateur pourra se défausser de cette vérification d'identité. L'article 38 de la loi prévoit, en outre, que les opérateurs

[101] V. Olivier de Mattos, *Le nouveau droit fixe dû par les opérateurs des jeux en ligne se fixe,* Comm. Com. Electr., mai 2010, n°5, alerte 57 ; Eric. A. Caprioli, *Paris en ligne*, Comm. Com. Electr., juillet 2010, n°7, comm. 79 ; Pauline Le More et Olivier Sautel, *L'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne en France : éclairages économique et juridique croisés,* Contrats, Concurrence, Consommation juin 2010, n°6, et. n°7 ; Linda Arcelin-Lécuyer, *Loi sur l'ouverture des jeux et paris en ligne à la concurrence : une réforme bien timide ;* Contrats, Concurrence, Consommation juin 2010, n°6, alerte 42 ; David Bosco, *Réformer la politique de sanction de l'Autorité ?,* Contrats, Concurrence, Consommation, novembre 2010, n°11, comm. 261 ; Loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne (JO du 13 mai 2010, p. 8881) ; Décret n° 2010-1070 du 8 septembre 2010 modifiant le décret n° 2010-481 du 12 mai 2010 relatif à l'organisation et au fonctionnement de l'Autorité de régulation des jeux en ligne (JO du 10 septembre 2010, p.16469 s.) ; Décret n° 2010-798 du 12 juillet 2010 modifiant le décret n° 2010-498 du 17 mai 2010 relatif à la définition des courses hippiques supports des paris en ligne et aux principes généraux du pari mutuel (JO du 14 juillet 2010, p. 13101 s.) ; Décret n° 2010-723 du 29 juin 2010 relatif aux catégories de jeux de cercle mentionnées au II de l'article 14 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne ainsi que les principes régissant leurs règles techniques (JO du 30 juin 2010, p. 11810 s.) ; Arrêté du 8 juin 2010 fixant le contenu et les modalités d'affichage des messages de mise en garde prévus par les articles 26, 28, 29 et 33 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne (JO du 9 juin 2010, p.10573 s.) ; Décret n° 2010-624 du 8 juin 2010 relatif à la réglementation des communications commerciales en faveur des opérateurs de jeux d'argent et de hasard ainsi qu'à l'information des joueurs quant aux risques liés à la pratique du jeu (JO du 9 juin 2010, p. 10575 s.) ; Décret n° 2010-623 du 8 juin 2010 fixant les obligations d'information des opérateurs agréés de jeux ou de paris en ligne pour la prévention des risques liés à la pratique du jeu et modifiant le décret n° 2010-518 du 19 mai 2010 relatif à la mise à disposition de l'offre de jeux et de paris par les opérateurs agréés de jeux ou de paris en ligne (JO du 9 juin 2010, p.10575 s.) ; Décret n° 2010-518 du 19 mai 2010 relatif à la mise à disposition de l'offre de jeux et de paris par les opérateurs agréés de jeux ou de paris en ligne (JO du 20 mai 2010, p.9295 s.) ; Décret n° 2010-509 du 18 mai 2010 relatif aux obligations imposées aux opérateurs agréés de jeux ou de paris en ligne en vue du contrôle des données de jeux par l'Autorité de régulation des jeux en ligne (JO du 19 mai 2010, p.9223 s.) ; Décret n° 2010-495 du 14 mai 2010 relatif à la procédure de sanction applicable aux opérateurs agréés de jeux ou de paris en ligne (JO du 15 mai 2010 ; p.9052 à 9054) ; Décret n° 2010-482 du 12 mai 2010 fixant les conditions de délivrance des agréments d'opérateur de jeux en ligne (JO du 13 mai 2010, p. 8930 s.) ; Décret n° 2010-481 du 12 mai 2010 relatif à l'organisation et au fonctionnement de l'Autorité de régulation des jeux en ligne (JO du 13 mai 2010, p.8927 s .).

[102] J.O U.E. du 5 décembre 2007, p.1 et s.

doivent mettre à disposition permanente de l'ARJEL (Autorité de régulation des jeux en ligne) – entre autres - les données portant sur l'identité de chaque joueur, son adresse et son adresse de courrier électronique ainsi que le compte du joueur. Les opérateurs doivent donc disposer d'une base de données à caractère personnel détaillée et respecter les exigences de la loi Informatique, Fichiers et Libertés (article 19). Là encore, rappelons que l'article 34 de cette dernière loi prévoit la mise en place de mesures de sécurité à l'initiative du responsable de traitement. L'objectif principal consiste à préserver la sécurité des données et, à ce titre, le responsable du traitement occupe une place prépondérante, de même que l'opérateur joue un rôle considérable dans le processus de protection et de vérification des données utilisées pour le site de jeux.

Il convient d'étudier maintenant, les aspects juridiques de la gestion des identités numériques qui pourraient faire l'objet de travaux à la C.N.U.D.C.I. en vue de contribuer à la confiance dans les communications électroniques internationales.

II. Mise en œuvre juridique internationale

La confiance repose principalement sur un sentiment psychologique des acteurs du marché[103]. Même si la confiance ne se décrète pas, les instruments juridiques internationaux, notamment ceux de la C.N.U.D.C.I., sont particulièrement importants dans la mesure où ce sont les seuls à pouvoir servir de supports juridiques aux pratiques et usages des méthodes d'authentification et de signature électronique. Les normes juridiques ont une portée et une effectivité du fait de la source de laquelle elles procèdent : une institution internationale, légitime et reconnue, la C.N.U.D.C.I.

Rappelons que la C.N.U.D.C.I. peut élaborer des instruments juridiques de natures très variées : règles normatives plus ou moins contraignantes (recommandations, guides et lignes directrices, principes généraux, loi-type, ou convention internationale). Il appartiendra, sans doute à la fin des travaux du groupe de travail, aux représentants des Etats membres de décider de la nature juridique du (ou des) instruments juridiques.

Encore faudra-t-il que lors de sa prochaine session[104], la Commission décide de (re)lancer le Groupe de Travail IV « *Commerce électronique* » dont la dernière session s'est tenue en 2004[105], sur les aspects juridiques de la gestion de l'identité dont certains aspects ont déjà été esquissés dans les travaux relatifs aux lois-types sur le Commerce et la Signature électroniques.

Dix-huit pays ont répondu à un questionnaire de l'OCDE sur la gestion des identités numériques. Outre les différences historiques et culturelles des systèmes juridiques, il apparaît qu'il ne peut pas y avoir une approche générique et unique sur ces questions[106]. Cependant, plusieurs facteurs devront être pris en considération lors de l'amorce

[103] Valérie-Laure Benabou et de Muriel Chagny (sous la direction), *La confiance en droit privé des contrats*, Paris, Dalloz, 2008.
[104] La 44ème session est prévue du27 juin au 15 juillet 2011 à Vienne.
[105] http://www.uncitral.org/uncitral/fr/commission/working_groups/4Electronic_Commerce.html.
[106] V. l'intervention de M. Laurent Bernat, membre du Secrétariat de l'OCDE, en date du 14 février 2011 lors du colloque de la CNUDCI à New York : www.uncitral.org. V. égale. Le site : www.oecd.org/sti/security-privacy.

d'éventuels travaux : l'interopérabilité, le respect de la vie privée, la confidentialité et l'ergonomie des nouveaux usages.

Les travaux sur les méthodes d'authentification et de signature pourraient envisager d'établir des règles relatives à certaines notions de base qu'il convient de définir et d'encadrer (a), mais aussi de poser les principes fondamentaux d'autres aspects essentiels à la mise en œuvre concrète (interopérabilité, méthodes d'authentification à suivre, horodatage, …) de la reconnaissance croisée des méthodes d'authentification, des fédération d'identités, ou encore de renvoyer aux Etats la mise en place des processus de labellisation respectant certains principes et objectifs (b).

A. Des règles normatives sur les éléments de base

Au regard des analyses développées ci-dessus, il apparaît qu'il existe de nombreux écueils à la reconnaissance des effets juridiques des méthodes d'authentification dans les communications électroniques internationales. Cependant, il est possible d'y pallier, à tout le moins pour partie, par la technique contractuelle, et sous réserve d'éventuelles prescriptions impératives du droit national applicable (droits et libertés fondamentales des personnes, droit de la consommation, droit social, dispositions pénales, …).

A l'heure actuelle, et outre certaines définitions techniques issues de normes internationales[107], régionales ou nationales[108], les définitions juridiques des principaux

[107] Par exemple, les normes :

- ISO/IEC 9797 Information technology - Security techniques - Message Authentication Codes (MACs) ;
- ISO/IEC 9798 Information technology — Security techniques — Entity authentication ;
- ISO/IEC 18013 Information technology — Personal Identification — ISO-compliant driving license et notamment :
  - ISO/IEC 18013-3:2009(E) Part 3: Access control, authentication and integrity validation ;
- ISO/IEC 24727 Identification cards — Integrated circuit card programming interfaces et notamment :
  - ISO/IEC FCD 24727-6 — Part 6: Registration authority procedures for the authentication protocols for interoperability.

L'IETF s'est également positionnée sur cette question :

- RFC 4422, Simple Authentication and Security Layer (SASL), Juin 2006.
- RFC 4954, SMTP Service Extension for Authentication, Juillet 2007.

L'ETSI prévoit :

- ETSI TS 187 001 V3.3.0 (décembre 2009, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) NGN SECurity (SEC) Requirements.

[108] En France, selon le R.G.S., dans le cadre d'une authentification lors d'un accès à un téléservice ou d'une authentification auprès d'une personne physique, la partie qui doit s'authentifier applique une transformation cryptographique, à l'aide de sa clé privée, à une requête d'authentification générée par la partie souhaitant vérifier l'authentification. Le lien entre cette phase d'authentification et les échanges qui suivent ("ouverture du canal de communication") doit ensuite être garanti avec une sécurité équivalente. Dans le cadre de l'authentification d'un message ou de données, l'authentification est réalisée par l'usager ou par l'agent en appliquant une transformation cryptographique au message ou aux données à authentifier, à l'aide de sa clé privée. Le service d'authentification permet de garantir l'intégrité et l'origine du message / des données authentifiées mais, contrairement au service de signature électronique, il ne signifie pas que l'émetteur manifeste son consentement sur le contenu du message ou des données.
Le service de confiance de signature électronique permet de garantir l'identité du signataire, l'intégrité du document signé ainsi que la manifestation du consentement du signataire quant au contenu des données électroniques ainsi signées. L'usager ou l'agent devant signer électroniquement un message ou un fichier utilise

concepts, en dehors de la signature sous forme électronique[109], ne sont ni unifiées, ni harmonisées[110]. Toutefois, de manière générale et non exhaustive, on notera que la question de l'authentification est consubstantielle de celle de la sécurité et qu'elle innerve à ce titre chaque produit ou service recourant à des réseaux mobiles, WIFI ou autres. En ce sens, les méthodes d'authentification jouent un rôle essentiel dans les communications électroniques internationales. Or, pour la sécurité juridique, il est important de connaître les définitions et les qualifications associées aux principales notions qui sont susceptibles de générer des conséquences juridiques. Par exemple, certains thèmes ci-dessous pourraient être étudiés dans le groupe de travail IV « *Commerce électronique* » de la C.N.U.D.C.I.

1. Authentification électronique

Il s'agit ici des méthodes les plus courantes telles que le login/mot de passe, jusqu'à des méthodes de vérification d'identité et d'origine d'une demande qui s'appuie sur des OTP (One Time password), des certificats électroniques ou encore à l'association de deux facteurs et deux médias (ex : en ligne et par téléphone mobile). Ainsi, l'authentification peut

---

une clé privée asymétrique qu'il détient et qu'il met en œuvre dans un dispositif de création de signature qu'il doit garder sous son contrôle.

[109] Loi type de la CNUDCI sur les signatures électroniques, 2001, art. 2-a) : *Le terme "signature électronique" désigne* ***des données sous forme électronique contenues dans un message de données ou jointes ou logiquement associées audit message, pouvant être utilisées pour identifier le signataire dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue*** ; Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux, 2005, art. 7 : *Aucune disposition de la présente Convention n'a d'incidence sur l'application d'une règle de droit obligeant les parties à communiquer leur identité, leur établissement ou toute autre information, ni n'exonère une partie des conséquences juridiques auxquelles elle s'exposerait en faisant des déclarations inexactes, incomplètes ou fausses à cet égard* ; art. 9 : *1. Aucune disposition de la présente Convention n'exige qu'une communication ou un contrat soit établi ou constaté sous une forme particulière. 2. Lorsque la loi exige qu'une communication ou un contrat soit sous forme écrite, ou prévoit des conséquences juridiques en l'absence d'un écrit, une communication électronique satisfait à cette exigence si l'information qu'elle contient est accessible pour être consultée ultérieurement. 3. Lorsque la loi exige qu'une communication ou un contrat soit signé par une partie, ou prévoit des conséquences en l'absence d'une signature, cette exigence est satisfaite dans le cas d'une communication électronique : a) Si une méthode est utilisée pour identifier la partie et pour indiquer la volonté de cette partie concernant l'information contenue dans la communication électronique ; et b) Si la méthode utilisée est : i) Soit une méthode dont la fiabilité est suffisante au regard de l'objet pour lequel la communication électronique a été créée ou transmise, compte tenu de toutes les circonstances, y compris toute convention en la matière; ii) Soit une méthode dont il est démontré dans les faits qu'elle a, par elle-même ou avec d'autres preuves, rempli les fonctions visées à l'alinéa a ci-dessus. 4. Lorsque la loi exige qu'une communication ou un contrat soit disponible ou conservé sous sa forme originale, ou prévoit des conséquences juridiques en l'absence d'un original, cette exigence est satisfaite dans le cas d'une communication électronique : a) S'il existe une garantie fiable quant à l'intégrité de l'information qu'elle contient à compter du moment où elle a été créée pour la première fois sous sa forme définitive, en tant que communication électronique ou autre ; et b) Si, lorsqu'il est exigé que l'information qu'elle contient soit disponible, cette information peut être présentée à la personne à laquelle elle doit être rendue disponible. 5. Aux fins de l'alinéa a du paragraphe 4 : a) L'intégrité de l'information s'apprécie en déterminant si celle-ci est restée complète et n'a pas été altérée, exception faite de l'ajout de tout endossement et de toute modification susceptible d'intervenir dans le processus normal de la communication, de la conservation et de l'affichage ; et b) Le niveau de fiabilité requis s'apprécie au regard de l'objet pour lequel l'information a été créée et à la lumière de toutes les circonstances y ayant trait .»* Eric A. Caprioli, *Droit international de l'économie numérique*, préface R. Sorieul, Ed. Litec, 2ème édition, mars 2007, p.87-90.

[110] Franck Violet, *Articulation entre la norme technique et la règle de droit*, Préface J. Schmidt-Szalewski, P.U. Aix-Marseille, 2003 ; Anne 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*, P. Aff., 11 février 1998, n°18, p. 28-34.

être dite « simple » ou forte en fonction des moyens de sécurité mis en place. Aujourd'hui, on parle de plus en plus souvent d'IAM (Identity & Acces Management) dans les grandes entreprises. Les instruments technico-juridiques d'IAM ont pour objectifs de fournir les principes et les modalités de gouvernance de tous les identifiants utilisés, ainsi que la gestion des droits et des habilitations de chacun. Pour l'organisation de ces éléments, les entités ont la possibilité de recourir à des politiques d'IAM, en fonction de leurs besoins et des méthodes utilisées. Toutefois, de telles politiques doivent être opposables aux utilisateurs qu'ils soient internes ou externes. Les Politiques d'IAM doivent assurer l'interopérabilité d'accès entre deux entités partageant un même single sign on (SSO). Elles permettent également de déterminer le niveau d'identification attendu par rapport à un produit ou un service. En effet, plus un service sera sensible (engageant financièrement), plus le niveau d'authentification requis sera important.

2. Signature électronique « technique »

Les deux principales fonctions juridiques de ce procédé sont le scellement à des fins d'intégrité et d'authenticité de l'origine. On retrouve ce système dans plusieurs textes de l'Union européenne telle que la signature électronique avancée, exigée dans le cadre des factures électroniques[111] et qui peut consister en une signature électronique technique, sans intervention humaine pour la saisine des données d'activation à l'occasion de chaque facture. Ces procédés de signature électronique technique renvoient également à la signature de la personne morale avec un certificat de serveur (voir infra II-A-4). Les types de procédés cryptographiques visés ont des applications multiples dans les échanges et les transactions électroniques, spécialement pour garantir de multiples preuves de faits juridiques comme des dates. Cela peut se traduire concrètement par des opérations sur les transmissions de documents électroniques comme les notifications, les envois, les dépôts, ou les accusés de réception. L'utilisation de ces procédés de signature électronique trouvent également leur place pour les documents des ressources humaines (bulletins de paie, notes de frais, …).

---

[111] L'article 233 de la directive 2006/112/CE relative au système commun de taxe sur la valeur ajoutée en ce qui concerne les règles de facturation modifié par la Directive 2010/45/UE du Conseil du 13 juillet 2010 (JOUE L 189 du 22 juillet 2010, p. 1–8) énonce :

« *1. L'authenticité de l'origine, l'intégrité du contenu et la lisibilité d'une facture, que celle-ci se présente sur papier ou sous forme électronique, sont assurées à compter du moment de son émission et jusqu'à la fin de sa période de conservation.*

Chaque assujetti détermine la manière dont l'authenticité de l'origine, l'intégrité du contenu et la lisibilité de la facture sont assurées. Cela peut être réalisé par des contrôles de gestion qui établiraient une piste d'audit fiable entre une facture et une livraison de biens ou de services.

On entend par "authenticité de l'origine" l'assurance de l'identité du fournisseur ou de l'émetteur de la facture.

On entend par "intégrité du contenu" le fait que le contenu prescrit par la présente directive n'a pas été modifié.

2. Outre le type de contrôles de gestion décrits au paragraphe 1, les méthodes suivantes constituent des exemples de technologies permettant d'assurer l'authenticité de l'origine et l'intégrité du contenu d'une facture électronique :

a) une ***signature électronique avancée*** *au sens de l'article 2, point 2, de la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques [*], fondée sur un certificat qualifié et créée par un dispositif sécurisé de création de signature au sens de l'article 2, points 6 et 10, de ladite directive ;*

b) un échange de données informatisées (EDI) tel que défini à l'article 2 de la recommandation 94/820/CE de la Commission du 19 octobre 1994 concernant les aspects juridiques de l'échange de données informatisées [**] lorsque l'accord relatif à cet échange prévoit l'utilisation de procédures garantissant l'authenticité de l'origine et l'intégrité des données.».

La traçabilité des opérations se retrouvent dans de très nombreuses applications métiers, et dans la plupart des secteurs d'activités économiques : banques, assurances, industries diverses comme l'aéronautique, l'automobile, la santé, la grande distribution, …). Par exemple, la traçabilité fera partie des mesures de sécurité techniques qu'il faut respecter du point de vue de la conformité légale[112] dans les systèmes de back et de middle office en salle de marché[113].

3. Datation électronique[114]

La datation électronique ou horodatage est un système qui consiste en l'association d'une date à un acte ou à un fait juridique. Sur le plan technique, le procédé d'horodatage se fonde sur la cryptographie[115]. Son utilité est très importante dans la mesure où le procédé permet d'assurer, en outre, une fonction d'intégrité des données auxquelles la date est associée. On va retrouver la datation électronique dans de nombreuses applications telles que les notifications et les envois recommandés avec ou sans accusé de réception[116],

Les lettres recommandées électroniques ont été prises en compte en France (Article 1369-8 du Code civil et son décret d'application : le Décret n° 2011-144 du 2 février 2011 relatif à

---

[112] Règlement n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement, art. 30-1 : *Les prestataires doivent disposer d'un système de suivi des opérations d'intermédiation permettant notamment : (…) d'enregistrer à la fin de chaque journée et de retracer individuellement toutes erreurs dans la prise en charge et l'exécution des ordres. Ces positions doivent être considérées au plan de la surveillance et de la maîtrise des risques comme des risques de marché pris pour compte propre. Les prestataires qui ne sont pas habilités à fournir le service de négociation pour compte propre dénouent ces positions sans délai. Chaque incident doit faire l'objet d'un document descriptif porté à la connaissance de l'un des responsables pour le contrôle permanent prévu au premier tiret du point a de l'article 6 dès lors que l'erreur est supérieure à un seuil établi par l'organe exécutif.* ; modifié notamment par un arrêté du 19 janvier 2010 modifiant le règlement n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement (JO n°0036 du 12 février 2010, texte n°35) ; v. égal. le règlement relatif aux fonds propres des établissements de crédit et des entreprises d'investissement « *Convergence internationale de la mesure et des normes de fonds propres* » (Bâle II), prévoyant la mise en place d'un dispositif de surveillance prudentielle qui « *vise non seulement à garantir que les banques disposent de fonds propres adéquats pour couvrir l'ensemble des risques liés à leurs activités, mais également à les inciter à élaborer et à utiliser de meilleures techniques de surveillance et de gestion des risques. Le processus de surveillance prudentielle reconnaît qu'il appartient à l'organe de direction d'élaborer un processus interne d'évaluation des fonds propres et de fixer des objectifs de fonds propres correspondant au profil de risque et à la structure de contrôle de l'établissement. Dans le dispositif révisé, l'organe de direction demeure chargé de veiller à ce que son établissement soit doté de fonds propres suffisants, au-delà des exigences minimales de base, pour couvrir les risques auxquels il est exposé.* »

[113] Tribunal correctionnel de Paris 5 octobre 2010, Société générale c./Kerviel, Comm. Com. Electr. Février 2011, com. n°16, p.36, note Eric A. Caprioli ; Didier Rebut, *Affaire Kerviel : «le tribunal n'avait pas le pouvoir d'individualiser les dommages et intérêts sur le modèle de l'individualisation des peines»*, JCP éd. G, 2010, 1019 ; pour une critique virulente de la décision : Félix Rome, *Ne tirez plus sur le lampiste,* D. 2010, Editorial du 14 octobre 2010, n°35 ; Expertises des systèmes d'information, Novembre 2010, p.362, Editorial, *Kerviel/Société générale : une affaire de fraude informatique.*

[114] Laurent Jacques, *La date électronique et le contrat,* in *Les deuxièmes journées internationales du droit du commerce électronique,* Litec, 2005, p. 165 et s.

[115] Marie Demoulin, *Aspects juridique de l'horodatage des documents électroniques*, in *Commerce électronique : de la théorie à la pratique*, Cahiers du C.R.I.D. n°23, Bruxelles, Bruylant, 2003, v .p.43 et s.

[116] Etienne Montero, *Du recommandé traditionnel au recommandé électronique : vers une sécurité et une force probante renforcées*, in *Commerce électronique : de la théorie à la pratique*, Cahiers du C.R.I.D. n°23, Bruxelles, Bruylant, 2003, v.p.69 et s.

l'envoi d'une lettre recommandée par courrier électronique pour la conclusion ou l'exécution d'un contrat[117]) pour les cas de mise en demeure, de résiliation, d'information obligatoire prévus par les textes.

L'admission de la lettre recommandée adressée par voie électronique pour la conclusion ou l'exécution du contrat est subordonnée au respect des conditions suivantes :

- le courrier doit avoir été acheminé par un tiers selon un procédé permettant d'identifier ce dernier ;
- l'expéditeur doit être désigné ;
- l'identité du destinataire doit être garantie ;
- la remise effective de la lettre au destinataire doit également être garantie ;
- la date d'expédition doit être fiable ou présumée fiable conformément aux dispositions du Décret n°2011-434 du 20 avril 2011)[118].
-

Par ailleurs, deux modalités de réception du courrier recommandé électronique sont prévues à l'alinéa 2 de l'article 1369-8 du Code civil, lesquelles sont laissées au libre choix de l'expéditeur à la condition que le destinataire soit un professionnel ou s'il s'agit d'un consommateur ou d'un non professionnel, que ce dernier ait sollicité un envoi d'une lettre recommandée sous forme électronique ou qu'il y ait préalablement consenti, notamment dans le cadre d'échanges antérieurs. Ainsi, d'une part, le courrier peut faire l'objet d'une réception électronique par le destinataire (lettre recommandée entièrement électronique) et d'autre part, le courrier peut être imprimé par le tiers chargé de l'acheminer puis distribué sous forme papier au destinataire par La Poste. Cette dernière possibilité est importante puisqu'elle vise certaines pratiques dites « *hybrides* ».

4. Signature « juridique » d'une personne morale[119]

Dans cette hypothèse, comme dans la précédente (signature technique), la signature s'opère également via un certificat de serveur, mais une différence fondamentale existe : elle engage une personne morale sans que la signature soit mise en œuvre directement par une personne physique qui saisit ses données d'activation de la clé privée, mais par le biais d'un agent électronique[120]. Le système de signature peut être entièrement automatisé. Dans tous les cas, il y a toujours une personne physique dument habilitée pour programmer le serveur et indiquer quels sont les messages qui doivent être signés par la machine au nom de la personne morale. En effet, lorsqu'une entreprise signe de nombreux contrats en ligne, il est très difficile en pratique de désigner une personne physique agissant au nom et pour le

[117] J.O. du 4 février 2011 p.2274. Pour un commentaire de ce texte, v. Eric Caprioli, Comm. Com. Electr., avril 2011.

[118] D. n°2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat, JO du 21 avril 2011, p.7093 ; Arrêté du 20 avril 2011 relatif à la reconnaissance de la qualification des prestataires de services d'horodatage électronique et à l'accréditation des organismes qui procèdent à leur évaluation, JO du 21 avril 2011, p.7094. Pour un commentaire, v. Eric Caprioli, Comm. Com. Electr. Juillet-Août 2011, p.42-43. *Les lettres recommandés électroniques*, Cahier de droit de l'entreprise, Mai-Juin, Fiche pratique, Eric Caprioli.

[119] Sur le sujet, v. Mireille Antoine et Didier Gobert, *La directive européenne sur la signature électronique. Vers la sécurisation des transactions sur l'Internet ?*, J.T.D.E., 2000, p.73 s.

[120] Eric A. Caprioli, *Consentement et systèmes d'information*, Revue de la rech. jurid. Droit prospectif, 1999-4, éd. PUAM, p. 1075 et s ; Yves Poullet, *La conclusion du contrat par un agent électronique*, Cahiers du CRID n°17, éd. Bruylant, Bruxelles, 2000, p. 129 et s. ; Eric A. Caprioli, L'a*gent électronique et le contrat*, in *Les deuxièmes journées internationales du droit du commerce électronique,* Litec, 2005, p. 215.

compte de la personne morale et qui entre ses données d'activation du certificat pour chaque transaction. Cette signature de la personne morale garantirait les fonctions juridiques de la signature électronique (identification et intégrité), en ce y compris la manifestation de volonté de la personne.

A la vérité, deux questions juridiques de fond se posent : est-ce que la personne morale n'est engagée que par la signature de la personne physique qui la représente ? Et, est-ce que la personne morale peut signer elle-même via un système d'information, de façon automatique et sans intervention humaine directe ?

L'article 12 de la convention de la C.N.U.D.C.I. de 2005 prévoit la validité ou la force exécutoire de la formation des contrats par l'interaction de systèmes de messagerie automatisée (agent électronique) ne peuvent pas être contestées. Mais cet article ne traite pas de la question de la signature électronique par un agent électronique. Les réponses législatives et règlementaires divergent.

Alors que le droit français semble exclure la possibilité d'une personne morale signataire d'un acte[121] sans l'intervention d'une personne physique, certains systèmes juridiques semblent avoir consacrés cette solution juridique de façon imparfaite. Ainsi, si l'on se penche sur la loi relative au commerce électronique du Luxembourg, la notion de signataire est définie à l'article 17 comme : « *toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une personne physique ou morale qu'elle représente* »[122]. En droit belge, en revanche, l'article 4 § 4 de la loi du 9 juillet 2001 dispose : « *une signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, est assimilée à une signature manuscrite, qu'elle soit réalisée par une personne physique ou morale* », mais son article 8 § 3 précise, ce qui n'est pas exigé par le droit du Luxembourg, que « *le prestataire de services de certification tient un registre contenant le nom et la qualité de la personne physique qui représente la personne morale et qui fait usage de la signature liée au certificat, de telle manière qu'à chaque utilisation de cette signature, on puisse établir l'identité de la personne physique*. ».

Une harmonisation internationale sur ce point semble opportune, étant donné les divergences qui existent sur le sujet avec des conséquences juridiques radicalement opposées : validité ou nullité de l'acte signé.

5. Certificats « éphémères » ou « à la volée »

Eu égard la lenteur du déploiement des signatures et des certificats électroniques, le marché a mis en œuvre d'autres méthodes plus pragmatiques mais qui n'omettent pas pour autant la sécurité juridique nécessaire à une transaction. Ainsi, les certificats « éphémères » ou « à la volée » auxquels les acteurs ont recours sur certains marchés notamment en France pour conclure des contrats de crédit à la consommation par voie électronique ou pour réaliser des

[121] Selon le Décret du 30 mars 2001, seule une personne physique peut être titulaire d'un certificat et a contrario, une personne morale ne peut pas l'être. V. égal. Thierry Piette-Coudol, *Le bilan de dix ans de signature électronique*, RLDI, Décembre 2010, spéc. p.78 à 81.

[122] André Prüm, Yves Poullet, Etienne Montero (sous la direction scientifique), *Le commerce électronique en droit luxembourgeois*, Bruxelles, Larcier, 2005, v. les développements sur ce texte : n°178 à 180.

paiements (par exemple des virements ou des prélèvements), ou encore pour souscrire des contrats d'assurance. Une réserve doit cependant être posée : ces solutions ne s'appliquent qu'à l'occasion de transactions avec des clients déjà connus et identifiés par l'établissement bancaire ou de crédit.

Ces certificats peuvent se définir comme des fichiers électroniques attestant qu'une bi-clé appartient à la personne physique (mais pourquoi pas à une personne morale ou à l'élément matériel ou logiciel identifié), directement ou indirectement (pseudonyme). Ce certificat transactionnel est valide pendant une durée de temps donnée qui est précisée dans un de ses champs[123]. Le certificat éphémère ne sera valable que pour un seul contrat ou transaction. Et il ne peut être mis en œuvre que pour des personnes déjà connues par le commerçant, étant donné qu'il convient de disposer au préalable des informations les concernant à des fins d'enregistrement pour établir le certificat.

Avec ce type de signature, il n'y a pas de Liste de révocation des certificats à gérer par le Prestataire de services de certification électronique (P.S.C.E.), ce qui réduit considérablement le risque de compromission du certificat.

En principe, il faut prévoir une politique de gestion de preuve afin que le fichier y afférent comporte tous les éléments informatiques (ex : contrat signé, certificat éphémère, date) nécessaires à l'établissement du contrat, avant que ce dernier ne soit verser au service d'archivage électronique.

Concrètement, le client signera à l'issue d'un processus contractuel en ligne, en cliquant sur un bouton où il est indiqué « *je signe* » ou « *signer* ».

De plus en plus souvent, pour des raisons de sécurité, cette technologie se double de l'envoi d'un OTP ou d'un code unique et généré de façon aléatoire sur le téléphone mobile du client comme mesure de « *sur-authentification* » ou d'authentification forte.

6. Obligations et responsabilités dans le cadre d'une Infrastructure à clé Publique (ICP).

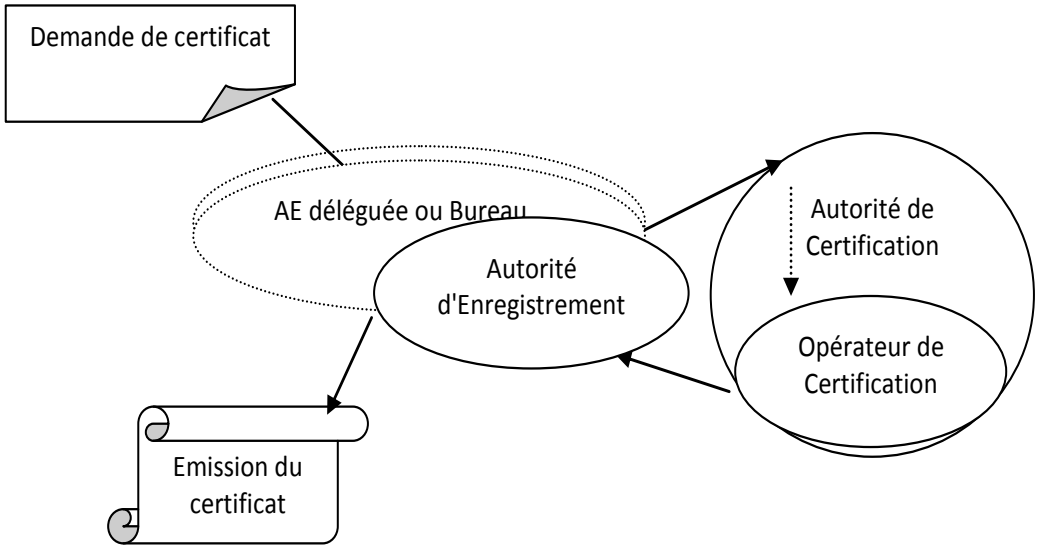
Une I.C.P. comprend plusieurs entités qui ont des fonctions et des responsabilités distinctes. A côté des utilisateurs des certificats (signataire et partie qui se fie au certificat), plusieurs métiers coexistent : Autorité de certification, Opérateur de certification et Autorité d'enregistrement, Services de publication (annuaire ou liste de révocation des certificats ou liste des autorités de certification reconnues), autorité de validation, autorité et opérateur d'horodatage.

Il ressort de ce système que la confiance dépend de l'ensemble des composantes de l'I.C.P. dont les rôles et responsabilités sont définis dans la politique de certification (P.C.) et les conventions.

L'I.C.P. est constituée d'un ensemble de moyens techniques, humains, documentaires et contractuels mis à la disposition des utilisateurs pour assurer un environnement sécurisé aux échanges électroniques. La mise en œuvre d'une Infrastructure à Clé Publique permet de

[123] En général, la durée varie de quelques dizaines de secondes à une à deux minutes au plus.

s'assurer de la correspondance entre une clé publique figurant dans un certificat et un titulaire du certificat (celui qui signe à l'aide de la clé privée), ainsi que de fournir des services à valeur ajoutée pour les transactions électroniques[124]. Les certificats électroniques peuvent servir aux courriers électroniques, transactions commerciales, téléprocédures, etc., mais aussi à la protection de la confidentialité des données. L'I.C.P. permet de vérifier et d'assurer l'exactitude et l'intégrité des informations concernant le titulaire, réunies lors de leur collecte au moment de l'enregistrement et figurant dans le certificat. Ces données sont particulièrement importantes lors l'identification du signataire d'un acte ou de son authentification. Elle peut prendre plusieurs formes techniques[125], allant du modèle interne pour un intranet d'entreprise jusqu'au modèle externe sur l'Internet.



Exemple d'organisation et d'interaction entre les composantes de l'ICP pour l'obtention d'un certificat.

[124] CNUDCI, Doc. A/CN.9/ 493, § 50 : «*Pour inspirer cette confiance, une Infrastructure à Clé Publique peut offrir un certain nombre de services, dont les suivants : 1) gérer les clés cryptographiques utilisées pour les signatures numériques ; 2) certifier qu'une clé publique correspond bien à une clé privée ; 3) fournir des clés aux utilisateurs finaux ; 4) décider quels utilisateurs se verront conférer tel ou tel privilège dans le système ; 5) publier un répertoire sécurisé des clés publiques ou des certificats ; 6) gérer des objets personnalisés (par exemple, carte à mémoire) capables d'identifier l'utilisateur au moyen d'éléments d'identification qui lui sont spécifiques ou capables de créer et de garder en mémoire les clés privées d'un individu ; 7) vérifier l'identité des utilisateurs et leur offrir des services ; 8) offrir des services de non-répudiation ; 9) offrir des services d'horodatage ; 10) gérer les clés de chiffrement utilisées pour le chiffrement de confidentialité lorsque le recours à cette technique est autorisé*.».

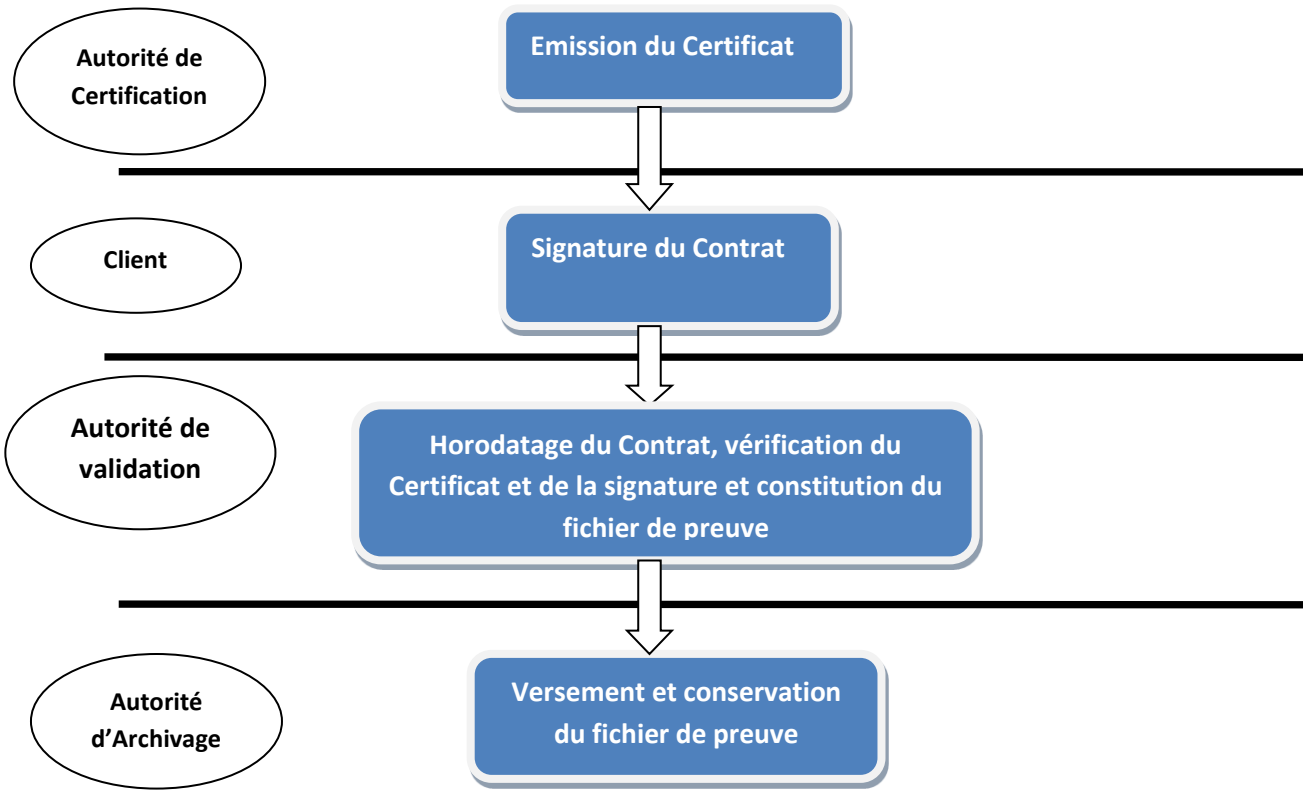
[125] CNUDCI, Doc. A/CN.9/ 493, § 51 : «*Une Infrastructure à Clé Publique s'appuie souvent sur divers niveaux d'autorité. Par exemple, les modèles envisagés dans certains pays pour établir ce type d'infrastructure se référant notamment aux niveaux suivants : 1) une autorité principale (autorité racine) unique, qui certifierait la technologie et les pratiques de toutes les parties autorisées à produire les paires de clés cryptographiques ou les certificats concernant l'utilisation de ces paires de clés, et qui enregistrerait les autorités de certification inférieures ; 2) diverses autorités de certification, situées en dessous de l'autorité racine, qui certifieraient que la clé publique d'un utilisateur correspond effectivement à sa clé privée ; et 3) diverses autorités locales d'enregistrement, placées en dessous des autorités de certification et chargées, d'une part, de recevoir les demandes de paires de clés cryptographiques ou de certificats relatifs à l'utilisation de ces paires de clés adressées par des utilisateurs et, d'autre part, d'exiger une preuve d'identification et de vérifier l'identité des utilisateurs éventuels*.»

A côté des utilisateurs (titulaires d'un certificat et parties qui se fient au certificat/destinataires), la question de la responsabilité reste une tâche délicate pour le titulaire ou pour la partie qui se fie au certificat (celle qui procède à la vérification de la signature à l'aide du certificat), victime d'une défaillance du certificat. L'identification de l'auteur de la faute est d'autant plus malaisée en raison du nombre d'entités nécessaires à l'émission et la gestion du certificat. Toutes les composantes permettant d'assurer le bon déroulement des étapes du processus de certification peuvent commettre des fautes, comme l'Autorité d'Enregistrement (A.E.) ou l'AE déléguée (bureau d'enregistrement), l'Opérateur de Certification ou l'Autorité de Certification. Mais d'autres composantes peuvent intervenir dans des systèmes plus complexes : autorité d'horodatage, opérateur d'horodatage, autorité de validation, service d'annuaires et de liste de révocation des certificats, service de recouvrement de clés de chiffrement, autorité d'archivage[126].

A titre d'exemple, on citera la question des validations de signature électronique qui se manifestent en pratique au travers d'un service qui respecte une politique de signature et une politique de validation. Quelle sera la valeur juridique de ces opérations de vérification techniques qui emporteront des effets juridiques ? Quelle sera la responsabilité de l'Autorité de validation si la signature « validée » est contestée ultérieurement ?

Si l'on se trouve en présence de certificats « éphémères », pour la preuve du contrat signé électroniquement, il faudra tenir compte de la Politique de Gestion de preuve. Qui assurera cette responsabilité ? Est-ce que cette entité sera assujettie à une obligation de moyen ou à une obligation de résultat ? Quel partage de responsabilité avec l'autorité d'archivage auprès de qui sera versé le fichier de preuve ?

[126] Comment assurer et garantir la conservation des signatures associées à des contrats ou documents dans le temps ? Ou encore, comment assurer la conservation des preuves d'authentification dans le cadre de la traçabilité des opérations ?



Exemple de processus de gestion de la preuve

En raison du caractère plural des intervenants, il est nécessaire qu'une seule entité – le plus souvent, l'Autorité de Certification – réponde des dommages causés aux titulaires ou parties qui se fient pouvant résulter d'une mauvaise exécution ou d'une inexécution fautive, à charge pour cette entité de prévoir contractuellement les répartitions des obligations et responsabilités des entités au sein de l'Infrastructure à Clé Publique. En effet, les relations existant entre chacune des composantes de l'I.C.P. – surtout lorsque les composantes sont indépendantes juridiquement – doivent être clairement précisées dans les contrats, reprenant notamment certaines dispositions de la Politique de Certification et de la (ou des) Déclarations des Pratiques de certification (DPC). La Politique de certification définit et précise les rôles et les obligations de chacune des composantes de l'I.C.P. ; elle est publique et accessible contrairement aux Déclarations des Pratiques de certification.

Il faut cependant, à ce stade, préciser qu'il n'est fait état que des relations entre une Autorité de certification et des utilisateurs et non pas de la relation entre une Autorité de certification Racine (ACR) et des Autorités de certification (AC) dont elle signe les certificats. Dans la seconde hypothèse, les responsabilités et les engagements souscrits (qui figurent dans la Politique de certification racine et le contrat) sont sensiblement différents de ceux de la première (entre l'AC et les utilisateurs).

B. Organisation juridique de la gestion des identités numériques

Parmi les éléments fondamentaux de la gestion des identités, nous retiendrons les trois solutions qui nous paraissent les plus adaptées parmi les solutions qui existent. Ces solutions procèdent de logiques différentes : la reconnaissance mutuelle transnationale des moyens d'identification, d'authentification et de signature (1), les fédérations d'identité sur la base d'un encadrement contractuel (2) et les systèmes de labellisation qui peuvent fournir des éléments de solutions dans des environnements de confiance, bâtis autour de référentiels techniques et sécurité (3). La C.N.U.DC.I. peut contribuer, selon la volonté des Etats membres, dans chacune de ces voies, en formalisant et en encourageant les bonnes pratiques en ce domaine, mais également en prenant des dispositions plus fermes pour des reconnaissance mutuelles sur la base de standards reconnus au niveau international.

1. Reconnaissance mutuelle

Pour assurer une coopération internationale et donc un véritable développement du commerce électronique, la reconnaissance mutuelle des signatures et certificats électroniques par différents pays doit être garantie. Celle-ci peut être réalisée, de manière générale, par la signature d'accords bilatéraux ou multilatéraux donc l'élément clef réside dans les considérations relatives aux mesures de sécurité (par exemple le niveau de sécurité qui peut être nécessaire), à la sécurité du stockage des données, aux critères d'acceptation des certifications transfrontières s'il y a lieu, etc.

Dans le cadre européen, on remarquera que les dispositions portent uniquement sur le certificat[127], car l'article 5-2 de la directive 1999/93/CE - s'appliquant aux autres signatures électroniques qui ne correspondent pas aux critères de la Signature électronique avancée - énonce un principe de non-discrimination : « *Les Etats membres doivent veiller à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées au seul motif que la signature se présente sous une forme électronique ou qu'elle ne repose pas sur un certificat qualifié, ou qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature* ». L'utilisation de ces procédés de signatures électroniques implique que l'on apporte, au juge, la preuve de leur fiabilité technique. Pour le certificat qui est « *une attestation électronique qui lie les données afférentes à la vérification de signature (la clé publique) à une personne et confirme l'identité de cette personne* », en revanche, la situation est différente pour les prestataires de services de certification établis en dehors de la Communauté européenne, car si ce sont des données électroniques qui sont amenées à circuler et à être utilisées dans le marché intérieur de l'Union européenne, elles doivent respecter les exigences des annexes I et II de la directive pour être reconnues équivalente aux certificats qualifiés délivrés par un prestataire établi dans la communauté.

Un rapport sur la mise en œuvre de la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques établi le 15 mars 2006 a permis pour la première fois d'analyser la mise en œuvre par les Etats Membres des dispositions de ce texte afin de

[127] V. Eric Caprioli, *La directive européenne n°1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques*, Gaz. Pal. 29-31 octobre 2000, p. 5 et s.

vérifier si un de ses objectifs premiers a pu être réalisé, à savoir l'élimination du risque de fragmentation que faisait peser, sur le marché intérieur des produits et services liés à la signature électronique, l'adoption par les Etats membres, de législations nationales divergentes[128]. Ainsi, la Commission a pu constater que les lenteurs de déploiement de la signature électronique dans les Etats membres ont un effet négatif sur les échanges commerciaux de biens et de services via l'Internet. En pratique, les entreprises et les citoyens de l'Union européenne ne disposent toujours pas d'un certificat électronique unique pour signer électroniquement des documents de la même façon que les documents manuscrits. Par conséquent, la Commission préconise la promotion de l'interopérabilité et de l'utilisation transfrontalière des signatures électroniques, à travers la poursuite des travaux de normalisation et l'utilisation de toutes sortes de technologies pour les signatures électroniques dans le marché intérieur.

Selon l'article 12 de la loi-type de la CNUDCI sur les signatures électroniques : « *1. Pour déterminer si, ou dans quelle mesure, un certificat ou une signature électronique produit légalement ses effets, il n'est pas tenu compte : a) Du lieu dans lequel le certificat est émis ou la signature électronique créée ou utilisée ; ou b) Du lieu dans lequel l'émetteur ou le signataire a son établissement. 2. Un certificat émis en dehors de [l'Etat adoptant] a les mêmes effets juridiques dans [l'Etat adoptant] qu'un certificat émis dans [l'Etat adoptant] à condition qu'il offre un niveau de fiabilité substantiellement équivalent. (…)* » Aux termes de cette brève analyse, on peut estimer que les nouvelles méthodes d'élaboration des règles internationales et européennes correspondent aux besoins du commerce électronique et expriment un savant dosage à grands traits de globalisation et de localisation[129].

Or, ces textes ne disent rien sur les effets juridiques des méthodes d'authentification, alors qu'il est opportun de favoriser l'efficacité de ces méthodes d'authentification de personnes étrangères sur le territoire d'un autre pays. Il en va de même pour les signatures électroniques émanant d'une personne étrangère. Pour ce faire, il faut reconnaître les méthodes d'authentification et de signatures électroniques étrangères. La reconnaissance transfrontière de ces méthodes reposera sur des critères techniques, organisationnels et juridiques, faute de quoi l'effectivité ne sera pas au rendez-vous. Il en résulterait une assimilation entre les méthodes d'authentification et de signature étrangères et nationales. Les méthodes étrangères bénéficieraient d'une véritable équivalence juridique. Une juridiction étatique ou arbitrale, appelée à décider de l'effet juridique d'une telle méthode, pourrait les examiner en fonction de leurs caractéristiques propres et juger de son assimilation à la méthode ayant le niveau le plus proche dans l'Etat où le moyen d'authentification est censé produire ses effets.

Afin de trouver et de mettre en place des nouvelles solutions pour éliminer les obstacles à l'interopérabilité transfrontalière des signatures électroniques qualifiées ainsi que des signatures électroniques basées sur des certificats qualifiés, la Commission Européenne a

[128] Rapport de la Commission au Parlement européen et au Conseil sur la mise en œuvre de la Directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques, COM (2006)120, 15 mars 2006, http://ec.europa.eu_society/policy/esignature/eu_legislation/legislation2.

[129] Eric A. Caprioli, *Aperçus sur le droit du commerce électronique (international)*, in *Souveraineté étatique et marchés internationaux à la fin du XXème siècle, Mélanges en l'honneur de Ph. Kahn*, Paris, éd. Litec, 2000, p. 247 et s. Eric A. Caprioli, *La loi type de la CNUDCI sur les signatures électroniques (Vienne 23 juin - 13 juillet 2001)*, Comm. Com. Electr. 2001, n°12, p.9. Thierry Piette-Coudol, *Le bilan de dix ans de signature électronique*, RLDI, Décembre 2010, p.69 et s..

décidé de mener une étude appelée « CROBIES », entre le mois d'août 2008 et juin 2010[130]. Cette initiative a permis de réaliser une analyse des exigences en matière de signature électronique dans le contexte international, avec comme référence les dispositions de la directive 1999/93/CE, les mesures nationales de sa transposition ainsi que les travaux de normalisation fondés sur ce te texte. Ainsi, CROBIES pourra contribuer aux différentes améliorations des règles applicables en matière tant juridique que technique. Parmi ses énonciations, nous retrouvons notamment une proposition d'un modèle commun de surveillance et d'accréditation des prestataires de service de certification, la création d'une « *liste de confiance* » regroupant les services de certification qualifiées, l'instauration d'une structure homogène des recommandations relatives aux dispositifs de création des signatures électroniques, l'élaboration d'une liste des algorithmes dont l'utilisation est recommandée pour les signatures électroniques etc.

Parallèlement, la Commission soutient la préparation d'une initiative sur la reconnaissance mutuelle de l'e-identification et de l'e-authentification dans le cadre d'un projet pilote STORK (Secure idenTity acrOss BoRders linKed) ayant pour objectif de faciliter l'accès aux services publics dans 18 pays européens[131].

Tous ces éléments ont conduit la Commission à vouloir remédier au manque de confiance des consommateurs et des entreprises dans les transactions en ligne. Elle a donc décidé de lancer une consultation publique auprès de ceux d'entre eux qui souhaitent apporter leur avis sur la façon dont les signatures, l'identification et l'authentification électronique peuvent contribuer à la réalisation du marché numérique unique en Europe. Les résultats de cette consultation permettront d'élaborer un nouveau cadre européen de la signature électronique, accompagnée de la révision de la directive 1999/93/CE.

Dans le cadre de ce système de « reconnaissance transfrontières», on signalera une réalisation très intéressante : le service « WebNotarius® » de Pologne. Il permet une vérification instantanée et sécurisée de différents formats de signatures électroniques ainsi que des certificats à clé publique les accompagnants. Le certificat électronique délivré suite à un tel processus de vérification est signé électroniquement et horodaté et peut donc être utilisé en tant que preuve lors d'un litige éventuel. Ce système présente des nombreux avantages, notamment le transfert de responsabilité envers l'utilisateur final du service ainsi que l'adaptabilité aux Trust-Service StatusLists (TSL, ce qui signifie la liste des autorités de certification qualifiées[132]) mis en œuvre dans les pays membres de l'Union européenne.

2. Fédération d'identités[133]

La gestion de l'identité numérique ainsi que le fait de permettre à un utilisateur d'utiliser un login unique pour accéder à différents services dans le cadre d'une fédération d'identités sont devenus des enjeux majeurs de l'économie numérique. A ce titre, il est important de signaler le consortium Liberty Alliance (disparu au profit de la «Kantara Initiative »[134]) qui a

[130] V. http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm.
[131] V. https://www.eid-stork.eu.
[132] V.http://www.webnotarius.eu/webnotariuseu/main.xml. Sur ce site, est publiée la liste de 407 Autorités de certification reconnues par ce service.
[133] V. l'article de Thomas J. Smedinghoff, *Introduction to Online Identity Management*, publié sur le site de la Conférence de la C.N.U.D.C.I : www.uncitral.org.
[134] http://kantarainitiative.org/, connue sous le nom de Liberty Alliance, http://www.projectliberty.org.

rédigé un ensemble de spécifications et de protocoles ouverts permettant de standardiser la gestion et la fédération d'identités. Ces protocoles, articulés aujourd'hui autour de SAML 2.0, permettent de mettre en place des "cercles de confiance" au sein desquels l'utilisateur ne s'identifie qu'une seule fois (au moyen d'un Single Sign On/SSO), tout en assurant la protection de sa vie privée.

Ce modèle semble actuellement l'approche la plus aboutie en terme de standardisation pour la gestion de données d'identité[135] sur l'internet[136]. Il met en œuvre des techniques d'anonymisation et de pseudonymisation et il s'appuie sur les standards les plus courants de services Web : la spécification SOAP développé par le W3C et les protocoles standardisés au sein du consortium OASIS tels que SAML. Un profil particulier LECP (Liberty-Enabled Client or Proxy) intègre un modèle de protocole de services Web visant un faible transfert de connaissance au sein d'un même cercle de confiance.

Cette architecture fait appel à un tiers de confiance qui détient pour le compte de l'utilisateur, certaines données à caractère personnel et fait un lien entre le propriétaire de ces données et un demandeur ; par exemple, un commerçant qui propose un service qui requière que l'utilisateur soit majeur pour acheter.

Ainsi, dans l'architecture Liberty Alliance, il était possible d'autoriser une personne à utiliser un ou plusieurs pseudonymes et de signer électroniquement les informations d'identité fournies par le tiers de confiance. Toutefois, autoriser un particulier à faire usage de plusieurs pseudonymes ne fait pas l'unanimité. Jusqu'à quelle limite peut-on demeurer anonyme ? A l'avenir, un cadre tel que celui proposé par le consortium Liberty Alliance, aura besoin d'être complété : des travaux sont notamment proposés pour interconnecter plusieurs cercles de confiance et permettre, par exemple, à un utilisateur reconnu par un premier cercle de confiance, d'accéder à un deuxième cercle de confiance avec le même niveau de sécurité quant à la gestion de ses données.
Les fédérations d'identités posent diverses problématiques juridiques relatives à la sécurité, la confidentialité et la protection des données personnelles (usage de l'anonymat), mais aussi à la gestion des droits et aux droits et obligations des utilisateurs.
Pour l'instant, la plupart des projets de fédérations d'identités se fondent sur une approche de nature contractuelle entre les membres. Les participants adhèrent en quelque sorte à un réseau « fermé », à l'image de ce qui existe en matière de cartes bancaires ou dans les réseaux EDI.

3. La labellisation de dispositifs de sécurité

Plusieurs initiatives gouvernementales, avec des objectifs plus ou moins étendues ont été entreprises dans certains pays afin de permettre la gestion des moyens d'authentifications et de signature électroniques. Ces labellisations peuvent procéder à partir de référentiels établis par l'Etat ou par le marché.

[135] A l'opposé de la fédération d'identité, la société Microsoft a développé un modèle propriétaire de cercle de confiance sur les réseaux, dans le cadre de son initiative Microsoft Passport.
[136] D'autres modèles existent : par exemple, en entreprise, la gestion des droits d'accès au sein de cercles de confiance repose souvent sur un annuaire conforme aux recommandations X500 ou au standard LDAP de l'IETF.

a. Le label ID Num (France)

Le gouvernement français a depuis longtemps présenté une volonté d'amorcer la transition vers la société de l'information en permettant aux citoyens de disposer de téléservices et d'un accès direct par voie électronique aux autorités administratives (administrations, collectivités territoriales, établissements publics administratifs, …). L'amélioration de la sécurité des infrastructures, des échanges et des données est un facteur clé de succès de cette transition.

Ainsi, à l'initiative du défunt Secrétariat d'Etat à l'Economie Numérique, a été lancé, le 1er février 2010, le label IDéNum. Il consiste à fédérer les outils d'authentification émis par différents acteurs, en garantissant un niveau homogène de sécurité et d'interopérabilité. Un outil labellisé pourrait ainsi donner accès à tous les services en ligne, publics ou privés, de ce niveau de sécurité, ce qui devrait créer une unification des moyens d'authentification – très diversifiés – sur le marché. Les émetteurs pourront dès lors proposer à leurs clients un nouveau service, plus utile dans la vie courante.

Ce label sera spécifié, testé et validé par les acteurs de l'économie numérique eux-mêmes et viendra compléter la liste des solutions de signature électronique déjà certifiées et régulées par le ministère de l'économie et des finances en prévoyant les produits IdéNum. Ces produits se présentent sous la forme de dispositifs physiques sécurisés dans lequel se trouvent des « *éléments propres* » au propriétaire, qui peut être peut déverrouiller au moyen d'un code PIN. Ces « *éléments propres* » sont deux bi-clés cryptographiques – l'une dédiée à l'authentification, l'autre à la signature électronique – pour lesquelles chaque clé publique a été certifiée. En tant que tel, il pourrait être constitué comme une solution provisoire dans l'attente de la Carte Nationale d'Identité Numérique.

Un produit IdéNum devrait pouvoir être obtenu auprès des prestataires de services de certification électronique (PSCE) dont l'offre IdéNum sera attestée comme étant conforme aux exigences techniques, figurant dans le cahier des charges.

Du fait de sa référence expresse au RGS[137], les produits et les téléservices référencés par l'ordonnance du 8 décembre 2005 seront automatiquement acceptés par toutes les autorités administratives qui disposent des services électroniques. Les services privés seront également autorisés à accepter les produits selon qu'ils sont référencés ou non. Le label IDéNum s'affichera sur les sites qui le reconnaissent et les internautes pourront choisir librement leur fournisseur. Ainsi, le label permettra de fournir aux internautes un moyen fiable d'identification pour simplifier leurs démarches en ligne (accès à leurs comptes administratifs, abonnement à des services payants, souscription de services ou de

[137] Référentiel général de sécurité (RGS), rédigé par l'Agence Nationale de la Sécurité des Système d'Information (ANSSI) et par la Direction Générale de la Modernisation de l'Etat (DGME), a été pris en application de l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005; décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, JO n°0029 du 4 février 2010, p. 2072 ; arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques, JO n°0113 du 18 mai 2010, p.9152. Il définit un ensemble de règles de sécurité s'imposant aux autorités administratives dans le but de sécuriser leur système d'information dans le cadre d'échange des informations par voie électronique.

contrats…), en unifiant le marché et en facilitant les formalités quotidiennes des administrés et des citoyens. Qui plus est, le label permettra au public de bénéficier de produits d'identification et de signature électronique de qualité garantie et d'identifier facilement les services en ligne qui acceptent ces produits[138].

b. Le Label suisNum (Suisse)

La carte SuisseID a été lancée à l'initiative du Secrétariat d'Etat à l'économie en Suisse et avec un budget de 17 millions de francs suisses attribué par le Conseil fédéral au titre du développement de l'espace économique électronique. Ce dispositif a pour objectif de permettre de réaliser des opérations sécurisées sur l'Internet et les réseaux numériques. Il se décline sur plusieurs supports : carte à puce ou clé USB et constitue une combinaison de deux fonctions essentielles : l'authentification électronique (vérification de l'identité) d'une personne qui a de multiples applications : autorisation et contrôle d'accès à des contenus, à des services en ligne (bancaires), ou au SI de l'entreprise, téléservices avec une autorité administrative, …), d'une part, et la signature électronique valable juridiquement, d'autre part. Il se fonde sur les mêmes technologies qu'IDénum. Grâce à ce premier produit standardisé en Suisse destiné à servir de preuve d'identité électronique, des transactions sécurisées peuvent être conclues directement en ligne entre les particuliers et les entreprises (BtoC), entre entreprises (BtoB) et entre les citoyens et l'administration (AtoC). L'acquisition de SuisseID exige un investissement de 164 francs suisses pour trois ans de validité pour une personne privée avec 65 francs suisses remboursés dans le cadre de la subvention fédérale pour toute acquisition de cette technologie par les particuliers. Toute personne physique peut se procurer des produits labellisés SuisseID auprès d'un des fournisseurs de signatures électroniques, lesquels seront chargés de la phase de l'authentification « physique » des personnes (QuoVadis, Trustlink Suisse SA ou La Poste Suisse/SwissSign AG). Quant aux autorités administratives, elles peuvent l'obtenir auprès de l'Office fédéral de l'informatique et de la télécommunication (OFIT) en vue de son utilisation par leurs collaborateurs. Plusieurs administration cantonales et fédérales, dont Genève, se sont déjà mises à niveau et d'adaptent en ligne à cette innovation technologique. Il est par exemple déjà possible d'utiliser la SuisseID avec certains services fiscaux ou pour demander une autorisation de manifestation. Au mois de septembre 2010, 110.000 certificats électroniques labellisés SuisseID avaient été déjà commercialisés.

Le label SuisseID présente des atouts non négligeables, à savoir un niveau élevé de sécurité des transactions électroniques et un gain de temps, très appréciable dans le milieu économique. Au surplus, si les institutions, les entreprises et les particuliers optent pour ce nouveau moyen d'identification et d'authentification, l'économie nationale pourrait épargner plusieurs centaines de millions de francs. La carte SuisseID est ainsi un élément fondamental dans le développement de l'administration et du commerce électroniques.

Le système a, comme le label IDéNum, des inconvénients et des avantages : il est limité à une reconnaissance au sein d'un système juridique national, mais il harmonise les usages de la sécurité en ligne, ce qui peut être très utile dans le cadre d'une reconnaissance à un

[138] V. Fédération Nationale des Tiers de Confiance (FNTC), *Vademecum juridique de la dématérialisation des documents,* rédigé par le Cabinet d'avocats, Caprioli & Associés, 3ème éd., avril 2010, p. 42, disponible sur le site de la Fédération Nationale des Tiers de Confiance, www.fntc.org et sur le site www.caprioli-avocats.com. Une prochaine édition (4ème éd.) sera disponible en juin 2011.

niveau plus large. A tout le moins, les instruments de comparaison des niveaux de sécurité existent et ils peuvent servir en vue d'une interopérabilité entre Etats et pourquoi pas constituer les fondations de règles de reconnaissance véritablement transnationales des méthodes d'authentification et de signature électronique.

c. Autres initiatives

Le label IDéNum et le label SuisNum s'inspirent de différentes initiatives entreprises dans d'autres pays européens. Ainsi, en Italie, des certificats sur des cartes à puce sont proposés au niveau régional. En Autriche, les certificats sont intégrés dans des cartes d'étudiants ; en Norvège sur des cartes de la loterie nationale ; en Suède sur des cartes remises à La Poste. En Turquie et dans des pays nordiques, les certificats sont transférables sur les téléphones mobiles.
Aux Etats-Unis, plusieurs acteurs majeurs de l'Internet (Google, Paypal, Verisign etc.), ont annoncé la formation de l'association **Open Identity Exchange** (OIX), qui vise à distribuer des certificats aux internautes. Plusieurs niveaux de confiance sont envisagés, dont le niveau supérieur peut être comparé à celui du label IDéNum. Ces certificats seront utilisables aussi bien dans le secteur public que dans le secteur privé.

Si l'analyse développée ci-dessus ne préjuge en rien de la forme que pourraient prendre les travaux de la C.N.U.D.C.I. sur les méthodes d'authentification et de signature électronique, en revanche, elle est de nature à identifier certains obstacles ou carences juridiques de nature à réduire la confiance dans les communications électroniques internationales et de proposer certains sujets à traiter. L'absence de confiance ne peut que freiner, voire restreindre le développement de ces moyens de sécurisation des communications électroniques à l'échelle internationale.

Selon René-Jean Dupuy, « *l'engagement dans l'universel consécutif à l'entrée dans l'ère informationnelle ne peut occulter les composantes nationales, économiques, financières culturelles d'un univers interconnecté. Ce n'est point le chaos : c'est la gestion d'un ordre à partir d'un désordre. On pense à Teilhard de Chardin : « Nous croyons traverser un orage ; en réalité nous changeons de climat.* [139]». Gageons que la C.N.U.D.C.I. contribue au « *changement climatique* » en matière de sécurité des communications électroniques internationales avec le passage de la fragmentation des souverainetés nationales à l'universel. La création d'un climat de confiance en dépend.

[139] René-Jean Dupuy, *Le dédoublement du monde*, Revue Générale de Droit International Public, 1996-2, p.321.