ARTICLE:

THE ARCHIVING OF ELECTRONIC DOCUMENTS UNDER FRENCH LAW

By **Sabine Marcellin and Pauline Ascoli**

Introduction

For various reasons including geography, weather conditions, government stability, competitive storage costs, and the availability of trained staff, France is considered by many as a prime location for the archiving of electronic documents. Part I of this article focuses on French electronic archiving legislation.[1] The authors also discuss how long electronic documents must be stored, French legal security requirements in respect of electronic documents, and the use of electronic documents as evidence before the French courts. From the point of view of a French organization, the location of branch offices, of servers and the offshoring or outsourcing of storage arrangements with foreign companies can raise many issues as to the laws applicable to its data. In Part II of this article, the authors express their thoughts on the importance of anticipating the possibility of international litigation, and emphasize that in order to minimize legal risk, the archiving of electronic documents and logs is a matter ideally addressed before the computer system design phase.

Part I French law on the storage of electronic documents

Archiving

How long electronic documents must be stored

There are many laws prescribing how long documents must be stored. The main French legal requirements are summarized as follows:

a) Commercial accounting documents and associated supporting documents: 10 years (art. L. 123-22 of the Commercial Code);

b) General statute of limitation for litigation by commercial entities against consumers: 2 years (art. 137-2 Consumer Rights Code);[2]

c) Preservation of contracts in electronic format concluded over the internet and for a sum greater than 120 euros: 10 years;[3]

d) Statute of limitation in civil matters: 5 years for personal litigation or legal action pertaining to movable property. It should be noted that the beginning of 5 year period is counted from the moment the plaintiff knew or should have been aware of the facts giving rise to the litigation (article 2224 of the French Civil Code);

e) Statute of limitation in civil matters pertaining to obligations between merchants or consumers and merchants (article L.110-4 of the Commercial Code);

f) For tax matters: 6 years (art. L.110-4 of the Manual of Tax Procedures).

When documents contain personal data,[4] the applicable regulations do not impose any specific retention period. French data protection laws focus on the careful safe-

[1] *See « Vers une politique d' archivage électronique des documents » (Steps toward a policy on electronic archiving documents), 2009, Association Forum des Compétences (forum-des-competences.org).*

[2] *Loi n° 2004-575 du 21 juin 2004 pour la Confiance dans l' économie numérique, article 134-2 du Code de la Consommation et Décret n° 2005-137 du 16 février 2005 (Law n° 2004-575 dated 21 June 2004 on the Preservation of Confidence in the Digital Economy, Article 134-2 of the Consumer Rights Code and Decree n°2005-137 dated 16 February 2005).*

[3] *Décret n° 2005-137 du 16 février 2005 pris pour l' application de l' article L134-2 du Code de la Consommation, JO n° 41 du 18 février 2005, P. 2780.(Decree n° 2005-137 dated 16 February 2005)*

[4] *That is, documents which directly or indirectly identify a physical person (first name, last name, telephone number, account number, electronic address, etc.), as set forth in Loi n°78-17 du 6 janvier 1978 relative à l' informatique aux fichiers et aux libertés (Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties) and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, OJ L 281, 23/11/1995 P. 0031 - 0050.*

keeping of personal data, but alongside this principle also stands a competing "right to be forgotten" principle which concerns the right to have documents destroyed after an appropriate length of time.[5]

Security standards

Subject to two conditions set forth in article 1316-1 of the French Civil Code, an electronic document has the same evidentiary value as a hard copy document.[6] The first condition is that the document be signed electronically in such a manner that there is clear consent of the parties to the obligations which flow from that transaction. The second is that it must be stored in conditions which secure its integrity. At issue is how to prove that the conditions which secure its integrity have been respected.[7] The general guiding principle is enshrined in article 1348 of the French Civil Code: the reproduction must be true to the original and durable. A reproduction is deemed durable if it is fully indelible (for instance, a photocopy from a photocopy machine that uses indelible ink) and from a support point of view, it cannot be modifiable (that is, a copy on a non rewritable CD or DVD).

For electronically signed documents, if a party proves that a document was secured by an electronic tamper seal, the opposing party will bear the burden of proving that the tamper seal program was unreliable if it wishes to contest the validity of the document.[8] In practice, when functioning correctly, an electronic tamper seal will invalidate an electronic signature if changes occur to it after the document was electronically signed.[9]

The right of access to archived documents

System administrators, users, internal auditors

French law contains detailed provisions on the length of time that documents must be archived. On the other hand, with the exception of personal data rights[10] and special secrecy laws, French law is fairly silent on the matter of who may obtain access to an organization's data. It is therefore for the organization to establish clear policies and procedures which address the matter of who may obtain access to archives documents, for what purposes and under what conditions. Typically, IT administrators are given rights to obtain access to manage and maintain the system. Internal auditors are granted rights to obtain access to be informed of the existence of documents and logs. Legal and compliance officers are granted rights to obtain access in the context of litigation or justifiable investigations. As a matter of law,[11] persons identified in the documents enjoy a right of access, correction and contestation.

Administrative authorities

In addition to the permissible consultations outlined above, certain administrative and judicial procedures in France result in the granting of permission to certain authorities to obtain access to archived documents. Below is a list of some of the authorities to be considered in the development of an organization's archiving policy.

a) La Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF) is the French agency in charge of protecting fair trade and competition. It may request, in the context of a simple inquiry, the disclosure of accounting and other professional documents.[12] The DGCCRF is entitled to copy corporate documents and to obtain access to them in situ. In the case of a complex inquiry, officials may seize documents relevant to the inquiry. Where product and service compliance is at issue, agents may take copies.[13]

b) The Haute Autorité de Lutte contre les Discriminations et pour l'Egalité (HALDE), the French anti-discrimination authority may request[14] disclosure of any document stored electronically or otherwise, in the context of an inquiry. Where the

[5] *Article 6-5 Loi n° 78-17 relative à l' informatique, aux fichiers et aux libertés (Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties).*

[6] *For an outline of the position on electronic evidence in France generally, see David Benichou and Ariane Zimra, ' France' in Stephen Mason, gen ed, International Electronic Evidence (British Institute of International and Comparative Law, 2008) pp 303 – 326.*

[7] *Stephen Mason, gen ed, Electronic Evidence, (2nd edn, LexisNexis Butterworths, 2010) Chapter 4 for an in-depth discussion of this topic.*

[8] *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 (Decree n°2002-272 dated 30 March 2001 on electronic signatures).*

[9] *It is notable that the United Nations Convention for the Use of Electronic Communications in Electronic Contracts, ratified as of November 2005, indicates in article 5 (b) that "The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances". France is not a signatory of the Convention.*

[10] *Articles 38 à 40 de la Loi n°78-17 du 6 janvier 1978 relative à l' informatique aux fichiers et aux libertés (Article 38 to 40 of Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties).*

[11] *Articles 39 and 40 of Loi n° 78-17 du 6 janvier 1978 relative à l' informatique, aux fichiers et aux libertés (Articles 39 and 40 of the Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties).*

[12] *Art. L 450 Code de commerce (Article L 450 Commercial Code.)*

[13] *Art. L 217-10 Code de la consommation (Article L 217-10 Consumer Rights Code).*

[14] *Loi n°2004-1486 du 30 décembre 2004 portant création de la Haute Autorité de Lutte contre les Discriminations et pour l' Egalité (Act n° 2004-1486 of the Act on the creation of the Equal Opportunity and Anti-Discrimination Commission)*

entity refuses to cooperate, the HALDE may bring the matter before a judge on a fast-track basis.

c) The Autorité des Marchés Financiers (AMF), the French Securities and Markets regulator, may request[15] a copy of all documents stored electronically or otherwise which are necessary for an investigation. The Autorité de Contrôle Prudentiel, the French banking regulator has similar powers.[16]

d) The Commission Nationale de l'Informatique et des Libertés (CNIL), the French privacy rights authority, may also access corporate offices and demand[17] a copy of all relevant document in the context of an investigation.

e) L'Administration des Douanes (ADD) the French customs administration has the right to conduct on-site visits anywhere in France and obtain copies of documents or seize relevant information.

f) The French Tax Department is granted the right[18] to receive communication of all accounting documents, regardless of their format. Where a presumption of fraud applies and a judge has issued a search warrant, documents held in any format can be seized anywhere in France.

Judicial authorities

As a general matter, the French courts have the power to issue orders pertaining to obtaining access to documents held or archived by business organizations. Information archived within France can also be the subject of demands by foreign courts and authorities, as discussed in Part II.

Criminal proceedings

The courts can order an inquiry (*enquête de flagrance*[19]) in respect of any person who may be in a position to establish the truth about a crime or misdemeanor committed within the last 8 days or in the process of being committed. A search warrant is carried out by a police officer without the consent of the persons concerned, (subject to certain constitutional, legal or privilege limitations) and he or she has the right to demand copies of relevant documents.

A preliminary hearing[20] is a process by which a judge can allow the police to gather evidence before charges are filed. Persons named in the order can be compelled to provide documents to the police, upon request. Documents in respect of which professional secrecy obligations apply cannot be requested by the police without prior authorization[21] from the prosecutor's office.

The criminal courts can establish rogatory commissions[22] for the purpose of delegating to a particular judge or police officer the power to gather or obtain evidence by way of hearings, searches and seizures. The judge or police officer has the power to compel the production of archived documents.

Pursuant to article 60-2 of the Code of Penal Procedure, a judge can make an order requiring certain telecommunications or other companies listed in article 6 of Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (Law 2004-575 enacted 21 June 2004 on the Confidence in the Digital Economy) to provide information electronically. This procedure is often used where a large volume of information is at issue.

Civil proceedings

There are many cases where parties can be compelled to produce archived documents in the civil context. For example, in France it is common practice to obtain evidence in an intellectual property case by way of seizure of evidence of infringement or *saisie-contrefaçon*.[23] A party alleging infringement can request that a bailiff be appointed to seize archived information contained, for example, on a server or database. The opponent is not informed of the motion and not provided with the opportunity to contest it to avoid the possibility of destruction of evidence.

[15] *Art. L 621-9-3 Code monétaire et financier (Article L 621-9-3 Monetary and Financial Code).*
[16] *Art. L 511-33 Code monétaire et financier (Article L 511-33 Monetary and Financial Code).*
[17] *Art. 11-2 de la Loi n° 78-17 relative à l' informatique, aux fichiers et aux libertés et Décret n°2005-1309 du 20 octobre 2005 modifié par le décret n° 2007-451 du 25 mars 2007(Article 11-2 of Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Libertiesand Decree n° 2005-1309 of October 20, 2005 modified by Decree n° 2007-451 of March 25, 2007).*
[18] *Art. L 102 B Code de procédure fiscale (Art. L 102 B Code of Tax Law Procedure)....*
[19] *Art. 53 Code de procédure pénale (Art. 53 Code of Criminal Procedure).*
[20] *Art. 75 Code de procédure pénale (Art. 75 of the Code of Criminal Procedure).*
[21] *Art. 77-1 Code de procédure pénale (Art. 77-1 Code of Criminal Procedure).*
[22] *Art. 151 Code de procédure pénale (Art. 151 Code of Criminal Procedure).*
[23] *Art. 615-5 Code de la propriété intellectuelle (Art. 615-5 Intellectual Property Code).*

Archiving to preserve evidence

Proof of the existence of a binding document

Under French law, an electronic document is of equal value to a hard copy document since the enactment of legislation on 13 March 2000 (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). The law modified article 1316 of the French Civil Code by giving a new definition of written evidence:

> La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.
>
> Documentary evidence, or evidence in writing, results from a sequence of letters, characters, figures or of any other signs or symbols having an intelligible meaning, whatever their medium and the ways and means of their transmission may be.

Subject to two conditions, an electronic document has the same evidentiary value as a hard copy document. The first condition is that the electronic document be signed electronically in such a manner that there is clear consent of the parties to the obligations which flow from that transaction. The second is that it must be stored in conditions which secure its integrity.

As set forth in 1316-1 of the French Civil Code, for an electronic signature to be valid, the use of a reliable identification process that guarantees identification to a particular document is required. In practice, this means the use of public and private keys and electronic certificates as contemplated by Decree.[24] Article 1316-4 of the French Civil Code establishes a presumption in respect of the validity of an electronic signature once the identity of the signer and the integrity of the document have been proved.

Certain documents must be paper-based where the law sets forth the admissibility of the document by the person adducing the document as evidence. This is the case, for example, for certain acts that require a manuscript signature addressing family law matters, wills and successions and documents pertaining to personal or real property.

There are several exceptions to the rule that a paper-based or signed document must be produced to prove the existence of a binding contract. For example, a copy can be produced where it is impossible to obtain the original or where force majeure exists. A reliable copy (art. 1348 subparagraph 2 of the French Civil Code) can also be acceptable. The courts have ruled that photocopies and facsimile transmissions were deemed reliable and durable.[25]

Proving a fact

In French civil law, a legal act (*acte juridique*) is a documentary expression of intention. A classic example would be a contract. A legal fact (*fait juridique*) on the other hand, is an event which may have legal repercussions. For example, the fact that someone sent a defamatory e-mail would be a legal fact. Article 1348 allows a party to adduce imperfect evidence such as testimony, presumptions, and unsigned documents to prove a legal fact. Another reason an organization may wish to archive information is for the ability to prove a legal fact at a later date, in the context of a trial, a regulatory investigation or otherwise.

Under French Law, a litigant may resort to perfect or imperfect evidence in order to prove a legal fact. Perfect evidence includes literal evidence which includes notarized documents, acts under private signature, and admissions made in court. Imperfect evidence includes unsigned documents (such as e-mails), testimony, presumptions, out-of-court admissions, and commencement of proof in writing. The proper archiving of documents will help an organization to prove legal facts by means of imperfect evidence.

Part II Minimizing legal risks associated with the storage of electronic documents

International litigation

An organization should make a careful assessment of the risk of international litigation, given the nature of its activities or services or the location of its branch offices. In the area of consumer or employee rights, it sometimes takes very little for a court to be able to

[24] *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 (Decree n° 2001-272 dated 30 March 2001 related to electronic signature).*

[25] *For photocopies, see Cass. 1ère Civ., 30 juin 1993, n° 89-21, Gaz. Pal.; for facsimile transmissions, see Cass.Com., 2 décembre 1997, JCP G 1998, II, n° 10097.*

accept jurisdiction in respect of a claim.

French civil procedure does not provide for pre-trial discovery or disclosure. Nevertheless, an organization established in France should consider the possibility of being compelled to produce documents in the context of international litigation. It should anticipate that if a claim is filed in a jurisdiction with pre-trial discovery or disclosure rules, it may be required to communicate written evidence to the opposing party prior to the trial. As for the documents that have to be retained for a set period of time by French law (as discussed above), the opposing party is likely to invoke French legal archiving provisions, which require the retention of certain documents. In the case of e-mails exchanged in the ordinary course of business, an organization should decide beforehand and as a matter of policy whether there is more risk in retaining or destroying old e-mails and ensure that its processes are in line with this policy. Destruction of evidence after it is requested by a foreign court can give rise to heavy sanctions or penalties as well as cause reputational damage.

Some organizations established in France tend to consider the French blocking statute[26] as an international litigation 'shield' which protects them from compliance with overseas pre-trial discovery or disclosure requirements. Subject to international treaties, the French blocking statute does prohibit communication of commercial, financial, economic or technical documents where disclosure would constitute a threat to France's essential economic interests, or for the purpose of constituting evidence in foreign judicial or administrative proceedings. However, many documents fall outside the ambit of these criteria. Violations of the statute are punishable by up to 6 months in prison and a maximum fine of 18,000 euros. On 12 December 2007, the Cour de Cassation convicted a French lawyer under the statute.[27] He was found guilty of attempting to obtain information of an economic nature for use in a United States trial, without recourse to the procedures under the Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters.

An increasing number of legal provisions authorize the communication of information to foreign public authorities. The new philosophy behind these provisions is to facilitate cooperation between supervisory authorities and for their efforts to be mutually recognized. For example in the banking sector, the Autorité de Contrôle Prudentiel has signed several conventions on the sharing of information with foreign supervisory authorities. In the area of legal procedure, the Hague Convention referenced above sets forth procedures concerning the communication of evidence for use in a foreign proceedings.

Prior to the computer system design phase

The reliable and durable archiving of an organization's data is not only a matter of using the right technology, but of integrating parameters which are consistent with applicable legal requirements. An archiving policy which complies with French law must take into consideration legal requirements on the proper conservation of documents and be consistent with the potential right of access by authorities, employees and persons whose personal data is recorded in the system. Above and beyond the legal requirements, a considerable number of choices need to be made about what data is to be retained or destroyed. Both the French and international legal environments need to be considered in making these decisions. They are best made at the system design phase, because it is often difficult to change system functionalities at a later date.

The Systems Development Life Cycle (as defined in Systems Development Life Cycle Guidance Document (Department of Justice, January 2003))[28] is a classical systems design model used internationally. It can be broken down into ten steps, some of which can be eliminated depending on the complexity to the project. The steps are: 1. Initiation; 2. System Concept Development (risk management plan, feasibility study, systems boundaries, etc.); 3. Planning; 4. Requirements Analysis (develops user requirements); 5. Design; 6. Developments; 7. Integration and Testing; 8. Implementation; 9. Operations and Maintenance (post implementation reviews), and 10. Disposition.

Ideally, legal analysis is performed at stages 2 and 4. At stage 2 counsel can, for example provide advice on: the legal risks associated with locating servers in one jurisdiction versus another; back-ups and business contingency planning; the legal implications of server virtualization and cloud computing; legal requirements for contracts whereby storage functions are outsourced

[26] *Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères (Act No. 68-678 of 26 July 1968 concerning the disclosure of documents and information of an economic, commercial, industrial, financial or technical nature to individuals or legal entities).*

[27] *C. Cass. Crim., 12 décembre 2007, n° 07-83228, Christopher X (for a translation of this case into English, see pp 130-133).*

[28] *Available at http://www.justice.gov/jmd/irm/lifecycle/table.htm; note also the further references to international approaches and the international research efforts in this area in Stephen Mason, gen ed, Electronic Evidence, (2nd edn, LexisNexis Butterworths, 2010) Chapter 4.*

domestically or internationally (offshoring); and applicable privacy legislation and other legislation on the security and safekeeping and storing of information. At stage 4, counsel can, for example, provide advice on: how long e-mails should be retained; when e-mails can be permanently deleted and the potential risks or benefits in archiving them; access policies in respect of archives; access policies in respect of e-mails; archiving of logs; other functionalities which will be tailored in accordance with the organization's views on the associated legal risks.

As any legal reader will be aware, competent legal advice in connection with data archiving can go a long way in minimizing an organization's exposure to regulatory sanctions and litigation. Shortcuts and failure to consider relevant legal issues can unfortunately, prove very costly to an organization.

Sabine Marcellin, French legal counsel, is also co director, with Lionel Costes, of the annual 'Guide Lamy Droit de l'informatique et des réseaux' (Sa Lamy, 2010).

Pauline Ascoli, lawyer, is a Member of the California Bar and the Quebec Bar.