

PERMANENCE AND CONSERVATION OF CIVIL-STATUS RECORDS

Françoise BANAT-BERGER
Management, Archives of the French Republic

Context: authentic electronic documents and archiving

The question of the permanent storage of registers was brought up during Parliamentary discussions regarding the vote of bill n° 2000-230 of 13th March 2000, on the adaptation of the law of evidence law to information technologies, relative to electronic signatures¹. The principle of this proposed law was to grant the same probative value to electronic records as is granted to paper records, as long as the identity of the records' authors is assured and that the records are drafted and conserved in such a manner as to guarantee their integrity². However, beyond this important innovation, an amendment was introduced aiming to allow authentic electronic records to also be drafted electronically³. This concerns the records with the greatest probative value in French law⁴. It is noticeable, in this regard, that electronic signatures have been imbued with a particular importance, since it is currently the signature that determines a record's authenticity. Concerning these records, an order was to be drafted with the aim of more precisely defining the conditions wherein the authenticity and permanence of electronic records would be guaranteed.

The question of storage is being considered, as parliamentarians are conscious that, when they speak of authentic records, these must be conserved over a long period of time. In effect, they would need to be conserved for an unlimited time, which would be the responsibility of County archiving departments.

Thus, it was possible to hear M. Vaillant, then Minister for Parliamentary Relations, recognise that *'Current techniques allow us to guarantee the storage of information for a limited time only, due to their rapid obsolescence. It is certainly possible to transfer information from one support to another as the technology evolves, but this would have to be done in secure conditions. The technical conditions for the computerisation of authentic records are not in place.'* And that *'in general, the Government accepts the idea of including the computerisation of records within the Civil Code, while postponing the question of the material conditions needed to carry this out'*.

In spite of this warning, two orders were rapidly drafted regarding notaries' and bailiffs' records. However, it was then necessary to wait several years (August 2005) for these texts to be published⁵, notably due to problems surrounding permanent storage: on the one hand, the problems surrounding the transfer from one format to another, and on the other hand, the long-term maintenance of electronic signatures, and finally, more generally, the complexity and cost of electronic storage in the long term⁶.

1. For more information, see the following article : BLANCHETTE, Jean-François and Françoise BANAT-BERGER. 2006. The 'dematerialisation' of authentic documents in French law. *Gazette des Archives, Association des archivistes français, n°204*.

2. ..."*subject to due identification of the person it originates from and to it being drafted and stored in conditions guaranteeing its integrity.*" (CC, art.1316-1)

3. *'It may be drafted electronically if it is established and stored in conditions decided by the State Council order'* (CC, art.1317)

4. Bailiffs' and notaries' minutes, Court minutes, and civil-status records.

5. Orders n° 2005-972 and 973 of 10th August 2005, respectively relating to notaries' and bailiffs' authentic documents.

6. It was necessary to wait a few more years for the notaries' central minute-record to be inaugurated on 28 October 2008, and

Several responses to those problems are provided in these orders, which, thus, take into account the notion of 'metadata', that is the recording and traceability of descriptive and structural elements, but also management and techniques, which allow the retrieval, identification, and easy characterisation of records. Similarly, the complexity of electronic archiving justified the choice to install a central minute-record classified by profession, notaries and bailiffs transmitting the quickly-elaborated records after they have been produced, and entrusting their storage to this central structure.

Finally, for the first time, the contradiction was mentioned between, on the one hand, maintaining the integrity of records in the technical sense (bit by bit), and on the other hand, maintaining the legibility of records in the medium and long term, which, among other things, implies proceeding with format changes which modify the record itself and, consequently, invalidate the signature-checking process (since the bit-by-bit integrity can no longer be ensured)⁷. This unsolvable contradiction, as soon as the legal security of a record depends on a technological process, has been kept at arm's length in the orders, by a legal countermeasure aiming to posit the fact that the necessary migrations for ensuring the legibility of the record do not alter the record's status as an original.

Civil-status records and their archiving

The current situation

Concerning civil-status records, keeping an original paper record is currently still mandatory⁸. However, since 1989, the copies left with the Court registry have not been kept up to date.

Over the last few years, we have seen a centralisation of new birth records, with 90% of the traffic being handled by just over 700 town halls, as well as massive use, since 1998, of civil-status software, with over 7000 town halls now computerised, including all towns over 8000 inhabitants. In numerous cases, also, paper registers still kept in town halls have been partially or totally integrated into the database (either as an image after computerisation, or after being re-entered in text form). However, the digital register has no probative value, this being the sole preserve of paper registers.

This is how, in computerised town halls, records are drafted and updated in digital form, whereas paper registers are printed out from the software, the civil registrar signing by hand each document thus produced. Council paper records are manipulated insofar as updates must be reproduced on paper and signed by hand as well. Only the central civil-status department in Nantes⁹ now only updates its digital record, but, and we will come back to this, the Nantes department is centralised. Information exchanges between town halls, other town halls and notaries are always by post, except for a few experiments with electronic transmission¹⁰.

Consequently, the system is relatively encumbered, especially given the significant increase in the number of marginal annotations, due to people's increasing familial mobility. Keeping both paper and digital registers, consequently, is often a complex process, and can cause divergences when keeping both types of register updated. Similarly, exchanges of information, due to geographical dispersal of records, are becoming more and more frequent, which increases the expense incurred by traditional postal exchanges.

immediately closed again awaiting its effective implementation.

7. See BLANCHETTE, Jean-François and Anne CANTEAUT. 2007. Integrity, signature and archiving process. In *La sécurité aujourd'hui dans la société de l'information*, edited by Stéphanie Lacour. L'Harmattan.

8. Order n° 62-921 of 3 August 1962 modifying certain rules relating to civil-status records

9. For foreign-born French nationals.

10. For example, the department of Deux-Sèvres is driving the dematerialization of requests for the validation of civil-status information between social organisations and institutions. A bill also concerns the dematerialization of transmissions between the Nantes civil-status department and its partners (professionals : notaries, retirement funds...), councils.

The dematerialisation of records using electronic-signature tools seems inevitable, and seems conducive to greater efficiency and simplicity, following the example of notaries and bailiffs. Then again, things are not that simple.

Towards dematerialisation?

First of all, some thought was given to constituting a national civil-status register, as was already decided for notaries and bailiffs, and has already been implemented in other countries such as Switzerland or Scotland. The advantages of a reliable service, particularly for updates, which can ensure reliable technical security while sharing the costs of digital storage in the long term, are self-evident. This being said, for now, the hypothesis has been abandoned for several reasons: cost reasons¹¹, of course, with questions regarding which organisation would take on the mission, uncertainties on the technical and legal environment, with legitimate questions from the point of view of the laws surrounding personal data which would be sure to be raised by the creation of a 'central population register'. Finally, the symbolic aspect of the change is extremely important, with the feeling of aimlessness that towns might feel regarding their traditional roles.

Another solution was then suggested: to give probative value to the digital register and demand that only one paper register be kept, which would not be updated. Several scenarios are possible, according to whether the council is computerised or not: paper register and digital register in one case¹²; digital register with implementation of electronic signatures and paper register in the second case. Only digital copies would be kept by the Court registry. This is, in appearance, a simple and pragmatic solution¹³, although it does not take into account the issue of permanent storage. However, basic questions have not been touched upon. For instance, concerning the digital copy of an original record in a non-computerized town hall: how will it be possible, with an electronic Document Managing System (DMS), without a business application, to manage the updating of scanned records at any given date?

Questions relating to electronic signatures

Furthermore, concerning records drafted in digital form with an electronic signature, what about the signatures on the updates? What about long-term technical signature-checking, once the records have expired (after a maximum duration of three years)?

This requires a short explanation of the technology employed for electronic signatures, as it is defined by order n° 2001-272 of 30 March 2001, in application of the law of 13 March 2000.

- The technology of the electronic signature

The system is based on three elements: the generation of a digest¹⁴, the signature of the digest with a private (secret) key, and the establishment of a link between the private key and its owner. The digest, of generally fixed size, is generated from the document whose integrity is being proved, thanks to a mathematical function called a hash function. This function restores a digest which is inseparable from the document it is extracted from, and of a fixed length. The digest is transmitted with the document and, when it arrives, using the same function, the system fetches a digest of the received document and compares both digests. If the results are identical, this means that there is a very high probability that the document was not altered during transmission.

11. Countries implementing centralised storage of civil-status documents are smaller countries, who, in certain cases, have based their systems on a tradition of centralisation that has existed for centuries, and in other cases do not have the same rules as France, particularly regarding updating.

12. With no electronic signature in this case.

¹³ With obvious savings as regards storing the registry's collection of paper

14. The hash-function is the function allowing the calculation of the digest.

However, during transmission, the document and its digest could have been stolen and replaced with another document, with its own digest. This is why the initial digest is signed using its author's private (secret) key, and the digest generated on arrival is checked with the public key corresponding to the private key, which is to be communicated to anyone who wishes to check the signature. This means that if the digest makes it possible to check that a document has not been altered, the signature also makes it possible to certify the origin of the document. In this case, it is appropriate to speak of 'non-repudiation': it is impossible for the author not to acknowledge his authorship of the document, as the public key can positively verify only what has been signed by the corresponding private key.

Finally, there remains to establish the link between the private key and its owner. This is where certification contractors intervene, with whom the public key will be registered. In this way, a third party (the contractor) acts as guarantor that the public key is really yours, and thus, creates a link between the public key and your identity. The registration is made in a certificate containing a certain amount of variable information according to security levels: proprietor identity, quality, public key, etc.

Two very important elements are, on the one hand, the duration of the certificate's validity (usually between one and three years) and, on the other hand, the transactions that are allowed for this certificate. Naturally, the certificate is also signed, using the contractor's private key.

This relatively complex system implies building an infrastructure, and you can see that checking a signature implies storage, not only of the document itself, but also of the signature algorithms used when the document was signed, and the certificates (only the one that was valid when the document was signed may be used).

- The long-term maintenance of electronic signatures

Under these conditions, how is it possible to maintain, in the long term, the possibility to check the electronic signature, without which checking the whole system cannot work, since the authenticity of the entire record rests on this signature?

Must we resign ourselves to the expiration of certificates' life spans¹⁵, all records for each certificate server, for a number that will only increase from year to year? The cost and the inconvenience of this solution are self-evident. Would it not be preferable to have a legal adaptation, allowing for escape from this encumbrance, for instance by imagining you could produce an attestation while carrying out the "original" checking of the record to make sure that such a signature, relating to a given record, was valid at such and such a date and that following this the maintenance of its integrity is dependent on the archiving process?

Questions relating to record-encoding formats

The format may be defined as being the entirety of the logical information organisation characteristics; this is what we call the data format, the file format, or the information representation format. However, there are several manners of representing the information in binary form. Bit streams, even grouped into binary words, have no significance for a human being. The translation of binary words into comprehensible information is carried out by computer programmes, also referred to as software. There exists an almost innumerable quantity, each filling different functions at different levels. These programmes must also be equipped with a complete knowledge of the way information is organised within a binary structure.

In their daily work, agents use text (or office) formats (Office suite formats, Open Office suite

15. At most every three years.

formats, text formats...), and also image formats.

The intrinsic difficulty is that, today, many agents work with formats that are said to be 'closed', which means that their specifications are not public. For instance, if a record was produced in Word 97 format, the possibility of opening it is tied to the Microsoft software which allows its interpretation, and to the adequate operating system (Windows XP, or Vista). Today, if an agent is working with Office 2007, he will no longer be able to open Word 97 files, and will not have access to the specifications of the software allowing him to read the files thus produced. The compatibility chain has been broken in less than ten years. Generally, software designers will allow for backwards compatibility between, for instance, version N and version N+1, but this will not carry through to the next version.

In contrast, formats published by Adobe¹⁶ are proprietary in that they belong to the Adobe Company, which may, of course, change its commercial policy. However, this company has always chosen to publish the specifications of its formats, which means that, when you wish to open a file from an old PDF version, it will always be possible to write a programme allowing the correct interpretation of this file from the specifications of the old format, which are publically available.

It is consequently essential, for documents that you wish to keep in the medium and long term, to choose open formats, whose documentation is complete and accessible to all, which are if possible compliant with standards or specifications¹⁷. These formats must, as much as possible, be independent from other formats, platforms (operating systems), and in economic terms (development costs for reasonable manipulation tools). Simple formats are preferable to complex formats.

If, right from the moment the civil-status records are produced, the formats used do not follow these criteria, the transfer to permanent formats will have to be implemented as soon as possible, which, of course, will invalidate the electronic signature checking processes. If, right from the start, permanent formats have been chosen, these transfers will be put back to a later date, but will still have to take place in the long term. It is impossible to imagine that a format might remain stable and not evolve for several decades.

Consequently, it will be necessary to anticipate this, in order to ensure the legal value of records thus transferred. The orders concerning notaries and bailiffs have allowed the transfers necessary to the legibility of records not to rob those records of the qualities of the original. More generally, this vision is close to the recommendation of 1 December 2005 of the Internet Rights forum (FDI)¹⁸ relating to digital storage. In fact, the recommendation defines what is meant by 'integrity', in order to interpret article 1316-1 of the Civil Code: this notion would, in fact, be ensured by the application of three criteria on a cumulative basis. Those are the legibility of the record, the stability of the content, and the traceability of operations carried out on the record.

Questions relating to secure storage

Generally, organisations which are considering dematerialising a process mention the gain in terms of traditional archiving space. This gain is, of course, real, but it is striking that, in parallel to this, the cost of digital storage is absolutely not evaluated, this time in terms of competencies, materials and

¹⁶ PDF formats

¹⁷ As far as office documents are concerned ODF (open document format), as used by the open office suite (ISO 26300, 2006 compliant), PDF version 1.7 which has become the ISO 32000-1, 2008 standard ; PDF/A-1 archiving format (ISO 19005-1 standard : Electronic Document file format for long-term preservation). For image formats : TIFF and JPEG formats (ISO/IEC 10918-1 standard), JPEG 2000 (ISO/IEC-15444 standard), PNG (ISO/IEC 15948,2003 standard). For languages, XML format, version 1.0, which is standardised by the W3C (World Wide Web Consortium)

¹⁸ FORUM DES DROITS SUR L'INTERNET (FDI). 2005. Electronic storage of documents. The recommendation is published at the following address : http://www.foruminternet.org/activites_evenements/lire.phtml?id=126

software.

- Archiving policy

Generally speaking, the implementation of secure archiving in the long term requires adopting an archiving policy, based on the one elaborated in 2006 by the central management of information systems security¹⁹.

Electronic archiving, the object of this archiving policy, aims to store information while restoring it entirely, in accordance with the original information. This operation of storing archives which have probative value and legal effects concerns all legal persons without exception, whether they are physical, moral, private or public.

In order to elaborate the archiving policy, it is necessary to determine first the responsibilities and obligations between the various agents, for instance between the department producing the materials, the information technology department, and the archive department. Notably, archiving authorities will be defined, as the archiving authority will be the one with the responsibility of archiving, and will be in charge of management, processing, storage, and communicating the data.

These are the minimal requirements, in legal, functional, operational, security, and technical terms, that an archiving authority must respect in order that the electronic archiving in place may be considered reliable.

- The necessity for secure storage

The securisation of storage must, of course, be ensured, whatever medium is used (online media: disks, delayed-access media: cartridges, tapes, removable optical media...). The choice will depend on needs in terms of quick access and number of consultations. But whatever choice is made, it is essential to monitor the chosen media (manually, and if possible automatically), in order to be able to carry out a migration if necessary. It will also be necessary to decide on the time frame for renewal, which will be determined by the type of media²⁰. This implies implementing procedures and having sufficient technical metadata in order to monitor representative samples, as well as sufficient knowledge of media and their quality²¹. In any case, also, it will be necessary, for obvious data security reasons²², beyond redundancy technologies, to ensure the duplication of information on two distant sites.

- The other costs involved

Beyond these costs, it will be necessary to include, as we mentioned, the costs of migrating from one medium to another (implementation of acknowledgement tools and validity of the entry and storage

19. *DIRECTION DE LA SECURITE DES SYSTEMES D'INFORMATION (DCSSI)*. 2006. Methodological tools for the security of information systems. Secure electronic storage <http://www.ssi.gouv.fr/fr/confiance/archivage.html>.

20. For example, if using tapes, decide to transfer systematically all documents after five years, and each year, unroll each tape.

21. So, for CD-R and DVD-R, two scientific studies commissioned by the management of French Archives from the National Laboratory of Computing Evaluation and Trials (LNE) allowed the definition of marks on CDs and DVDs associated to types of recorders, likely to have a real archiving function without depending on the assertions of manufacturers (Instruction DITN/RES/2005/004 of 29 March 2005 relating to recording, storage and evaluation of CD-R. Instruction DITN/RES/2006/003 of 20 December 2006 relating to the results of the study on CD-R stored by public archiving departments. Note DITN/RES/2008/012 of 19 December 2008 relating to the results of a second study on CD-R and recorders on the market, as well as a study on DVD-R and recorders on the market : <http://www.archivesdefrance.culture.gouv.fr/gerer/archives-electroniques/stockage/>

²² A research campaign carried out by Google (in fact, statistics based on continuous observation over the course of several months of 100 000 hard drives of different brands, capacities and speeds, used by Google at its headquarters in Mountain View, California) shows, on the one hand, a risk of 'sudden death' for new hard drives (breakdown rate is roughly twice as high with hard drives under three months old than it is for hard drives that are over a year old), and on the other hand, a rapidly increasing breakdown rate : over the first year of use, only 1.7% of Google's 100 000 hard drives had to be replaced, then 8% over the second year, then 8.6% over the third year... and finally, the existing alert systems are relatively inefficient : 56% of hard drives that died did so without there being any alerts. Furthermore, it would seem that hard drives become increasingly fragile, the larger their capacity).

formats, storage tools with rigorous traceability of operations and storage of original formats) ; the costs of devices relating to the securisation of stored document space (technologies relating to the generation of digests and timestamping : it must be possible to prove that such and such an operation was carried out at such and such a date, and to prove that the documents stored have retained their integrity since they were drafted) ; and the costs of transmission, for instance for final archiving in public archiving systems : data export according to the format of standard data exchange for archiving²³ to be implemented, without taking into account costs related to search and enquiry with the associated security clearances.

Conclusion

It is apparent that digital archiving involves major complexity, competencies and costs. Who, in the case of digital civil-status records, should bear these expenses, and what organisation should be put in place?

The sharing of costs is at once an obvious source of economy and security, but implies major initial costs (central service) and major legal problems. This solution has been abandoned for the present.

Therefore, if you keep the organisation currently in place, the responsibility and cost would be borne by councils and Court registries, whose agents currently have neither the profile nor the competencies for this long-term digital storage. This responsibility would then be taken over by county archiving departments after a delay which, as things look today, will last a hundred years...

The greatest danger lies in not asking these questions, and thus implementing dematerialisation without giving oneself the means to store digital data safely, either by believing that security is already ensured by electronic signature technology, which in itself is not very permanent, or else by believing that security is achieved by retaining, for instance, an original paper record that is no longer updated, while the long-term storage of digital data is not secure.

Consequently, it is not permissible to improvise, being 'content' with legal security provided by an order relating to the State's fundamental records and the law of persons. It is necessary to implement legal, technical, archive security; otherwise, we will be playing sorcerers' apprentices and will have regressed several hundred years in terms of the storage of people's civil-status records.

23. This refers to the data exchange format for archiving published in 2006 by the DAF and the Directorate General for modernisation of the State (DGME) for archive departments and their partners (notably archive producers). This format specifies the structure and content of messages produced in the framework of these transmissions, as well as the transfer slips which are transferred at the same time as the documents to be archived. The standard also defines the elimination process (printing a digital elimination slip which must then be signed by archive management https://www.ateliers.modernisation.gouv.fr/ministeres/projets_adele/a103_archivage_elect/public/standard_d_echange_d_folder_contents).