CHAPTER 5: LONG-TERM PRESERVATION

5.1 Aims

This chapter will:

- explain, in practical terms, what it means to preserve records;
- describe the various mechanisms currently used to preserve electronic records;
- outline the nature and function of metadata in the preservation process; and
- identify the skills required to preserve electronic records.

5.2 Scope

This chapter of the *Workbook* covers approaches to the long-term preservation of electronic records. Long-term is defined within the chapter as being longer than the lifetime of the system (hardware and software), which created the records – typically five years at current rates of technical change. It assumes that some means of identifying what records should be preserved is already in place. It makes no assumptions about the purpose for which records are to be preserved, or what type of access is to be provided to them.

5.3 Preservation requirements and implications

Before considering specific technical solutions to the long-term preservation of electronic records, it is important to reflect on what one is trying to achieve by preserving them. Our aim, in general, is the same for electronic records as it is for records held on paper or other traditional materials. But the special characteristics of electronic records, and in particular their relative fragility and susceptibility to change, mean that some aspects of the preservation task assume greater importance and urgency. Preservation is not an end in itself; we preserve things for a purpose, and sometimes for a number of purposes.

The assumption is made in this chapter that the primary reason for preserving records is for their evidential value: to demonstrate that actions were taken or not taken, that decisions were made or not, as the case may be. Evidence as used here does not relate purely to formal legal processes.

We also assume another possible purpose for the preservation of records – the reuse of the records themselves or the information that they contain. This is of particular relevance because reuse of electronic information is typically far easier than it is with information on paper, particularly when we are dealing with large quantities of data or documents. Our preservation actions should not put barriers in the way of such reuse. But we must also take care not to infringe any legal barriers to unrestricted reuse of information.

One might ask why we are worried about the reasons for preservation. By examining the practical steps we need to take, it should become clear the end purpose can dictate what actions should be taken and what actions institutions can afford *not* to take. There is no suggestion, for instance, of attempting to preserve the behaviour and appearance of old computer software and hardware as a museum might want to do. Because of this, any step taken which alters the appearance of a record, but which still preserves its principal characteristics, its evidential value and the information within it can be considered adequate for our purpose.

We are not talking exclusively about the *permanent* preservation of electronic records, but rather about their long-term preservation. This *includes* permanent preservation, as might be appropriate for records selected by a body such as a national archive. But it also includes preservation for fixed periods which greatly exceed the lifetime of the software and hardware used to create the records, such as personnel records which might need to be retained for 75 or 100 years from their creation or such other period as law may provide. It also includes preservation for indefinite, but not infinite, time periods which can be expected to exceed 5 years, such as building records which will be retained for at least as long as the life of the building to which they refer.

The common characteristic is that the preservation period is greatly in excess of the expected hardware, software and media lifetime, and is usually longer than the period for which we can make firm predictions about technological change. The uncertainty this introduces is a key influence on the strategies institutions need to adopt to ensure effective preservation.

The remainder of this section considers the requirements, which arise from the combination of:

- the reason(s) we are preserving electronic records; and
- the nature of electronic records themselves.

It also considers some of the implications, which arise from those requirements, such as the need for the creation and preservation of record metadata.

Basic requirements

To achieve our preservation purposes, records must be:

- authentic;
- complete;
- accessible and understandable;
- processable; and
- potentially reusable.

For each of these requirements, institutions should be able to reassure themselves and demonstrate to others that they have been met. There is also the desire to meet these requirements with the minimum of effort and the least disruption to the normal processes involved in creating and using the records as part of normal business. This chapter considers each of the essential characteristics in turn.

Authenticity

To show a record is **authentic** we simply need to be able to demonstrate that the record is what it claims to be. This is not the same as demonstrating the truth or accuracy of all the information, which the record contains. For an electronic record, there is the need to show that the record was created or received at the time which we claim for it, that the process which created it (whether a human being or an automated process) was the one we claim for it, that the record is truly part of the system which it claims to form part of, and that its contents have not been altered in any way since it became part of the record-keeping system.

For example, consider an e-mail received from outside the organisation which has been kept as part of a record system. The received e-mail has many similarities to a paper letter received in the post. Strong assertions can be made about some aspects of the e-mail

and the letter. We can say when we received them, who they were delivered to, and whether they received a reply. On the paper letter, this may be done with official stamps applied in the post room or correspondence logbooks, or a variety of other means. For the e-mail, the system may have added information to the e-mail headers as it was received and may also have logs of its arrival in the system and its delivery to its final recipient.

But in both cases there is little that can be said about other aspects of the message. We cannot be sure when it was written, although both the e-mail and the paper letter will probably carry a date of authorship. Unless special steps are taken to ensure security of communications, we cannot be confident about the identity or location of the sender, or of the integrity of the message contents (i.e. have they been amended or supplemented by a third part en route?). Finally, we can almost never attest to the accuracy of the message contents. For both paper and electronic systems these drawbacks do not alter the usefulness of the record. We keep the message, knowing it was received at this time, read by this person, contained this information and claimed to come from this source. If the identity of the sender or integrity of the contents were matters of particular concern to us, we may have means in the world of paper and electronic records to ensure this: both are likely to involve cryptography or identifiable signatures. To establish the **authenticity** of the record, we need only demonstrate that we have preserved what we knew about it when we received it.

It is worth noting that the authenticity of a record can usually be demonstrated without any knowledge of its contents (or even any means to access them).

Completeness

Completeness is typically used as a characteristic of a set of records rather than an individual item within the records, although it can apply to both. For a set of records to be **complete** we must be confident that no items have been added or removed from the set other than in accordance with the rules established for that set. This is a similar requirement to the **authenticity** requirement for a single item.

Completeness is not simply a matter of saying everything is still there because there may be very good reasons why some things are no longer there. It also involves saying nothing is there which should not be there. Let us consider e-mail again. We may have a policy that dictates how long different emails should be retained. At various times the recordkeeping system will contain different messages, and over time the number of messages within it will reduce. As long as we can demonstrate that the messages removed were removed in accordance with organisational policy, and that no messages appear which were not originally present, then we have demonstrated completeness.

Accessibility/understandability

Our complete and authentic collections are of no use if we cannot access them, or if we cannot make sense of their contents. Hence we impose a further requirement that the records are **accessible** and **understandable**. By **accessible** we mean that we still have some technology, both hardware and software, that allows us to locate records of interest and then translate them into a form which human senses can deal with, such as marks on paper or words on a screen. By **understandable** we mean that we can make sense of the record and the meaning it is intended to convey. This understanding may require assistance or support of other information, which is also part of the record system, it is not an absolute requirement that each record makes sense in isolation.

Records can be **accessible** even if we no longer have the hardware or software initially used to produce them. All that is required is that we have something, which can still be used to make them readable by people, even if the record does not have all the properties of the software that created them. For instance, documents will have been created with a programme which allowed them to be altered and viewed in a variety of ways; we may provide long-term access to them using a programme, which only allows us to view the documents, and only in one form. This still provides access to the records. But if all we have is the original digital medium, such as a floppy disk or a CD, and not any software or hardware, which allows us to access the contents of that medium, the records are not accessible. Similarly, if an original recordkeeping system depended on a sophisticated access mechanism, which allowed records to be sorted and located by properties such as date, title and author, it will be necessary to replicate something of that access mechanism in order to preserve the records in the system. A collection of thousands of files without any means of identifying which is which, other than reading them, is not, in any meaningful sense, **accessible**.

Records may be **understandable** in themselves if they are accessible – many documents and e-mails will fall into this category, assuming that the language in which they are written is one we can read. But other types of record may require additional information to be understandable. For instance, we may have records which document a survey of agricultural land in which a coding scheme was used to indicate the grade of land or the type of soil present on each plot. The coding system may assign a single letter or digit to each type of land or soil. Clearly, the records which contain these codes are not themselves understandable since the codes carry no intrinsic meaning. But if we also preserve the coding system with the records, then the records become understandable. Indeed, it would be correct to say that the coding system *is part of* the record, but in many computer systems it may not be part of the electronic system. It may exist only as a paper document, or only as part of instructions for those using the system. So to ensure the record is preserved in a form that we can understand, we must:

- ensure that the computer-based record is preserved in a processible form; **and**
- ensure that the paper documents for the coding system, or the information which they contain, are preserved in an accessible form; **and**
- ensure that the link between the record and the information on the coding system is preserved.

Processable

For records to be considered **processable** we must be able to manipulate, select and display them using criteria appropriate to their preservation purpose. This may mean using facilities similar or identical to those, which existed in the original record creating system. But in many cases, the system in which the records were created may have functions which are not required for the types of access which we will need in the long-term. Again, the example of word-processor files is useful. A collection of preserved word-processed documents only needs to provide means to locate documents of relevance and to view their contents via a screen, a printed copy, or some other suitable means. It does not need to preserve the ability to edit them or to carry out other actions which the original word processor software may have permitted.

Potentially reusable

Records are **potentially reusable** if it is possible to extract information from the record or otherwise allow the record to interact with modern information processing systems. This is a more rigorous requirement than those of accessibility or processability. Those requirements could conceivably be met by keeping the original hardware and software in

which the records were created active for as long as access to the records is required. This would allow the records to be accessed and processed. But if the older computer system does not have any means of exchanging information with newer computer systems, the records are effectively trapped within it. They are not, therefore, potentially reusable.

This requirement for reusability differs from the others in that it can be argued that for some purposes it is not necessary to allow for potential reuse of records. If we have met all our obligations through satisfying the other requirements, then reusability can be ignored. But in many cases it is desirable to aim for reusability even if no specific future use can be foreseen. By doing so, one has also usually ensured the record's accessibility and comprehensibility.

Technological development and changes

Technological change is an inescapable reality when dealing with computer systems. The pace of change is rapid compared to other areas of human progress in information recording and processing. The changes are driven by market forces which are often far from our requirements for long-term, stable access to authentic, unchanging information. It can therefore be a challenge to satisfy our requirements using a set of tools which will change even as we are considering how to employ them.

Our aim is to achieve the requirements stated above whilst all the mechanisms used to create, protect, manipulate, access and display the records change, and to be able to demonstrate that the records have retained essential attributes throughout that time.

The changes can take a number of forms. New application software is the most obvious. New software may simply be an updated version of existing software, or it may be a completely new package which has been adopted because it is cheaper or better than the old package, or because it offers greater compatibility with software being used elsewhere in an organisation. It is not always easy to tell the difference between updated software and new software, and it is not always useful to know. Version 3 of package X may simply be version 2 of package X with a small, well-defined set of new features. Or it may be a completely rewritten programme which happens to have the same name and which performs many, but not all, of the same functions.

Changes can also occur in the hardware used to run applications and make permanent copies of our records. Sometimes these changes have little relevance, as equipment suppliers strive to ensure that new equipment is compatible in as many ways as possible with the old, ensuring that old software continues to run and old media can continue to be accessed. But this compatibility does not persist forever. Each new generation of computer can typically handle the things that were new with the previous generation of computer. But they cannot necessarily handle the devices from three or more generations back. The changes that have greatest impact are those that involve changes in media types and attachment technologies. The shift from 5.25" to 3.5" floppy disks took place some years ago, and although it is still technically possible to attach a device to read 5.25" disks to a modern PC one would not choose to create or access records using such devices. The only reason we can still get them today, barely 20 years after their invention, is because their use was once so widespread. Other less widely used recording media of a similar age would present far greater challenges to access today (e.g. punch cards).

Changes also occur in the logical structures used to record information – what is usually referred to as the file format. Sometimes these changes come about as a direct result of changes in application software. Where they do, even if the newer software is capable of reading files in the older format, some inaccuracies may occur in the transformation and it can be difficult to confirm that all files will be transformed without error unless one has good knowledge of both the file formats and the software used to write and read them.

File format changes can also be driven upon us by external influences. It may be easier to manage our records, for instance, if they are all in a single format. Hence if newer records arrive in a different format from older records, this may prove an incentive to convert the older records to a newer format. Alternatively, there may be need to do so because the older format is no longer supported even for reading by current systems because no software has created files in that format for many years.

How important these changes are and how difficult it can be for us to deal with them depends on how much warning we have of them and how much we know about what the change involves. It is worth remembering that although many of the problems referred to can be overcome with sufficient ingenuity and technical knowledge, it can be very expensive to do so. Most archivists usually wish to avoid the heroic efforts that are necessary to recover information from 20-year-old recording media.

One of the most common conclusions reached by those involved in record preservation is that some form of migration is necessary to ensure the long-term survival of records. Other techniques do exist, some of which are the subject of intensive research, but migration is the technique in which there is most practical experience. Migration involves both copying records periodically to newer recording media, of the same type or of different types (this is known as 'refreshing') and moving information from one file format to another, more contemporary file format.

Relationship to the original system (i.e. the records creation system)
In a small number of cases it may be feasible to preserve records within the system that created them or its successors. These may even be essential when the original business purpose which the records served remains necessary and the records must continue to be accessed from within the same environment as other, more contemporary records. When this is true, the organisation should ensure that the periodic reimplementation of the system which will inevitably occur faithfully migrates information in older records to the newer formats, or that the system is capable of processing information in all the formats in which it has ever been created.

But in most cases organisations should preserve records independently of the systems that created them. This can be for a number of reasons:

- the systems will not exist for as long as the records;
- the systems will change function to the extent that old records can no longer be kept within them;
- performance reasons dictate that no more than a given number of records can be held within the system;
- authenticity cannot be assured within the creating system; and
- there is a need for access to the records which cannot be met by the system which created them (for instance, access by the general public to records created within a secure government system).

Some of these reasons are likely to provide greater control over when records need to be moved out of original systems. Decommissioning of record-creating systems is typically something which is planned some time in advance. As long as those responsible for long-term preservation are part of the overall planning process, sufficient time should be given to allow for an orderly transfer of records to the system needed for long-term preservation.

Other reasons for transfer can be very sudden. Performance problems are a frequent cause of sudden, unplanned transfers. The performance change may not be gradual and it may occur when the amount of information goes over a critical limit. Analysis of the system can usually indicate when this will occur and in an ideal world one will plan for these eventualities by monitoring the amount of information in the system and performing a planned extraction shortly before a critical limit is reached. But experience shows that this is the exception rather than the rule.

Sudden transfers are to be avoided if at all possible. They may lead to loss of information, loss of contextual metadata or loss of authenticity. It can also prove very difficult for the receiving organisation to deal with large volumes of records which it was not expecting.

Three tasks should be performed in order to preserve records outside the systems that created them. First, organisations should preserve the records themselves, whether they be individual documents, e-mail messages, or images. Second, it is important to preserve the contextual information that accompanies records (i.e. the recordkeeping metadata). This may range from indices of the documents through code lists and fixity information such as checksums or mechanisms for verifying digital signatures within the documents.

Finally, the relationship between the metadata and the documents (or other electronic records) themselves should be preserved. If there is a list of dates, titles and authors, the system should have an unequivocal way of linking that list to the electronic objects to which it refers. But the metadata may be less obvious and the relationship to the records less certain unless efforts are put in place to make them so. It is not uncommon for databases, for instance, to employ coding systems for some elements of information and for those coding systems to have altered during the lifetime of the system. Organisations may have a set of documents detailing each of the coding systems, but without clear information on when each was employed it is difficult to know how to interpret a particular coded record in the database.

But if organisations preserve the original objects in a form which is accessible to current computer users and in a way that ensures the authenticity of each individual object, and if they preserve the metadata which list each object and describe them, then they have achieved our aims of authenticity, completeness, accessibility and understandability. If the metadata and documents themselves can be processed by the new system together, then processability and, potentially, reusability have also been achieved.

Relationship to the access system

The system in which we preserve records, and the formats that we preserve them in, are not necessarily those which we will use to provide access. Separation of the two systems is often required when the community of users who may access the records is much larger, and different in nature or location, from those who created the records. Separation of access from preservation also allows the choice of file formats and software systems for

preservation, which are likely to be long-lived without needing to compromise our choice because of short-term requirements of the user community.

For instance, the TIFF file format has been recognised as the ideal choice for the preservation of digital still images since the early 1990s and it is likely that it will continue to be ideal for at least the next 10 years. Throughout this time, it has never been considered the ideal format in which to provide digital still images to most end users. There are a variety of reasons for this:

- colour images in TIFF files are very large, and hence slow and costly to transfer over network links;
- many users lack software which enables them to deal easily with TIFF images; and
- some end-user formats allow those who own the rights in the images more control over what the end user can do with the images than does TIFF.

The formats in which images have been provided to users of image archives have changed every few years in response to changes in fashion, technology and user demand and are likely to continue to change. These changes do not necessarily lead to changes in the methods used to preserve the images.

There are other advantages to constructing separate systems for preservation and access. In many cases, there is no need to provide access for part or all of the period during which we preserve things, or the access we need to provide is only to a small group of specialists (such as the archivists responsible for the records' safe custody.) By designing a preservation system which does not incorporate user access, but which has clear interfaces which permit user access systems to interact with it, savings can be made in terms of cost and complexity in the preservation system. Additionally, the system may more easily be adjusted to changing requirements for access in the future.

'Access' to electronic records once meant providing a means to print them; it has meant providing a machine-readable copy on tape or floppy disk; providing interactive access via the worldwide web; or providing access to users with a mobile telephone or other hand-held device. More mechanisms are likely to emerge in future. A properly designed preservation system will permit any and all of these to be dealt with without requiring any changes to the mechanisms or formats used to preserve the records.

Chapter 6 discusses access systems and their requirements in more detail.

The types and functions of metadata

We will focus here on three sources of metadata: recordkeeping metadata, archival metadata and technical metadata.

Recordkeeping metadata

Recordkeeping metadata are those which originated with the records themselves or within the organisation which created them. They might include elements such as author, date of creation, title, sensitivity and keywords. Recordkeeping metadata generally exist because they were necessary for the original purpose for which the records were created.

Archival metadata

Archival metadata are those which are added to help manage the records after they were originally created. This may be done by the original organisation as part of mechanisms for management of non-current records or by the eventual recipient such as a national

archive. Archival metadata might include such elements as last review date or originating organisation name.

Technical metadata
Technical metadata are those which are necessary for understanding and processing the records. Some may be considered recordkeeping metadata, since they come from the original system. Other aspects may be archival metadata, in that they are added as part of the long-term preservation process.

Examples of technical metadata include file format and date of last format migration. Technical metadata are often identified as metadata which the end-user need not be aware of as they are only used by other computer programmes to manage the records and preserve them. This is usually true but some users may need to have access to technical metadata. This may be particularly relevant if it comes to light (for instance) that a particular version of software which had been in use in the originating organisation some years ago was flawed. Some users would then want to know which records might be affected by that flaw.

5.4 Preservation methods

There are a number of approaches, both technical and organisational, to the preservation of electronic records. This section discusses these approaches and outlines the issue that might influence the choice of approach.

Different types of record will lend themselves more to one or other approach. The first section outlines in broad terms the different types of record that current computer systems are likely to create. The second and third sections consider the ways in which records can be preserved. Finally, in the fourth and fifth sections we make observations about bitstream preservation and about migration to new storage media.

The preferred preservation method will be influenced by:

- types of record creators and recordkeeping systems;
- the role of the archives in relation to records creation agencies and functions;
- legislation;
- the archives' skills and technical infrastructure; and
- the types and levels of user services planned (see **Chapter 6**).

Some of these will be absolute influences. Legislation, for instance, may mandate where certain records are preserved. Some influences will be relative and will allow for a degree of value judgement. The archives' skills and technical infrastructure is one instance of this. Such influences also need to be re-assessed periodically as changes in circumstances may warrant a change in approach.

Relevant types of electronic records
This *Workbook* does not attempt to present a complete taxonomy of the types of electronic file or object that can exist. Rather, we list some of the more common ones which may be found in current recordkeeping systems.

Office documents, such as memoranda, reports, presentations and e-mail, are all close analogues of record types which exist in the world of paper. Many of the principles by which they will be tracked will be similar, and it is relatively straightforward to assess which elements of the record need to be preserved to ensure we meet the requirements

stated earlier in this chapter. Note that for these, as for any other record type which comprises a collection of what can otherwise be treated as independent computer files, we will have a set of metadata which turns those separate files into a record collection, with order, provenance and other essential information. That metadata set will itself constitute a form of database, albeit a small and often relatively simple database. Preserving the metadata often requires the same techniques as would be used to preserve a database.

Databases are another extremely common application which generate records requiring long-term preservation action. They are often equivalent to some forms of paper record system such as registers, particular instance records, logbooks or catalogues. But the power of computers usually means that databases are far more complex systems than ever would have been created with paper, with many more information types within them and complex inter-relationships between those information types.

Websites and the documents within them are also worth special consideration. In many respects they are similar to any office document collection, but they are often more rapidly changing, and there is also explicit linkage and relationships to be maintained between the documents. Many websites also contain elements of interactivity with their readers which more traditional document types rarely display and websites also often involve elements, which are driven by databases rather than document collections.

Computers are used increasingly to create and manage collections of maps, drawings, photographs, sound and moving images, any of which may constitute a record collection. For the purposes of this document, all of these will have the same generic properties as the office document collection: they will constitute a set of individual files to which individual actions in relation to formats, authenticity and the like can be applied; and will be associated with a set of metadata which forms a structured database for the whole collection. These turn a set of files and information into a set of records.

Preservation methods in the creating environment

In some cases, preservation can effectively be carried out in the original environment and even in the original record-creating system. This will typically be true if all of the following conditions are met:

- the original system needs to be kept functioning for a primary business purpose;
- the original system meets the needs of those who are entitled to access the records; and
- the original system is able to retain all the records we wish to preserve without compromising its functionality or performance in meeting its primary business need.

It may be possible to use the original system for preservation alone even if the second condition is not fully met. To do so, one would have to build a compliant access system (compliant, that is, with user needs) which can extract records from the original system. This is a particular illustration of a general principle that the systems that we use to preserve records are not necessarily those that we use to provide access to them.

When it is possible, there are certain advantages to retaining records within the original system. There is no need to invest in mechanisms to extract and potentially transform the records into some other format in order to preserve them; and one does not have to incur the additional expense of constructing and administering a separate preservation system. Furthermore, organisations can be far more confident of the authenticity of the preserved records since they have not undergone any potentially damaging processes of translation.

Lastly, organisations can see the context and systems used to create the records. This may provide greater insight into the records, their creators and the interaction between them.

There are also disadvantages to this method. Over a very long period, the original system is unlikely to be retained in exactly the same form. Typically, changes in technology and changing business requirements may mean that the system slowly evolves in a way which may not be obvious in the short-term but which over longer periods may have an impact on the older records within it. Word processing packages are upgraded to newer versions; databases undergo alterations to the record structures within them as fields are added and removed, and the functions and interpretations of fields are changed. Unless careful attention is paid to the impact of these changes on older records problems may result, and the problems may not be noticed until it is too late to deal with them.

This will happen very easily unless the older records are being used for the conduct of current business. If the older records are only being retained for archival purposes, the checks which will be made to test that the new system functions properly may not involve any use of older records. This can be dealt with by ensuring that any testing methodology used as part of system upgrades has tests involving archival records built into it. One should also test periodically that older records can be accessed and rendered in a meaningful way.

Another disadvantage of this approach concerns access. Although we have said it is a prerequisite that the original system meets our needs for access for it to be used for preservation, this assumes that access requirements will not change. If they do, we may find that we need a radical change in how the records are preserved because the original record-creating system cannot meet our new access requirements.

In some cases, enabling a system to deal with very old records eventually makes it difficult to maintain and upgrade. At this point, it will be more cost-effective for the organisation to create separate mechanisms for older records and allow the system to deal only with current records. One should ensure that periodic monitoring of maintenance processes takes this into account. If at some point the system cannot cope with old records and current records, one may be faced with a sudden and urgent requirement to remove the archival records from the system and create a preservation system to store them in; doing this in response to a crisis, rather than as part of a planned process, will inevitably be more costly and riskier.

Some of these objections can be dealt with in a slight variant of this approach. We may choose to use the original software which created the records but in a separate computing environment (that is, typically, on separate hardware) from that which is being used to manage current records. This gives us almost all of the advantages of this method but can deal with some of the disadvantages, such as those related to performance. To do this, mechanisms are needed to identify and extract archival records from the current system, and there is the additional cost of running two systems.

A further option is to use a technique known as emulation, in which newer computer systems are provided with software that allows them to mimic (i.e. emulate) older hardware or software systems. Using this technique, a modern and presumably relatively inexpensive and easily maintainable computer can continue to run old software applications designed for quite different computers. We must, of course, continue to preserve the original software application in a form and on media which can be read by these

modern computers. Emulation is still being tested but it has already been demonstrated to be a practical solution in certain contexts.

All of these approaches can also suffer from the problem that they will eventually fail to meet our requirement that records be reusable. Eventually, older systems will not provide adequate mechanisms to interchange information with newer systems and at that point we may have to change our approach if the reusability of our records is one of the motives for preserving them.

Preservation methods in archives and other custodial institutions

Generally, the option of using the original system to preserve and provide access to our records is not available. There is a need to implement a specific system to preserve the records and mechanisms to move the records from the system which creates them to the system which will preserve them. This mechanism may also have to delete, or mark in some other way, the records thus exported from the creating system. Whether the records exist in only one system (the creating system or the preserving system) or potentially exist in both simultaneously is driven by business need. It is legitimate for records to exist in both places if, for instance, there is a business need to retain them in the original system, but that system is incapable of providing public access to the archival records it holds. By contrast, it is not legitimate to retain records in the original system if the primary need for them no longer exists, they contain personal or confidential information and they are being preserved only for future historical interest and/or legislation forbids their retention once the original need for them no longer exists.

In general, there is also the need to adopt a format for the preserved records (and their metadata), which is independent of any particular software system or hardware. Ideally, the format chosen will be defined by an international or national standard. Failing this, it should be defined by a standard that is publicly available and not subject to patent or licensing restrictions. Either of these will ensure that we are not dependent on any one supplier of hardware or software to ensure continued access to the records. Formats defined by such standards are usually well supported by many software suppliers. Even if we reach a stage where no commercially available software exists which can process our preserved files, the existence of the standards document means that we can create software afresh to read, render, process and reformat the files. If the standard comes from a recognised standards body, we can be confident that copies of the standard will be available from copyright libraries and similar bodies effectively in perpetuity. If it comes from a less formal body, it may be prudent to retain and preserve a copy of the standards document alongside the records.

The format we choose should be:

(a) able to represent all information and relationships between information in the original record that we regard as significant;
(b) defined by an international, national or publicly available standard;
(c) proven in terms of longevity or widespread adoption;
(d) directly usable for access purposes, or be capable of being transformed into formats which are thus usable;
(e) independent of any particular software or hardware environment;
(f) capable of automated conversion from original formats to preservation formats, with automated detection and reporting of conversion problems or errors where applicable; and
(g) (optionally) capable of automated conversion from our preservation format to the format used in the original or current record-creating systems.

Unfortunately not all types of information have file formats which meet all of these requirements today. At the time of writing, geographical information systems (GIS) are one example. Although open file formats have been developed in the past and a new, more advanced open GIS format is undergoing active development, tools are generally not available to translate from proprietary formats in which GIS records are created into the open formats in which we would like to store them. Thus, we cannot satisfy requirement (f). Tools do exist, however, to perform the reverse function – translating from open formats to proprietary formats. Thus, if one can construct a tool to convert GIS information into an open format, the format satisfies all our other requirements.

Some of the requirements are worthy of further clarification. Requirement (a) is intended to allow some flexibility in what we store and how we store it. It recognises that the original file may have some properties which are not intrinsic to the record we are trying to preserve and that a preservation format which cannot represent them still allows us to the preserve the record, even if it is not preserving everything in the original computer file. For a text document such as this, for instance, the words and the order in which they appear is of significance, and usually matters such as pagination and section numbering are also important, particularly if internal or external cross-references may exist to specific sections or pages of the document. The exact font or type size used is not usually so relevant, although stylistic variation such as the use of bold, italic or underlined text is often material to the meaning. Exactly which properties are significant needs to be assessed depending on the type of record and the information within it. We usually seek to show that the conversion process we employ preserves all significant properties by definition, or at least is able to warn us if it encounters a document where it cannot do so (second part of requirement (f)).

Requirement (f) ensures that we can take records from their original system into archival custody with the minimum of manual effort, and ensures that a robust exception reporting system exists which alerts us to any problems that require human intervention to resolve. Having an automated system, or at least a well-defined process and workflow, improves the auditability of the preservation process and helps to demonstrate the integrity of the end result. We can focus our efforts on the process and the tools used within it, rather than on proving the qualities of each preserved object.

Requirement (g) is noted as optional since in many cases it is not necessary. It is only a requirement if we foresee a need to move records back and forth between preservation in archival custody and use in the original record creating system. Even if we foresee this need, requirement (g) only becomes significant if the original record-creating system cannot import records using the access formats which requirement (d) says we need. If the creating system can use these formats to input records, then (g) is satisfied. This requirement may be difficult to meet if we have chosen a preservation format which discards some part of the original information content which we deemed not worthy of preservation. An example arises with word-processor file formats. The numbering of sections, pages, tables and figures is usually automated, with the word processor automatically renumbering everything as material is added and removed during the process of editing. Further, many word processors will extend this renumbering to the use of references within the text to other page or section numbers, or to the numbers of figures and tables. They do this by specially marking references to figures, distinguishing (for instance) the use of the words 'figure 3' from a reference of the form 'figure <n>' where '<n>' currently happens to be '3', but may later become 2 or 4. We may choose a preservation format that loses this special linkage, on the reasonable presumption that our preserved documents no longer need to be edited and so no longer require such function-

ality. But if the document is to be reused in its original system, and editing results in changes to table numbers or page numbers, the loss of the automatic renumbering of references to those pages and tables significantly reduces the usefulness of our preserved record within its original system.

Bitstream preservation

All of the methods of preservation we have discussed depend ultimately on our ability to carry out what is known as bitstream preservation. This is the ability to take a particular sequence of digital information, represented as a sequence of 1 and 0, and preserve it exactly without regard to its meaning or content. When preserving records we are at any one time usually dealing with a collection of bitstreams.

To ensure bitstreams are correctly preserved, we carry out a few basic actions and make one assumption: every bitstream has some unique identifier which does not alter during the time which we are preserving it and which can be used to retrieve it from the preservation system. To ensure completeness we must be able to demonstrate that we have every bitstream that we have been entrusted with, and that we do not possess any bitstreams which we have not been entrusted with. Doing this usually requires that we maintain some list of bitstream identifiers separate from the system in which they are preserved and usually with access controls that ensure no one person can simultaneously affect the information in both systems. Periodically we can compare the information in both systems.

We must also ensure that we can read every bitstream without error. This is typically done by periodic checks, which may be automated or manual. Once every six months to 2 years is a typical frequency for such checks. For small record collections on media such as CD, it is sufficient to ensure that all files on the CD can be copied to another medium (which may be temporary disk) without system-detected error. This would take only a few minutes of staff time every few months. To guard against hardware error, it is recommended that these checks are carried out on a system other than that which was used to write the media. (Some types of failure can result in media that can only be read in the tape or disk drive which created them).

Finally we must ensure that the bitstreams are unaltered. This is unusually done by a cryptographic technique to create a checksum, a small piece of information of fixed size, independent of the size of the bitstream but dependent on the contents of the bitstream. The checksum should have the property that it is difficult for any accidental or deliberate alteration of the file to take place without the checksum being altered. Checksums should be computed when files are taken in to archival storage and stored separately from the preserved files. Periodically files are re-read, their checksums re-computed, and compared with those computed when they were originally acquired. Any alteration is indicative of systems failure or deliberate human tampering, either of which needs to be investigated. A widely used checksum is the one known as MD-5, which is relatively straightforward to compute on any system, relatively strong cryptographically and not burdened by any patent restrictions. But continuing advances in computing power mean that these decisions should be reviewed approximately every 5 years.

Whenever we alter the format of our preserved files, we are altering the bitstreams and hence the actions above need to be carried out again as if the file was newly acquired for preservation.

Migration to new storage media

One further technique is used to protect against the fact that no computer storage medium is permanent, and most are subject to rapid degradation compared with paper. We should plan periodically to copy our files to new storage media, either of the same type as before or of a different type, more appropriate to current technology patterns. This process is known as 'migration.' In the past, we might have copied files from 5.25" floppy disks to 3.5" disks or to CD, or from 800 bpi ½" magnetic tape to 3480 tape cartridge. It is impossible to predict the medium to which copies will be made in future; all that is known is that there will be a need to do so. Most computer storage media last for periods of about 5 years - longer for some types under ideal storage conditions; but shorter for many types in conditions which are far from the ideal temperature, humidity or ambient light levels. Creating multiple copies of each of the preserved files and storing these copies at multiple locations helps to protect information. Digital copies, unlike copies of paper records, are potentially perfect and they are relatively cheap to produce. The protection institutions achieve through the use of multiple copies can mean that they can reduce the frequency of some of the other tests and processes referred to in this section.

5.5 Skills

The skills and knowledge required to ensure the long-term preservation of records are likely to come from a variety of people and are often split between the organisation responsible for creating the records and that which is responsible for preserving them. This is not materially different from the situation with traditional, paper records. Institutions depend on records having been created and managed by people with at least basic skills in record management, classification schemes, and the application of retention and disposal schedules; they rely on the archive which retains them having people who understand the organisations which created the records, who can describe them and make them accessible to their readers. Equally, the archive must have people with the necessary skills in preservation and conservation to ensure that the records are managed well and stored in conditions which will ensure their long-term survival.

Little is different with electronic records. Institutions may find that the necessary skills are spread through a greater number of people. For instance, the record-creating organisation is still required to have the basic skills to ensure that retention and disposal schedules are developed and applied to electronic records. But to apply the schedules effectively, and to audit that they have been applied, may require the advice or cooperation of someone with an understanding of the software and hardware systems in which the records exist. Such understanding can typically be found in people described as systems analysts. It is also important to recognise that although the systems analysts can help devise the necessary means of ensuring that schedules are applied correctly, they are unlikely to have the records management skills necessary to develop the schedules in the first place.

To ensure effective long-term preservation, institutions need people who understand the organisation and context in which the original records are created, just as we do with any other records. People with knowledge of file formats, and the use to which those formats are put, are also required. This knowledge rarely needs to be very technical. Most organisations use a small number of common file formats which are also used by organisations worldwide. Guidelines should be developed with appropriate expert input on how to deal with the most common file formats. Such guidelines already exist for digital images and digital audio files, as well as for a number of textual file formats. Therefore, it

is sufficient that most organisations have someone who is capable of assessing which guidelines are applicable to the organisation and of understanding how to apply them.

If the organisation has to deal with unique or obscure file formats for which no guidelines exist, or for which existing guidelines do not provide sufficient practical advice, it will be necessary to have a greater level of technical skills available to develop the necessary tools to preserve the records and to be able to test and validate those tools. Someone other than the author of the tools should ideally carry out the test and validation steps. Hence the organisation must have access to at least two people, or groups of people, with the necessary technical skills. It may be possible to ask another archival institution to help with the validation of tools one has developed in-house, or to use external consultancy. Alternatively, the tools can be developed by external software specialists and validated and tested using in-house expertise.

Archival institutions which have a duty to advise other organisations on how to create records will want to acquire skills in the design and use of common business applications so as to be able to provide appropriate advice. This may relate to the best use of e-mail applications for business purposes, or may be more technically oriented. For example, it might involve advising on configuring a particular database application to ensure it preserves auditable transaction records.

Organisations which are already actively involved in the management and preservation of electronic records have typically found that IT skills (in systems management and/or software development) and archival skills are both required, and that each specialist needs to have some basic understanding of the role of the other. Software engineers do not need to become qualified archivists, and archivists do not need to become systems programmers. Each, however, needs to be able to find a common language to discuss what they do and what each needs from the other. Mechanisms, which ensure that this dialogue is continuous and natural, have been shown to be most beneficial. In those organisations where the management of archives is organisationally and physically distant from those responsible for IT systems, communication tends to be both infrequent and ineffective and characterised by either fear or hostility. Conversely, if mechanisms are developed which allow for formal and informal communication to occur between these groups at all levels of responsibility, common cause is often found, problems arise less frequently and are solved more rapidly when they do arise. In short, there is a premium on team working and communication skills.

5.6 Summary

This chapter has addressed the practicalities of preserving electronic records. Any preservation technique must be consistent with the core requirements of authenticity; completeness; accessibility and understandability; processability; and potential reusabilty. Consideration of requirements does note lead us to advocate any one preservation technique as the solution which archives should adopt. It would be foolish to do so, not least at a time when solutions continue to evolve rapidly. Indeed one of the principal considerations in planning for preservation is how we best allow for future change. This chapter has shown the need to plan in the light of that contingency. But equally it has argued that the prospect of future change should not deter archivists from taking action now. The surest means of beginning to acquire experience and expertise in the field is to act – rather than to watch others.

FRANCÉS a)

CHAPITRE 5 : CONSERVATION À LONG TERME

5.1 Buts

Ce chapitre :

- explique, en termes pratiques, ce que conserver des documents veut dire ;
- décrit les différents procédés actuellement en usage pour conserver des documents électroniques ;
- présente la nature et le rôle des métadonnées dans le processus de conservation ; et
- identifie les compétences nécessaires pour conserver des documents électroniques.

5.2 Aperçu

Ce chapitre *du Manuel* traite des méthodes de conservation à long terme de documents électroniques. Par long terme, on entend, dans ce chapitre, une durée supérieure à la durée de fonctionnement du système (matériel comme logiciel), qui a produit les documents – durée qui n'excède généralement pas cinq ans au rythme actuel des changements technologiques. Il présuppose résolue la question de l'identification des documents à conserver. Il ne préjuge en rien des buts précis pour lesquels les documents doivent être conservés, ou du genre d'accès qu'on y aura.

5.3 Exigences et implications de la conservation

Avant de considérer les solutions techniques spécifiques de la conservation à long terme de documents électroniques, il est important de réfléchir à ce que l'on essaye de faire en les conservant. Notre but, en général, est le même pour des documents électroniques et des documents papier ou sur d'autres supports traditionnels. Mais les caractéristiques spéciales des documents électroniques, en particulier leur fragilité relative, et leur facilité de modification, impliquent que certains aspects de la conservation prennent plus d'importance et d'urgence. La conservation n'est pas une fin en soi ; nous conservons dans un but précis, et parfois, dans plusieurs buts.

Le présupposé de base de ce chapitre est que la première raison pour laquelle on conserve des documents est leur valeur de preuve : pour manifester que des actions ont été accomplies ou non, que des décisions ont été prises ou non, selon le cas. La notion de preuve employée ici ne doit pas être réduite à un aspect purement juridique.

Nous imaginons aussi un autre but possible pour la conservation de documents - la réutilisation des documents eux-mêmes ou de l'information qu'ils contiennent. Ceci est particulièrement pertinent car la réutilisation d'informations électroniques est beaucoup plus facile que pour des informations sur papier, en particulier quand il faut traiter des volumes importants de données ou de documents. Les actions de conservation ne doivent pas créer d'obstacles à ce genre de réutilisation des informations. Pour autant, il faut veiller à ne pas enfreindre la législation en matière de réutilisation d'informations.

On pourrait se demander pourquoi nous nous inquiétons des raisons de la conservation. En examinant les étapes pratiques nécessaires, il devrait devenir clair que le but final poursuivi exerce une contrainte très forte sur ce que les établissements chargés de la conservation peuvent faire et sur ce *qu'ils ne peuvent pas se permettre de faire.* Par exemple, personne ne suggère que nous devions préserver le comportement et l'apparence d'anciens logiciels et matériels comme un musée pourrait vouloir le faire. C'est pourquoi, toute mesure qui modifie l'apparence d'un document tout en conservant ses caractéristiques principales, sa valeur de preuve et les informations qu'il contient, est compatible avec notre but.

Nous ne parlons pas exclusivement de conservation *définitive* de documents électroniques, mais plutôt de leur conservation à long terme. Ceci *inclut* la conservation définitive, telle qu'elle convient aux documents sélectionnés par une institution du type Archives nationales. Mais cela comprend aussi la conservation pour une durée prévisible qui excède très largement la durée de fonctionnement du logiciel et du matériel utilisés pour créer les documents, comme les dossiers de personnel qu'il faut conserver pendant 75 ou 100 ans à partir de leur création ou toute autre période fixée par la loi. Cela comprend aussi la conservation pour une durée non définie, mais pas infinie, dès lors qu'elle excède 5 ans, comme les dossiers relatifs à la construction d'un bâtiment qu'il faudra garder au moins aussi longtemps que durera le bâtiment concerné.

Le point commun de tout ceci, est que la durée de conservation envisagée est très supérieure à la durée de vie qu'on peut attendre du matériel, du logiciel et des supports, et qu'elle est habituellement plus longue aussi que la période pour laquelle nous pouvons faire des prévisions valables sur l'évolution technologique. Cette incertitude exerce une influence essentielle sur les stratégies adoptées par les services en vue d'assurer une conservation efficace.

Le reste de cette section étudie les exigences, qui résultent de la combinaison des deux critères suivants :

- la (ou les) raison (s) pour laquelle nous conservons des documents électroniques ; et
- la nature des documents électroniques eux-mêmes.

Elle traite aussi de certaines conséquences qui découlent de ces exigences, comme la nécessité de créer et de conserver des métadonnées sur les documents.

Exigences de base

Pour réaliser nos buts de conservation, les documents doivent être :

- authentiques ;
- complets ;
- accessibles et intelligibles ;
- techniquement exploitables ; et
- potentiellement réutilisables.

Les services doivent s'assurer eux-mêmes et prouver à autrui, qu'ils sont capables de satisfaire chacune de ces exigences. Il y aussi le désir de satisfaire ces exigences avec le minimum d'effort et de rupture dans les processus habituels de création et d'utilisation des documents dans le cours normal des activités. Ce chapitre traite successivement de chacune de ces caractéristiques essentielles.

Authenticité

Pour montrer qu'un document est **authentique** nous devons simplement être capables de démontrer qu'il est bien ce qu'il prétend être. Ceci n'est pas la même chose que de montrer la vérité ou l'exactitude de toutes les informations contenues dans le document. Dans le cas d'un document électronique, il faut prouver qu'il a été créé ou reçu au moment où on affirme qu'il l'a été, que le processus qui l'a créé (qu'il soit automatique ou le fruit d'une intervention humaine) est bien celui qu'on prétend, et que le document fait vraiment partie du système dont il se réclame, et enfin, que son contenu n'a en rien été modifié depuis qu'il a été intégré dans le système d'archivage.

Prenons l'exemple d'un courrier électronique reçu d'un correspondant extérieur à l'organisation et versé dans un système d'archivage. Le courrier électronique a beaucoup de ressemblances avec un courrier papier reçu par la poste. On peut établir à propos de l'un comme de l'autre certains faits avec une grande certitude. On peut dire quand ils ont été reçus, à qui ils ont été distribués et s'ils ont reçu une réponse. Pour une lettre sur papier, on parvient à ces conclusions grâce aux tampons officiels appliqués sur elle par le service du courrier, ou par les livres d'enregistrement du courrier, ou grâce à d'autres moyens. Pour un courrier électronique, le système de messagerie peut ajouter ce genre d'information à l'en-tête du message, lors de sa réception, et peut aussi enregistrer la date de son arrivée, et l'identité du destinataire final.

Mais dans les deux cas, on ne peut guère en dire plus sur d'autres aspects du message. On ne peut être certain de la date de rédaction, bien que l'un comme l'autre portent probablement une telle date. Et, en l'absence de mesures particulières prises pour assurer la sécurité des communications, on ne peut être certain de l'identité de l'expéditeur, ni de l'endroit d'où il a envoyé le message, pas plus que de l'intégrité du contenu de message (c'est-à-dire a-t-il été modifié ou complété par une tierce personne en cours de route ?). En définitive on ne peut pratiquement jamais certifier l'exactitude du contenu d'un message. Ces inconvénients n'amoindrissent pas l'utilité des messages, qu'ils soient électroniques ou sur papier. On utilise le message, sachant qu'il a été reçu à tel moment, lu par telle personne, contenant telle information et prétendant provenir de telle source. Si l'identité de l'expéditeur ou l'intégrité du contenu posent un problème particulier, il existe des moyens, dans le monde du papier comme dans celui des documents électroniques, pour le régler : dans les deux cas, il s'agira probablement d'utilisation de techniques cryptographiques ou de signatures identifiables. Pour établir **l'authenticité** du document, on doit simplement prouver que l'on a conservé ce que l'on en savait quand on l'a reçu.

Il faut souligner ici que l'authenticité d'un document peut généralement être démontrée sans avoir connaissance de son contenu (ni même sans avoir un moyen d'y accéder).

Exhaustivité

La notion d'**exhaustivité** est habituellement employée pour caractériser un ensemble de documents plutôt qu'un article isolé, bien qu'elle puisse s'appliquer aux deux. Dans le cas d'un ensemble de documents, on pourra le considérer comme **complet,** si l'on est sûr qu'aucun article n'y a été ajouté ou n'en a été retiré, si ce n'est conformément aux règles applicables à cet ensemble. C'est une exigence semblable à l'exigence **d'authenticité** pour un article simple.

L'exhaustivité ne signifie pas que tout est toujours là parce qu'il peut y avoir de très bonnes raisons pour que certaines choses ne soient plus là. Elle signifie aussi que rien n'est là qui ne devrait pas y être. Revenons à l'exemple du courrier électronique. On peut avoir des règles qui fixent pendant combien de temps les différents courriers électroniques doivent être conservés. Selon le moment considéré, le système d'archivage contiendra divers messages et, avec le temps, le nombre de ces messages diminuera. Tant qu'on peut démontrer que les messages supprimés l'ont été conformément à la politique de l'organisation et qu'aucun message, qui n'existait pas à l'origine, se trouve dans le système, on a apporté la preuve de l'exhaustivité.

Accessibilité et intelligibilité

Les fonds conservés peuvent être complets et authentiques, ils resteront inutiles si on ne peut y avoir accès ni donner un sens à leur contenu. C'est la justification d'une nouvelle exigence qui veut que les documents soient **accessibles** et **compréhensibles**. Par **accessible,** nous voulons dire qu'on dispose toujours d'une technologie quelconque, tant en termes de matériel que de logiciel, qui permette de trouver les documents présentant un intérêt et de les traduire ensuite dans une forme accessible aux sens humains, telle que des marques sur un papier ou des mots sur un écran. Par **compréhensible** nous voulons dire qu'on peut donner un sens au document et comprendre ce qu'il est sensé transmettre. Cette compréhension peut nécessiter le recours à d'autres informations, incluses elles aussi dans le système d'archivage ; on n'exige pas que tout document, considéré isolément, ait un sens.

Les documents peuvent être **accessibles** même si on ne dispose plus du matériel ou du logiciel utilisés à l'origine pour les produire. Tout ce qui est exigé est que l'on ait un moyen de rendre ces documents lisibles par des êtres humains, même si les documents n'ont pas toutes les propriétés conférées par le logiciel qui les a créés. Par exemple, des documents sont créés par un logiciel qui permet de les modifier et de les présenter sous différents aspects ; on peut imaginer d'offrir un accès à long terme à ces documents, en employant un programme qui ne permettra que de les visualiser et sous une seule forme. Cette méthode permet bien l'accès aux documents. Mais si tout ce qui a été conservé n'est que le support informatique d'origine, tel qu'une disquette ou un CD, sans qu'on ait de logiciel ou de matériel qui permette d'avoir accès au contenu de ce support, alors les documents en question ne sont pas accessibles. De même, si le système originel de gestion des documents dispose de mécanismes élaborés d'accès, permettant de trier et de repérer les documents selon des critères tels que la date, le titre et l'auteur, il sera nécessaire de reproduire certains aspects de ces mécanismes d'accès pour conserver les documents. Un tas de plusieurs milliers de fichiers sans autre moyen d'identification que de les lire un par un, ne peut, en aucune façon, être considéré comme **accessible**.

Les documents peuvent être **compréhensibles** par eux-mêmes dès lors qu'ils sont accessibles - beaucoup de documents et de courriers électroniques entrent dans cette catégorie, en supposant connue la langue dans laquelle ils sont écrits. Mais d'autres types de documents peuvent nécessiter le recours à des informations complémentaires pour être compréhensibles. Par exemple, on peut être confronté à des documents relatifs à une enquête agricole, qui utilise un système de codage pour indiquer la catégorie de terre ou le type de sol sur chaque parcelle. Le système de codage peut faire correspondre à chaque type de terre ou de sol un caractère unique, chiffre ou lettre. À l'évidence des documents ainsi codés ne sont pas intelligibles puisque ces codes n'ont aucune signification intrinsèque. Mais si nous conservons aussi le système de codage avec les documents, alors ils deviennent compréhensibles. En fait il serait juste de dire que le système de codage *fait partie intégrante* du document, mais dans beaucoup de systèmes informatiques, il en est séparé. Il peut n'exister que sous forme papier, ou comme une partie des instructions données aux utilisateurs du système. Aussi pour s'assurer qu'un document est conservé sous une forme compréhensible, il faut :

- veiller à ce que le document informatique soit conservé sous une forme exploitable par une machine, **et**
- veiller à ce que les documents sur papier relatifs aux système de codage, ou l'information qu'ils contiennent, soient conservés sous une forme accessible ; **et**
- veiller à ce que le lien entre les documents et l'information sur le système de codage soit toujours maintenu.

Techniquement exploitable

Pour qu'un document soit techniquement **exploitable**, il faut être en mesure de le manipuler, de le sélectionner et d'en voir le contenu, selon des critères appropriés au but pour lequel on le conserve. Ceci peut revenir à utiliser des équipements semblables ou identiques à ceux qui existaient dans le système d'origine des documents. Mais dans de nombreux cas, le système dans lequel les documents ont été créés peut offrir des fonctions qui ne sont pas nécessaires pour les types d'accès dont on aura besoin à long terme. L'exemple des fichiers issus de traitements de texte est à nouveau éclairant. La conservation d'un ensemble de documents de ce type ne nécessite que de pouvoir trouver les documents pertinents, et d'en voir le contenu via un écran, ou une copie imprimée, ou tout autre moyen approprié. Il n'est pas nécessaire de conserver la capacité de les modifier, ou d'effectuer d'autres actions, que le logiciel de traitement de texte d'origine offrait.

Potentiellement réutilisable

Les documents sont **potentiellement réutilisables** s'il est possible d'en extraire une information pour la traiter ou s'il est possible, par tout autre moyen, de faire interagir les documents avec les systèmes informatiques contemporains. C'est une spécification plus exigeante que celles d'accessibilité ou d'exploitabilité technique. Ces dernières, en effet, pourraient être satisfaites en maintenant en activité, le temps nécessaire, le matériel et le logiciel d'origine des documents. On permettrait ainsi d'accéder aux documents et de les traiter. Mais si un système informatique ancien n'a pas la possibilité d'échanger d'informations avec des systèmes plus récents, les documents qu'il contient y sont littéralement pris au piège. Ils ne sont, dès lors, pas potentiellement réutilisables.

Cette exigence de réexploitation diffère des autres en ce qu'on peut estimer que, dans certain cas, il n'est pas nécessaire d'envisager la réutilisation des documents. Si toutes les autres exigences sont remplies, on peut donc l'ignorer. Mais dans des nombreux cas il reste préférable de tendre vers sa satisfaction, même si aucune utilisation spécifique future n'est encore prévisible. De plus, ce faisant, on assure généralement aussi l'accessibilité et l'intelligibilité des documents.

Développement et évolution technologiques

Le changement technologique est une réalité inéluctable en matière informatique. L'allure de ce changement est rapide comparée à d'autres secteurs du progrès humain dans le traitement et la conservation de l'information. Cette évolution est dirigée par les forces du marché qui sont souvent éloignées de nos exigences pour un accès pérenne et stable à des informations authentiques et non modifiées. C'est donc un défi à relever que de satisfaire ces exigences en employant une série d'outils qui évoluent au moment même où l'on se demande comment les utiliser.

Le but est de remplir les exigences exposées ci-dessus alors même que tous les mécanismes employés pour créer, protéger, manipuler, voir et faire voir les documents, et y avoir accès, ne cessent de changer, tout en faisant la preuve que ces documents n'ont perdu, au cours du processus, aucune caractéristique essentielle.

Ces changements peuvent prendre de nombreuses formes. Le cas d'un nouveau logiciel est le plus évident. Le nouveau logiciel peut simplement être une mise à jour du logiciel existant, ou il peut être un produit totalement nouveau, choisi parce qu'il est meilleur marché, plus performant que l'ancien, ou parce qu'il offre une compatibilité plus grande avec un autre logiciel employé dans l'organisation. Il n'est pas toujours facile de faire la différence entre la mise à jour d'un logiciel et un nouveau logiciel, et il n'est pas toujours utile de savoir. La version 3 du logiciel X peut être simplement la version 2 du logiciel X avec quelques petites nouveautés, bien déterminées. Ou il peut s'agir d'un programme complètement réécrit qui se trouve avoir le même nom et qui a des fonctionnalités identiques, mais pas toutes, à celles du précédent.

Les changements peuvent aussi concerner le matériel utilisé pour faire des copies de conservation des documents. Parfois ces changements ont peu de conséquences, car les fabricants de matériels s'efforcent d'assurer la compatibilité la plus large possible entre ancien et nouveau matériel, de sorte que d'anciens logiciels puissent toujours fonctionner et que d'anciens supports informatiques restent lisibles. Mais cette compatibilité n'est pas éternelle. En général, chaque nouvelle génération d'ordinateurs peut exploiter ce qui était nouveau pour la génération précédente d'ordinateurs. Mais ces nouveaux ordinateurs ne sont pas nécessairement capables d'exploiter les fichiers remontant à trois générations ou plus en arrière. Les changements qui ont l'impact le plus grand sont ceux qui concernent les types de supports et les technologies qui s'y rattachent. Le passage de la disquette 5.25 pouces à celle de 3.5 pouces s'est produit il y a plusieurs années déjà, et, bien qu'il soit toujours possible techniquement de relier à un micro-ordinateur actuel un système de lecture capable de lire des disquettes 5.25, plus personne n'utilise ce genre de système pour créer des documents ou y avoir accès. La seule raison pour laquelle on en trouve encore aujourd'hui, à peine 20 ans après leur invention, est que leur utilisation a été très largement

répandue. Il serait beaucoup plus difficile de lire aujourd'hui des supports datant de la même époque, mais d'usage moins répandu (par exemple des cartes perforées).

Les changements peuvent aussi concerner la structure logique utilisée pour enregistrer l'information - ce qu'on appelle généralement le format de fichier. Parfois ces changements sont le résultat direct de modifications du logiciel. Quoi qu'il en soit, et même si la version la plus récente du logiciel est capable de lire des fichiers de format ancien, des erreurs peuvent se produire dans le passage d'une version à une autre, et il peut s'avérer difficile d'être certain que tous les fichiers seront transformés sans erreur à moins que l'on n'ait une bonne connaissance tant du format de fichier que du logiciel utilisé pour les créer et les lire.

Des considérations extérieures peuvent aussi nous amener à faire des modifications de format. Par exemple, il peut être plus facile de gérer nos documents s'ils sont tous dans un format unique. Ainsi, l'arrivée aux Archives des documents récents, se présentant dans un format différent de documents déjà collectés, peut constituer une motivation pour convertir les documents anciens à un nouveau format. Ou il peut être nécessaire de procéder ainsi parce que l'ancien format n'est même plus lisible par les systèmes du moment, car aucun logiciel n'a créé de fichiers dans ce format depuis plusieurs années.

Le degré d'importance de ces changements et de difficulté à y faire face, dépend de la conscience que nous en avons et de notre connaissance de ce qu'ils impliquent. Il vaut la peine de se rappeler que, même si beaucoup des problèmes de ce genre peuvent être surmontés avec de l'ingéniosité et des connaissances techniques, cette tâche peut s'avérer très coûteuse. La plupart des archivistes préfèrent d'habitude éviter les efforts héroïques nécessaires pour récupérer des informations stockées sur des systèmes vieux de 20 ans.

Une des conclusions les plus communément admises par tous ceux qui sont impliqués dans la conservation de documents électroniques est qu'une forme de migration est nécessaire pour assurer leur survie à long terme. D'autres techniques existent, dont certaines font l'objet d'un effort intensif de recherche, mais la migration est la technique pour laquelle on dispose du plus d'expérience pratique. La migration s'applique aussi bien à la recopie périodique de documents sur de nouveaux supports, du même type ou de types différents (on parle de " régénération ") qu'au transfert de l'information d'un format de fichier à un autre format de fichier, plus " à la page ".

Relation avec le système originel (c'est-à-dire le système de création de documents)

Dans un petit nombre de cas, on peut conserver les documents dans le système qui les a créés ou ses successeurs. Ceux-ci peuvent même être essentiels quand les raisons pour lesquelles ils ont été créés restent valables et qu'ils doivent rester accessibles dans le même environnement au même titre que d'autres documents, plus récents. En pareil cas, il faut s'assurer que les inévitables mises à jour du système s'accompagnent d'une migration fiable des documents des formats anciens vers les nouveaux, ou que le système est capable de traiter tous les types de format d'information utilisés depuis sa création.

Mais dans la plupart des cas il faut conserver les documents indépendamment des systèmes qui les ont créés. Et ceci pour plusieurs raisons :

- Les systèmes durent moins longtemps que les documents ;
- Les fonctionnalités du système évoluent tellement qu'il ne peut plus traiter les anciens documents
- Les contraintes de performance imposent que ne soit conservé qu'un nombre limité de documents ;
- L'authenticité des documents ne peut être garantie dans le cadre du système d'origine et
- L'apparition d'un besoin d'accès aux documents sous une forme que leur système d'origine ne permet pas, (par exemple, l'accès du grand public à des documents administratifs créés dans un environnement sécurisé).

Certaines de ces raisons sont de nature à permettre un meilleur contrôle du moment où les documents doivent être sortis des systèmes originels. Ainsi, la cessation d'activité d'un système d'information est généralement une opération prévue à l'avance. Tant que les responsables de la conservation à long terme sont associés au processus de planification, ils auront le temps nécessaire pour organiser le transfert, en bon ordre, des documents vers le système chargé de les conserver à long terme.

D'autres motifs de transfert peuvent apparaître de façon subite. Les problèmes de performance sont une cause fréquente de transferts soudains et imprévus. La dégradation des performances n'est pas toujours progressive et peut se produire lorsque le volume d'informations traitées atteint un seuil critique. Généralement, l'analyse du système permet de savoir quand cela arrivera et, dans un monde idéal, on ferait face à ces éventualités en sur-

veillant le volume d'information dans le système et en réalisant une migration bien avant que soit atteint le seuil critique. Mais l'expérience montre que c'est l'exception plutôt que la règle.

Dans toute la mesure du possible, il faut éviter les transferts soudains. Ils peuvent entraîner la perte d'information, de métadonnées contextuelles ou d'authenticité. Il peut aussi s'avérer très difficile pour le service amené à recevoir les documents d'avoir à traiter d'importants volumes qu'il n'attendait pas.

Trois tâches doivent être exécutées pour conserver des documents hors des systèmes qui les ont créés. D'abord, les organisations doivent conserver les documents eux-mêmes, qu'il s'agisse de documents particuliers, de courriers électroniques ou d'images. Ensuite, il est important de conserver l'information contextuelle qui accompagne des documents (c'est-à-dire les métadonnées du système de gestion). Ce type de métadonnées va de l'indexation attribuée aux documents jusqu'aux listes de code et aux informations relatives à l'intégrité des documents, telles que les données de contrôle mathématiques et les systèmes de vérification des signatures électroniques.

Enfin, le lien entre les métadonnées et les documents (ou d'autres documents électroniques) eux-mêmes doit être préservé. Face à une liste de dates, de titres et d'auteurs, un système peut établir un lien sans ambiguïté entre cette liste et les objets électroniques auxquels elle se réfère. Mais il arrive que les métadonnées soient moins évidentes et leurs relations avec les documents moins assurées, sauf à déployer des efforts particuliers pour les clarifier. Par exemple, il n'est pas rare pour des bases de données que soient utilisés des systèmes de codage pour certaines données et que ces codes changent au cours de la vie de la base de données. On peut avoir des listes détaillant chacun des systèmes de codage, mais en l'absence d'information précisant quand chacun d'eux a été employé, il est difficile d'interpréter chacun des documents codés dans la base.

Mais si on conserve les objets originaux dans une forme accessible aux utilisateurs d'ordinateur contemporains et d'une façon qui en assure l'authenticité, et si l'on conserve aussi les métadonnées correspondantes, alors on aura atteint les buts d'authenticité, d'exhaustivité, d'accessibilité et d'intelligibilité que nous avons fixés. Si, de plus, les métadonnées et les documents eux-mêmes peuvent être traités par le nouveau système, alors l'objectif d'exploitabilité, et, virtuellement, celui de possibilité de réutilisation, sera aussi atteint.

Rapport au système de communication

Le système dans lequel on conserve les documents et les formats dans lesquels ils sont conservés, ne sont pas nécessairement les mêmes que ceux utilisés pour y accéder. La séparation des deux systèmes est souvent exigée quand la communauté des utilisateurs qui peuvent avoir accès aux documents est nettement plus large que celle des producteurs des documents et en diffère par sa nature ou sa localisation. La séparation entre communication et conservation permet aussi de choisir pour cette dernière des formats et des logiciels qui auront plus de chance d'être pérennes sans que ces choix soient compromis par des exigences à court terme de la communauté des utilisateurs.

Par exemple, le format de fichier TIFF a été reconnu comme le choix idéal pour la conservation des images numériques depuis le début des années 1990 et il est probable qu'il le restera pour au moins les dix ans qui viennent. Pour autant, il n'a jamais été considéré comme le format idéal pour permettre l'accès aux images aux utilisateurs finaux, et cela pour plusieurs raisons :

- les images en couleur prennent beaucoup de place en format TIFF et, de ce fait, sont lentes et coûteuses à télécharger sur des réseaux ;
- beaucoup d'utilisateurs ne disposent pas d'un logiciel capable de traiter facilement des images au format TIFF et
- certains autres formats permettent aux détenteurs de droits sur les images d'exercer un plus grand contrôle de leur utilisation par l'utilisateur final que ne le fait le format TIFF.

Les formats dans lesquels on fournit des images aux utilisateurs d'archives iconographiques changent fréquemment sous l'influence de la mode, de la technologie et des demandes des utilisateurs et vont probablement continuer à changer. Ces changements n'entraînent pas obligatoirement une modification des méthodes utilisées pour conserver les images.

Il y a d'autres avantages à créer des systèmes séparés pour la conservation et la communication. Dans de nombreux cas, il n'y a aucun besoin de fournir l'accès pour une partie ou pour toute la période de conservation ; parfois, l'accès qu'il faut assurer ne concerne qu'un petit groupe de spécialistes (comme les archivistes responsables de la bonne conservation des documents.) En concevant un système de conservation qui n'incorpore pas l'accès d'utilisateur, mais qui dispose d'interfaces efficaces permettant à des systèmes d'accès d'entrer en relation

et d'interagir avec lui, on peut réaliser des économies en termes de coûts et de complexité du système de conservation. De plus, à l'avenir, ce système pourra s'adapter plus facilement à de nouvelles exigences en matière d'accès.

L'accès aux documents électroniques a d'abord été conçu comme la possibilité de les imprimer ; puis, il s'est agi d'en fournir une copie lisible par machine sur bande ou sur disquette ; maintenant, on vise la fourniture d'accès interactif par internet ; ou on parle d'offrir aux utilisateurs l'accès aux documents sur leur téléphone portable ou d'autres dispositifs miniaturisés qui tiennent dans la main. D'autres dispositifs vont probablement apparaître dans l'avenir. Un système de conservation bien conçu doit permettre l'utilisation de tous ces dispositifs sans qu'il soit nécessaire de modifier les mécanismes ou les formats de conservation.

Pour plus de détails sur les systèmes d'accès et leurs spécifications, voir le **chapitre 6.**

Types et fonctions des métadonnées
Nous nous concentrerons ici sur trois types de métadonnées : les métadonnées de gestion, les métadonnées archivistiques et les métadonnées techniques.

Métadonnées de gestion
Les métadonnées de gestion sont celles qui ont été générées avec les documents eux-mêmes ou dans l'organisation qui les a créées. Elles peuvent comprendre des éléments comme l'auteur, la date de création, le titre, le caractère "sensible" des informations et des mots-clés. Ces métadonnées existent parce qu'elles étaient nécessaires à l'accomplissement de la tâche pour laquelle les documents ont été créés.

Métadonnées archivistiques
Les métadonnées archivistiques sont celles qu'on ajoute, après la création des documents, pour en faciliter la gestion. Cela peut être fait par le service producteur des documents, comme éléments d'une procédure de gestion des documents qui ne sont plus d'utilité courante, ou par un destinataire final éventuel tel qu'un service d'Archives nationales. Les métadonnées archivistiques peuvent inclure des éléments tels que la dernière date de révision ou le nom du service producteur d'une information.

Métadonnées techniques
Les métadonnées techniques sont les métadonnées nécessaires à la compréhension et au traitement des documents. Certaines peuvent être considérées comme relevant des métadonnées de gestion, car elles proviennent du système original. Sous d'autres aspects, on peut voir en elles des métadonnées archivistiques, dans la mesure où elles ont été ajoutées au cours du processus de conservation à long terme.

Comme exemples de métadonnées techniques on peut citer le format de fichier et la date de dernière migration de format. On considère souvent que l'utilisateur final n'a pas à connaître les métadonnées techniques dans la mesure où elles ne sont utiles qu'aux programmes informatiques qui gèrent et conservent les documents. C'est en général exact, mais certains utilisateurs peuvent avoir besoin d'accéder à ces métadonnées. Cela peut être particulièrement utile, s'il s'avère (par exemple) qu'une version particulière du logiciel utilisée auparavant par le service producteur comportait un défaut. Certains utilisateurs pourraient alors vouloir savoir quels documents ont pu être affectés par ce défaut.

5.4 Méthodes de conservation

Il existe plusieurs approches, aussi bien techniques qu'organisationnelles, pour la conservation de documents électroniques. Cette section discute ces approches et donne un aperçu des points particuliers susceptibles d'influencer le choix de l'une d'entre elles.

Divers types de documents se prêteront mieux à une méthode qu'à une autre. La première section traite, d'un point de vue général, des différents types de documents que les systèmes informatiques actuels produisent. Les deuxième et troisième sections traitent des moyens par lesquels on peut conserver les documents. Enfin, dans les quatrièmes et cinquièmes sections nous faisons des observations sur la conservation de flux de bits et la migration sur de nouveaux supports de stockage.

Le choix de la méthode de conservation sera fonction :

- des types de producteurs et de systèmes de gestion des documents ;
- du rôle des Archives par rapport aux services producteurs et de leurs fonctions ;
- de la législation ;

- des capacités et de l'infrastructure technique des Archives
- des types et des niveaux de services aux utilisateurs envisagés (voir **le Chapitre 6**).

Certains de ces critères auront une valeur absolue. La législation, par exemple, peut prescrire où doivent être conservés certains documents. D'autres critères n'auront qu'une valeur relative et laisseront une certaine liberté de jugement. Les capacités et l'infrastructure technique des archives sont un exemple de ce type de critère. Ceux-ci doivent être réévalués périodiquement car des changements de circonstances peuvent entraîner une modification d'approche.

Types pertinents de documents électroniques

Ce *Manuel* ne prétend pas présenter une taxinomie complète des types de fichier ou d'objets électroniques existants. Nous préférons plutôt donner la liste des types qu'on rencontre le plus communément dans les systèmes actuels de gestion de documents.

Les documents bureautiques, tels que mémorandums, rapports, présentations et courriers électroniques, sont tous similaires aux types de documents correspondants dans le monde du papier. La plupart des principes utilisés pour en suivre la trace archivistique seront les mêmes et il est relativement aisé de déterminer quels éléments constitutifs des documents doivent être conservés pour satisfaire aux spécifications exposées plus haut dans ce chapitre. Notez que pour ces documents, comme pour tout autre type de documents constitués de ce qui pourrait, par ailleurs, être considéré comme une série de fichiers informatiques distincts, on aura des métadonnées qui feront de ces fichiers séparés un ensemble organisés de documents, avec un ordre précis, une provenance et d'autres informations essentielles. Cet ensemble de métadonnées constituera lui-même une forme de base de données, d'un genre peu volumineux et souvent relativement simple. La conservation des métadonnées relève souvent des mêmes techniques que celles employées pour conserver une base de données.

Les bases de données sont une autre catégorie très courante d'applications informatiques qui produit des documents nécessitant une conservation à long terme. Elles sont souvent équivalentes à certains types de documents papier, tel que des cahiers d'enregistrements, des séries de dossiers individuels, des livres de bord ou des catalogues. Mais la puissance de l'informatique fait des bases de données des systèmes d'informations beaucoup plus complexes que tout ceux qu'on a pu créer sur papier, et comportant une plus grande variété d'informations entretenant des relations très diversifiés entre elles.

Les sites internet, comme les documents qu'ils contiennent, méritent une attention particulière. À bien des égards ils sont semblables à une collection quelconque de documents bureautiques, mais ils sont beaucoup plus fréquemment mis à jour, et, ils comportent des liens techniques, ou des relations, entre les documents qui doivent être conservés. Beaucoup de sites internet ont des possibilités d'interactivité avec les internautes que des types de document plus traditionnels offrent rarement ; enfin, les sites internet contiennent souvent des éléments dont le fonctionnement repose sur des bases de données et non sur un simple ensemble de documents.

On utilise de plus en plus l'informatique pour créer et gérer des collections de cartes, de dessins, de photographies, d'enregistrements sonores et d'images animées, dont chacune peut constituer un ensemble de documents d'archives. Pour les besoins de ce *Manuel*, nous considérerons que ce type de documents a les mêmes propriétés génériques qu'une collection de documents bureautiques : ils constituent un ensemble de fichiers séparés, auxquels des actions de conservation distinctes en terme de formats, d'authenticité, etc., peuvent être appliquées ; ils se verront attribuer un jeu de métadonnées, valable pour la collection prise dans son ensemble et formant une base de données structurée. Ainsi, on aura fait d'une série de fichiers et d'informations distincts un ensemble cohérent de documents d'archives.

Méthodes de conservation dans l'environnement de création

Dans certains cas la conservation peut être assurée efficacement dans l'environnement d'origine des documents, voire même par le système qui les a produits. C'est en particulier le cas, lorsque les conditions suivantes sont remplies :

- le système producteur doit être maintenu en fonctionnement pour remplir sa fonction première ;
- le système producteur répond aux besoins des personnes qui ont droit d'accès aux documents ; et
- le système producteur peut garder tous les documents que nous voulons conserver sans que cela compromettre ses fonctionnalités ou ses performances dans l'exécution de la tâche pour laquelle il a été conçu au départ.

Il est même possible d'utiliser le système producteur pour la conservation si la deuxième condition n'est pas entièrement remplie. Il suffit pour ce faire de mettre au point un système d'accès aux documents adéquats (en-

tendons adéquats aux besoins d'utilisateur) qui puisse extraire des documents du système producteur. C'est une illustration particulière du principe général selon lequel les systèmes de conservation des documents ne sont pas nécessairement ceux utilisés pour leur communication.

Lorsque cela est possible, conserver les documents dans le système qui les a produit présente des avantages certains. Il n'y a aucun besoin d'investir dans des mécanismes d'extraction, et, éventuellement, de conversion vers un autre format des documents pour les conserver ; on n'a pas non plus à supporter les dépenses qu'entraînent la création et la gestion d'un système de conservation distinct. En outre, on est beaucoup plus assuré de l'authenticité des documents conservés, puisqu'ils n'ont pas subi de conversion, opération toujours susceptible de causer des dégradations. Enfin, on peut ainsi connaître le système producteur et le contexte dans lequel les documents ont été produits. Ceci fournit une meilleure compréhension des documents, de leurs auteurs, et des relations entre eux.

Il y a aussi des inconvénients à cette méthode. Sur la longue durée, il est peu probable que le système utilisé au départ soit maintenu exactement sous la même forme. Ainsi, l'évolution technologique, comme les variations des besoins des utilisateurs, peut entraîner une modification progressive du système qui peut paraître sans conséquence à court terme, mais qui, à long terme, peut avoir un impact sur les documents les plus anciens. Les logiciels de traitement de texte sont mis à jour par de nouvelles versions ; les structures des bases de données sont modifiées par l'ajout ou la suppression de champs et par des changements dans la fonction ou l'interprétation des champs. A moins de les suivre avec une grande vigilance, l'impact de ces changements sur les documents les plus anciens peut créer des difficultés qu'on ne remarquera pas avant qu'il ne soit trop tard pour les régler.

Ce phénomène se produira très facilement sauf si les documents les plus anciens sont toujours utiles à la poursuite des activités du moment. Si les documents les plus anciens ne sont conservés qu'à des fins archivistiques, les contrôles faits pour tester les nouvelles fonctions du système ne les concerneront pas réellement. On peut remédier à cela en veillant à ce que toute méthode de test mise en œuvre à l'occasion d'une mise à jour du système comporte des tests sur les documents à valeur archivistique contenus dans le système. Il faut aussi vérifier régulièrement que les documents les plus anciens restent lisibles et présentables sous une forme compréhensible.

Un autre inconvénient de cette approche concerne la communication. Nous avons établi qu'une des conditions préalables à l'utilisation du système producteur des documents pour leur conservation, était que ce système réponde aux besoins en matière de communication ; mais ceci suppose que ces besoins n'évoluent pas. Dans le cas contraire, on peut être confronté à la nécessité d'une modification radicale de la méthode de conservation, car le système producteur ne sera pas capable de satisfaire les nouvelles exigences apparues en matière de communication.

Dans certains cas, rendre un système capable de traiter de très anciens documents, complique, en définitive, son entretien et sa mise à jour. À ce stade, il devient plus rentable de créer des mécanismes séparés pour conserver les documents les plus anciens, et de ne faire traiter par le système que les documents courants. Il faut veiller à ce que les contrôles périodiques du processus de maintenance prennent en compte cette question. Si à partir d'un moment donné, le système n'est plus capable de traiter ensemble les documents actuels et les plus anciens, on peut être confronté à la nécessité, aussi soudaine qu'urgente, de retirer les documents à valeur archivistique du système et de créer un système de conservation pour les y stocker ; faire cela en période de crise, plutôt que dans le cadre d'un processus planifié, sera inévitablement plus coûteux et plus risqué.

Certaines de ces difficultés peuvent être évitées en recourant à une légère variante de la méthode. On peut utiliser le logiciel qui a créé les documents, mais dans un environnement informatique séparé (c'est-à-dire, en fait, sur un matériel distinct) de celui utilisé pour gérer les documents courants. On bénéficie ainsi de presque tous les avantages de la méthode, en évitant certains de ses inconvénients, comme ceux liés aux problèmes de performance. Pour ce faire, il faut avoir des mécanismes d'identification et d'extraction des documents à valeur archivistique, et il faut tenir compte du surcoût entraîné par le fonctionnement de deux systèmes.

Une nouvelle méthode consiste à employer la technique dite de l'émulation, qui consister à implanter sur des ordinateurs actuels un logiciel capable d'émuler (c'est-à-dire de simuler) le comportement d'anciens logiciels ou matériels. Grâce à cette technique, un ordinateur moderne et, peut-on penser, peu coûteux et facile à maintenir, peut faire fonctionner de vieilles applications informatiques conçues pour des ordinateurs tout à fait différents. Il faut, bien sûr, toujours conserver le logiciel originel sous une forme et sur des supports lisibles par les ordinateurs actuels. L'émulation est toujours en cours d'évaluation, mais elle a déjà montré qu'elle constituait, dans certains cas, une solution pratique.

Toutes ces approches peuvent pâtir du fait, qu'en définitive, elles ne rempliront pas l'exigence de réexploitabilité des documents. Des systèmes anciens finiront par ne plus disposer d'interfaces adéquates pour communiquer avec des systèmes plus récents, et, parvenus à ce stade, on devra changer d'approche, si la réexploitabilité des documents est l'un des motifs de leur conservation.

Méthodes de conservation dans des services d'Archives ou d'autres institutions patrimoniales

Le plus souvent, la conservation et la communication des documents par le système qui les a produits ne sont pas des options envisageables. Il faut mettre en œuvre un système spécifique pour la conservation des documents et leur transfert du système qui les crée au système qui les conservera. Le mécanisme de transfert doit aussi supprimer, ou marquer de quelqu'autre façon, les documents ainsi exportés du système de création. Savoir si les documents doivent être présents dans un seul des deux systèmes (celui qui les produit ou celui qui les conserve), ou, virtuellement, dans les deux, est fonction des nécessités de la gestion courante. Il est légitime que les documents soient maintenus dans les deux systèmes, si, par exemple, ils sont nécessaires à la conduite des affaires courantes et, que, par ailleurs, le système producteur ne permet pas la communication au public des documents à valeur archivistique qu'il conserve. En revanche, il n'y a pas lieu de conserver des documents dans le système producteur s'ils ne sont plus d'utilité courante, s'ils contiennent des information personnelles ou confidentielles et ne sont conservés que dans un intérêt historique et/ou que la législation interdit leur conservation une fois satisfaite la finalité pour laquelle ils ont été créés à l'origine.

D'une manière générale, il faut choisir un format de conservation pour les documents (et leurs métadonnées), qui soit indépendant de tout logiciel ou matériel. Dans l'idéal, le format choisi sera défini par une norme internationale ou nationale. À défaut, il doit être défini par une norme publiée et non soumise à brevet ou licence. Ces caractéristiques garantissent l'indépendance des archivistes, dans leur effort pour permettre un accès pérenne aux documents, face aux fournisseurs de matériel ou de logiciel. Les formats définis par ce genre de norme sont habituellement utilisés par de nombreux fournisseurs de logiciel. Même s'il vient un moment où il n'existe plus sur le marché de logiciel capable de traiter les fichiers ainsi conservés, l'existence même d'une norme signifie qu'il reste possible de recréer un logiciel pour lire, restituer, traiter et reformater les fichiers. Si la norme provient d'un organisme reconnu de normalisation, on peut être certain que des exemplaires en seront disponibles dans les bibliothèques de dépôt légal, ou d'autres institutions du même genre, et ce, à perpétuité. Si elle provient d'un organisme moins bien établi, il peut être prudent d'en conserver un exemplaire avec les documents.

Le format choisi doit :

(a) pouvoir représenter toute les informations, et leurs liens, contenus dans le document et considérés comme significatifs ;
(b) être défini par une norme internationale, nationale ou rendue publique ;
(c) avoir fait la preuve de sa longévité et être largement utilisé et répandu ;
(d) être directement utilisable pour communiquer les documents, ou permettre une conversion vers des formats ainsi utilisables ;
(e) être indépendant de tout logiciel ou matériel ;
(f) permettre une conversion automatisée du format d'origine vers le format de conservation, avec détection et signalement automatiques des éventuels problèmes ou erreurs de conversion ; et
(g) (facultatif) permettre une conversion automatisée du format de conservation vers celui d'origine ou vers les formats courants du moment.

Malheureusement, à l'heure actuelle, les informations électroniques ne se présentent pas toutes sous des formats de fichier qui remplissent ces conditions. À l'heure où nous écrivons ces lignes, les systèmes d'information géographiques (SIG) sont un exemple de ce cas. Bien que des formats de fichier ouverts aient été développés dans le passé et qu'un nouveau format ouvert de SIG, plus avancé, soit en cours de développement, les outils de conversion des formats propriétaires dans lesquels les documents de SIG sont créés vers les formats ouverts dans lesquels on souhaiterait les conserver ne sont pas disponibles. En conséquence, la condition (f) ne peut être remplie. Il existe, cependant, des outils capables de faire l'inverse – convertir des formats ouverts aux formats propriétaires. Ainsi, si on peut mettre au point un outil pour convertir l'information SIG dans un format ouvert, toutes les autres conditions seront remplies.

Certaines de ces conditions méritent de plus amples explications. La condition (a) vise à apporter de la souplesse dans la façon de conserver et dans le choix de ce qui est conservé. Elle admet que le fichier original peut avoir des propriétés qui ne sont pas indissociables du document qu'on veut conserver et qu'un format de conservation qui ne les prend pas en compte, remplit cependant sa tâche, même s'il ne conserve pas tous les éléments du fichier original. Pour un document textuel comme ce *Manuel*, par exemple, les mots et l'ordre dans lequel ils

apparaissent sont signifiants et, généralement, des aspects tels que la pagination et la numérotation des sections sont aussi importants, en particulier s'il existe des renvois, internes ou externes, aux sections ou aux pages du document. En revanche, la police ou la taille de caractères employée n'ont pas autant d'importance, bien que des choix de mise en forme, comme l'utilisation de caractères gras, italiques ou soulignés, soit un élément matériel de la signification du texte. La détermination précise des propriétés significatives doit s'appuyer sur le type de document et d'information en cause. On considère, normalement, que le processus de conversion utilisé préserve, par définition, toutes les propriétés significatives, ou, à tout le moins, est capable de signaler les cas où il n'y parvient pas (seconde partie de la condition (f)).

La condition (f) garantit que l'on puisse transférer les documents du système producteur dans celui chargé de les conserver à titre d'archives avec le minimum d'effort manuel et qu'il existe un système fiable de détection d'anomalie signalant les problèmes qui exigent une intervention humaine. Disposer d'un système automatisé, ou au moins, d'un processus de traitement des flux bien défini, favorise la capacité d'audit du processus de conservation et aide à démontrer l'intégrité du résultat final. On peut donc se concentrer sur le processus lui-même et les outils employés, plutôt que chercher des preuves des qualités de chaque élément conservé.

La condition (g) est notée comme facultative car, dans beaucoup de cas, elle n'est pas nécessaire. Elle ne l'est que si l'on prévoit d'avoir besoin d'un aller et retour des documents entre leur conservation dans le système d'archivage et leur utilisation dans le système qui les a créés. Et même dans ce cas, la condition (g) ne devient effective que si le système qui a créé les documents ne peut pas les importer en utilisant un format de communication conforme à la condition (d). Si le système producteur peut employer un format de ce type, alors la condition (g) est remplie. Cette condition peut s'avérer difficile à remplir si on a choisi un format de conservation qui ne prend pas en charge certains aspects de l'information originale, aspects dont on pense qu'ils ne méritent pas d'être conservés. Les logiciels de traitement de texte fournissent un exemple de ce cas. Ces logiciels assurent automatiquement la numérotation des pages, sections, tableaux et schémas, y compris la mise à jour de la numérotation au fur et à mesure des modifications apportées au document au cours de sa rédaction. Mieux encore, la plupart des logiciels de traitement étendent cette renumérotation automatique aux renvois présents dans les documents, à d'autres pages, sections, tableaux ou schémas. Ils accomplissent cela en attribuant des marques distinctives aux chiffres, en distinguant (par exemple) l'utilisation des mots ' schéma 3 ' d'une référence du type ' numéro < n> ' où ' < n> ' se trouve être, à un moment donné, '3', mais peut plus tard devenir 2 ou 4. On peut choisir un format de conservation qui perd ce lien spécial, en se fondant sur la présomption raisonnable que les documents une fois conservés n'ont plus besoin d'être modifiés et que cette fonctionnalité n'est plus nécessaire. Mais si les documents doivent être réutilisés dans leur système d'origine et que cette réutilisation entraîne des changements dans les numéros de tableaux ou de pages, la perte de la fonction de renumérotation automatique des références à ces pages et tableaux réduira nettement l'utilité des documents conservés dans leur système d'origine.

Conservation de flux de bit

Toutes les méthodes de conservation évoquées ici dépendent en fin de compte de la capacité de pratiquer ce qu'on appelle la conservation de flux de bit. Il s'agit de la capacité à prendre une suite précise d'informations numériques, représentée comme une suite de 1 et 0, et de la conserver telle quelle, indépendamment de toute considération quant à sa signification et son contenu. Conserver des documents électroniques se ramène toujours à conserver des flux de bit.

Pour conserver correctement des flux de bit, il faut accomplir certaines tâches, en se basant sur une supposition : tout flux de bit dispose d'un identifiant unique, qui ne change pas, et qui peut être employé pour le retrouver dans le système de conservation. Pour satisfaire à l'exigence d'exhaustivité il faut de plus prouver que l'on a toujours tous les flux de bit qui nous ont été confiés et que l'on n'en pas d'autres, qui soient différents. Pour ce faire, il faut conserver une liste des identifiants de flux de bit, indépendamment du système de conservation, et il faut aussi avoir des contrôles d'accès qui garantissent que personne ne peut simultanément modifier les informations du système de conservation et de la liste des identifiants. On peut comparer à intervalle régulier les informations des deux systèmes.

Il faut aussi s'assurer qu'on peut lire chaque flux de bit sans erreur. C'est habituellement fait par des contrôles périodiques, qui peuvent être automatisés ou manuels. Une fréquence de contrôle comprise entre 6 mois à 2 ans est généralement pratiquée pour ce type de contrôles. Pour des fonds peu volumineux, stockés sur des supports du type CD, on peut se contenter de vérifier que tous les fichiers peuvent être copiés sur un autre support (qui peut être un disque provisoire) sans détection d'erreur. Ceci ne prend que quelques minutes de travail par mois. Pour éviter les erreurs dues au matériel, il est recommandé que ces contrôles soient effectués sur une plate-

forme technique différente de celle utilisée pour écrire sur les supports testés. (Dans certains cas, les supports ne peuvent être lus que par le matériel qui les a créés).

Enfin, il faut s'assurer que les flux de bit restent inchangés. On recourt parfois, exceptionnellement, à la technique de la cryptographie ; il s'agit de créer une donnée de contrôle mathématique, de taille fixée, indépendante de la taille du flux de bit, mais dépendante de son contenu. Cette donnée est conçue de telle sorte que toute modification accidentelle ou délibérée du fichier entraîne une modification de la donnée de contrôle. Les données de contrôle doivent être calculées à l'arrivée des fichiers aux Archives, et les résultats conservés séparément des fichiers. À intervalle régulier, on relit les fichiers, on recalcule les données de contrôle et les résultats sont comparés avec ceux calculés lors du versement. Toute modification est le signe soit d'une défaillance du système, soit d'une falsification délibérée, due à une intervention humaine, les deux cas méritant une enquête. Le système de données de contrôle le plus largement employé est le MD-5, qui est relativement facile à utiliser sur n'importe quel système informatique, relativement puissant sur plan cryptographique, et n'est pas soumis à des restrictions d'usage liées à un brevet. Mais l'augmentation continue de la puissance de calcul des ordinateurs nécessite que les choix en la matière soient révisés environ tous les 5 ans.

Lorsqu'on change le format de conservation des fichiers, on modifie les flux de bit. Toutes les opérations décrites ci-dessus doivent alors être à nouveau effectuées comme si les fichiers venaient d'être versés aux Archives.

Migration sur de nouveaux supports de stockage

Une autre technique est employée pour remédier au fait qu'aucun support de stockage informatique n'est éternel et que tous sont soumis à une dégradation rapide comparativement au papier. Il faut prévoir de recopier périodiquement les fichiers sur de nouveaux support de stockage, soit du même type que ceux utilisés jusque là, soit d'un type différent, plus approprié aux dernières évolutions de la technologie. On nomme ce processus 'la migration'. Dans le passé, on a pu ainsi copier des fichiers de disquettes souples 5.25" vers des disquettes 3.5'' ou vers des CD, ou passer de bandes magnétiques de densité 800 bpi ½ " à des cartouches 3480. Il est impossible de prévoir ce que sera le support de stockage de l'avenir ; tout ce qui est sûr, c'est qu'il faudra faire des copies. La plupart des supports de stockage informatiques ont une durée de vie d'environ 5 ans – durée qui peut être plus longue, pour certains d'entre eux, dans des conditions de stockage idéales ; mais qui peut être plus courte pour beaucoup d'autres dans des conditions de température, d'humidité ou de luminosité éloignées des valeurs idéales. La création des copies multiples de chaque fichier archivé, copies stockées dans des lieux distincts, aide à protéger l'information. Contrairement aux copies de documents papier, les copies numériques sont pratiquement parfaites et relativement peu coûteuses. Le degré de protection atteint à l'aide des copies multiples, permet aux services qui utilisent ce moyen de réduire la fréquence de certains des tests et autres processus mentionnés dans cette section.

5.5 Compétences

Les compétences et connaissances requises pour faire de la conservation à long terme de documents électroniques vont se retrouver chez une grande variété de personnes et sont souvent dispersées entre le service producteur des documents et celui qui est responsable de leur conservation. Ce n'est pas matériellement différent de la situation qui prévaut pour les documents traditionnels, sur papier. Les services dépendent de documents qui sont créés et gérés par du personnel ayant, au minimum des compétences élémentaires en *records management*, plans de classement et tableaux de conservation ; ils comptent sur les Archives qui les conservent grâce à du personnel qui comprend l'organisation des services producteurs, qui peut les décrire et les rendre accessibles à leurs lecteurs. Les Archives doivent aussi disposer d'un personnel compétent en matière de conservation matérielle afin que les documents soient bien gérés et conservés dans les conditions qui assureront leur survie à long terme.

La situation est légèrement différente avec les documents électroniques. Les services peuvent constater que les compétences nécessaires sont réparties parmi un plus grand nombre de professionnels. Par exemple, il faut toujours que le service producteur ait des personnes capables de veiller à ce que des tableaux de conservation soient élaborés et appliqués aux documents électroniques. Mais pour les appliquer concrètement et vérifier qu'ils l'ont été, il faut l'aide de quelqu'un qui ait une certaine connaissance du logiciel et de la plate forme technique avec lesquels ces documents ont été créés. Ce genre de connaissance est la caractéristique propre de ceux qu'on qualifie d'analystes-système. Il est aussi important de noter que, si les analystes-système peuvent aider à concevoir les moyens de veiller à ce que les tableaux de conservation soient correctement appliqués, il y a peu de chances pour qu'ils aient aussi les compétences nécessaires pour élaborer ces tableaux au départ.

Pour assurer une conservation à long terme efficace, les services ont besoin de personnes qui comprennent l'organisation et le contexte dans lequel les documents originaux sont créés, comme cela se fait avec les autres

documents. Mais il faut aussi avoir des personnes qui connaissent les formats de fichier et leurs utilisations. Cette connaissance a rarement besoin d'être très technique. La plupart des services emploient un petit nombre de formats de fichier, d'usage commun, et qui sont aussi largement employés à travers le monde entier. Il faut élaborer, avec l'aide d'experts compétents, des directives sur la façon de traiter les formats de fichiers les plus courants. De telles directives existent déjà pour les images numériques et les fichiers numériques audio, ainsi que pour un certain nombre de formats de fichier texte. Il suffit donc que chaque service dispose en son sein d'une personne capable de déterminer quelle directive est applicable et de savoir comment l'appliquer.

Si l'on a affaire à des formats uniques ou peu connus, pour lesquels il n'existe aucune directive, ou pour lesquels les directives existantes ne fournissent pas d'indications pratiques suffisantes, il faudra avoir un niveau de compétences techniques plus élevé pour développer les outils nécessaires à la conservation des documents et être capable d'évaluer et de valider ces outils. Dans l'idéal, la personne chargée de faire les tests d'évaluation et de validation ne doit pas être celle qui a mis au point les outils. Donc, le service doit disposer d'au moins deux personnes ayant les compétences techniques requises. On peut aussi s'adresser à un autre service d'archives pour faire valider des outils développés en interne, ou recourir à un consultant extérieur. Réciproquement, les outils peuvent être développés par des spécialistes extérieurs et validés en interne.

Les services d'archives dont la mission est de conseiller d'autres services sur la façon de créer des documents devront acquérir des compétences dans la conception et l'utilisation d'applications informatiques courantes afin d'être capables de fournir le conseil approprié. Cela peut concerner l'optimisation de l'utilisation du courrier électronique, ou des questions plus techniques. Par exemple, il pourrait s'agir de conseils sur la configuration d'une base de données particulière afin qu'elle conserve des traces de chaque transaction.

Les services qui sont déjà activement impliqués dans la gestion et la conservation de documents électroniques ont constaté que les compétences informatiques (dans la gestion de systèmes et/ou le développement de logiciel) et les compétences archivistiques sont toutes deux nécessaires, et que chaque spécialiste doit avoir une compréhension minimale du rôle de l'autre. Les informaticiens n'ont pas besoin de devenir des archivistes qualifiés et les archivistes n'ont pas besoin de devenir des programmeurs de systèmes. Chacun, cependant, doit trouver un langage commun pour discuter de ce qu'ils font et savoir ce que l'autre attend de lui. On a montré que des mécanismes qui rendent ce dialogue continu et naturel, sont plus efficaces. Dans des organisations où la gestion d'archives est fonctionnellement et physiquement éloignée des responsables informatiques, la communication a tendance à être peu fréquente, inefficace et caractérisée soit par la crainte soit par l'hostilité. Au contraire, s'il existe des procédures qui favorisent la communication, formelle et informelle, à tous les niveaux de responsabilité, entre ces deux groupes, un but commun se dégage, et les problèmes surgissent moins fréquemment et sont résolus plus rapidement quand ils surgissent. Bref, il y a une prime au travail d'équipe et aux compétences en communication.

5.6 Résumé

Ce chapitre a traité des aspects concrets de la conservation des documents électroniques. Toute méthode de conservation doit être compatible avec les exigences fondamentales d'authenticité ; d'exhaustivité ; d'accessibilité et d'intelligibilité ; de possibilité technique d'exploitation et de réutilisation. La prise en compte de ces exigences ne doit pas amener à préconiser une méthode particulière de conservation comme étant la solution que les Archives doivent adopter. Il serait stupide d'agir ainsi, ne serait-ce que parce que les solutions ne cessent d'évoluer à grande vitesse. En effet, une des considérations principales à prendre en compte pour la conservation est de savoir comment on peut mieux se préparer aux changements futurs. Ce chapitre a montré la nécessité de faire des plans à la lumière de cette éventualité. Mais il a également montré que la perspective de changements futurs ne doit pas empêcher les archivistes d'agir maintenant. Le meilleur moyen de commencer à acquérir de l'expérience dans ce domaine est d'agir soi-même - plutôt que de regarder faire les autres.

INGLES 6)

HRWG ica
human rights working group
international council on archives
groupe de travail sur les droits de l'homme
conseil international des archives

INTERNATIONAL COUNCIL ON ARCHIVES

HUMAN RIGHTS WORKING GROUP

BASIC PRINCIPLES ON THE ROLE OF ARCHIVISTS AND RECORDS MANAGERS IN SUPPORT OF HUMAN RIGHTS

A working document of the International Council on Archives

September 2016

INTRODUCTION

Archives are useful for human rights purposes. Many of these archives are essential to secure rights and benefits: personnel records, records of social insurance programs, records of occupational health and safety, records of military service. Other archives help prove civil rights: voter registrations, land titles, citizenship records. Still others provide evidence of the abuse of human rights, such as the records of military, police and intelligence units from periods of dictatorship, even records of prisons, hospitals, morgues and cemeteries.

Archivists and records managers handling archives with human rights aspects deal with concrete legal issues, questions of broad social policy, and matters of personal professional ethics. In many countries, this is complex but manageable using the best professional practice. However, archivists and records managers in a variety of situations and institutions may find themselves under pressure as they attempt to manage such archives. They may not be permitted to have access to the records for purposes of management or appraisal, they may be pressured to approve the disposal of archives that they believe have human rights implications, they may be instructed not to acknowledge in finding aids that the archives exist, they may not be able to undertake necessary preservation actions on these archives, they may not be permitted to make decisions about public access on these archives or provide them to qualified researchers. And they may fear retaliation if they seek to follow professional principles.

All archivists and records managers look for support from the profession at large as they seek to show the profession in its best, most competent light as they handle archives of importance for human rights. The International Council on Archives adopted a *Code of Ethics* in 1996, which provides a set of ethical parameters within which archivists carry out their professional duties. In 2011 the *Universal Declaration on Archives*, adopted by UNESCO in 2011, gave voice to the significance to the peoples of world of archives and the work of archivists and records managers. These important documents provide a general framework for the responsibilities of the profession; however, the important linkage between human rights and archives makes it important to clearly focus on the ethical and practical problems that are stated only generally in the framework Code and Declaration.

The *Basic Principles on the Role of Archivists and records managers in Support of Human Rights* is organized in two parts: a Preamble and a set of Principles. The Preamble provides the conceptual framework for the Principles. Each Principle is accompanied by explanatory text which is not part of the Principle. The Principles are grouped in five sections. The first two sections cover the basic archival functions; the third covers the special situations of working with archives that appear to document wrongdoing and with displaced archives; the fourth and fifth sections are devoted to the roles and rights of archivists and records managers as professionals.

The *Principles* are followed by definitions of terms used in the *Principles* and a list of international treaties, covenants, agreements, opinions and related matter that serve as foundation for the *Principles*.

Basic Principles of the Role of Archivists in Support of Human Rights

Preamble

Whereas the enforcement of human rights and fundamental freedoms to which all persons are entitled under the *Universal Declaration of Human Rights*, the *International Covenant on Civil and Political Rights* and its two Optional Protocols, the *International Covenant of Economic, Social and Cultural Rights* and other international treaties and legal instruments is strengthened by the preservation of archives and the ability of individuals to gain access to them;

Whereas the United Nations High Commissioner for Human Rights' *Updated Set of Principles for the Protection and Promotion of Human Rights through Action to Combat Impunity* asserts that it is responsibility of the State to "ensure the preservation of, and access to, archives concerning violations of human rights and humanitarian law;" proclaims that the right to know, including knowing what is in archives, is both a personal and collective right and that the State has a duty to remember; and emphasizes the importance of archives in ensuring that persons will be held accountable while guaranteeing the fair defense of everyone charged with a penal offense,

Whereas governments have the responsibility to promote and protect the right to seek and receive information as a fundamental prerequisite to ensuring public participation in governance,

Whereas adequate protection of the human rights and fundamental freedom to which all persons are entitled, be they economic, social and cultural, or civil and political, requires that all persons have effective access to archival services provided by independent archival professionals,

Whereas professional associations of archivists and records managers have a vital role to play in upholding professional standards and ethics, providing archival services to all in need of them, and cooperating with governmental and other institutions in furthering the ends of justice and the public interest,

Whereas the preservation of archives and access to them can be guaranteed only if all concerned—institutions and individuals—contribute to such goals, according to their respective responsibilities;

The *Basic Principles on the Role of Archivists and records managers in Support of Human Rights*, set forth below, have been formulated in order to:

- assist institutions that preserve archives in their task of ensuring the proper role of archivists in support of human rights,
- provide guidelines for individual archivists and records managers who, in the course of their everyday work, must take decisions that might affect the enforcement and protection of human rights,
- provide support for professional associations of archivists and records managers, and
- help international officials dealing with human rights issues understand the importance of the issues covered by the *Principles* and the contribution that professional archivists and records managers can provide to the protection of human rights.

The Principles

I. Selecting and Retaining Archives

1. ***Institutions, archivists and records managers should create and maintain recordkeeping regimes that protect archives that document human rights and should act to ensure that the management of those archives preserves the integrity of the archives and their value as evidence.***

   Regardless of format, archives need to support rights and entitlements or enable persons to protest effectively when their rights are violated, and must be strongly managed from their inception to ensure that they are accessible and trustworthy. The International Organization for Standardization (ISO) has published a number of standards which address these requirements. ISO 15489, "Information and documentation – Records management", for example, establishes core concepts and principles for the creation, capture and management of archives. Aligned with ISO 15489, the ISO 30300 series provides a systematic approach to the creation and management of archives, focused on the implementation and operation of an effective Management System for Records (MSR). In the digital environment, ISO 16175 "Principles and Functional Requirements for Records in Electronic Office Environments" provides internationally agreed principles and functional requirements for software used to create and manage digital information in office environments. Systems that create and manage human rights archives needs to ensure those archives can be proven to be genuine, are accurate and can be trusted, are complete and unaltered, secure from unauthorised access, alteration and deletion, can be found when needed, and are related to other relevant archives. ARMA International's *Generally Accepted Recordkeeping Principles* provide a benchmark for managing archives in both public and private sectors.

2. ***Institutions, archivists and records managers should prevent the destruction of archives that are likely to contain evidence of the violation of human rights or humanitarian law.***

   Principle 14, "Measures for the Preservation of Archives," of the United Nations High Commissioner for Human Rights' *Updated Set of Principles to Combat Impunity* states, "The right to know implies that archives should be preserved. Technical measures and penalties shall be applied to prevent any removal, destruction, concealment or falsification of archives, especially for the purpose of ensuring the impunity of perpetrators of violations of human rights and/or humanitarian law." While an archivist or records manager may not know that a body of archives contains evidence of violations, an archivist or records manager may be able to presume, based on the provenance of the archives, that the content may contain such information and should not be destroyed.

3. ***Archivists and records managers should select, acquire and retain archives that are within the scope and mandate of their archival institution, without discrimination that is proscribed by the Universal Declaration of Human Rights.***

   Article 2 of the *Universal Declaration of Human Rights* states that everyone is entitled to rights and freedoms "without distinction of any kind, such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." Archivists should ensure that they acquire archives that reflect and are pertinent to all groups. Some archives have a special focus, such as archives of faith-based bodes, archives of indigenous communities, or archives documenting social movements. These institutions discriminate in their acquisition program in accordance with their mandate, but regardless of their special focus within their mandate they are inclusive.

4. ***Archivists and records managers should consider in each appraisal decision the utility of that body of archives to support or identify a claim of human rights, to assist in the identification of perpetrators of human rights violations, to permit the identification of persons who held positions that might have involved them in human rights violations, to clarify the events that led to the violation of human rights, to help resolve the fate of missing persons, or to enable individuals to seek compensation for past violations of human rights.***

   Following the concepts developed in the United Nations High Commissioner for Human Rights' *Updated Set of Principles to Combat Impunity*, transitional justice is understood to require holding perpetrators accountable, ensuring that persons responsible for abuses in the old regime are not in positions of power in the new one; determining the truth of what happened to society as a whole, to groups within the society and to individuals; and obtaining restitution and reparation. Similar demands are made in democratic states in the aftermath of state actions that caused civic trauma and, increasingly, the actions of private bodies that violate rights. Archives are essential in these processes.

   Many other bodies of archives support human rights, from civil registries to land titles to personnel files of the clergy to archives that show a business enterprise's due diligence when it contracts for goods, as required by the *UN Guiding Principles on Business and Human Rights* adopted in 2011. Archivists and records managers should be aware of the rights that might be supported by the archives they manage.

5. ***Governments should ensure that archives concerning violations of human rights and humanitarian law are preserved. Governments and private institutions ensure the provision of sufficient funding and other resources for the professional management of these archives.***

   Principle 3, "The Duty to Preserve Memory" of the United Nations High Commissioner for Human Rights' *Updated Set of Principles to Combat Impunity* states, "A people's knowledge of the history of its oppression is part of its heritage and, as such, must be ensured by appropriate measures in fulfillment of the State's duty to preserve archives and other evidence concerning human rights violations and to facilitate knowledge of those violations. Such measures shall be aimed at preserving the collective memory from extinction and, in particular, at guarding against the development of revisionist and negationist arguments."

The Principle does not say the State must preserve only the State's archives; it instead says "archives." A State has many options for supporting preservation and access to non-governmental archives, such as making forceful public statements on preservation and access, enacting legislation requiring such archives be preserved, obtaining court rulings that require specific archives be preserved, providing monetary support for non-government archives, conducting surveys and creating databases to identify for the public where relevant archives are located, taking donations of private sector archives, or providing a "safe haven' trusted repository for endangered archives.

6. ***Institutions, archivists and records managers should ensure that the archives of temporary bodies established to assist in transitional justice are protected and preserved, both while the entity exists and after it closes; public notice should be given prior to the disposal of any archives from these bodies.***

Principle 5, "Guarantees to Give Effect to the Right to Know," of the United Nations High Commissioner for Human Rights' *Updated Set of Principles to Combat Impunity* reads in part: "Societies that have experienced heinous crimes perpetrated on a massive or systematic basis may benefit in particular from the creation of a truth commission or other commission of inquiry to establish the facts surrounding those violations so that the truth may be ascertained and to prevent the disappearance of evidence. Regardless of whether a State establishes such a body, it must ensure the preservation of, and access to, archives concerning violations of human rights."

The archives of transitional justice institutions, whether created by governments or by private institutions, concern violations of human rights and fall within this scope. Giving public notice before destroying part of an archives is an established practice in states such as Spain and the United States and provides an opportunity for the public to object to the disposal of bodies of archives, which is particularly important when the archives are the product of these sensitive transitional justice institutions.

II. Providing Access to Information in Archives

7. ***Archivists should include in the description of archival holdings information that to the best of their knowledge enables users to understand whether the archives might contain information that would be useful to exercise a claim of human rights, with particular regard to information regarding gross human rights violations, information that would help resolve the fate of missing persons, or information that may enable individuals to seek compensation for past violations of human rights.***

Principle 2, "The Inalienable Right to the Truth," of the United Nations High Commissioner for Human Rights' *Updated Set of Principles to Combat Impunity* states, "Every people has the inalienable right to know the truth about past events concerning the perpetration of heinous crimes and about the circumstances and reasons that led, through massive or systematic violations of human rights, to the perpetration of those crimes. Full and effective exercise of the right to the truth provides a vital safeguard against the recurrence of violations." The right to know the truth also is recognized explicitly in the

International Convention for the Protection of All Persons from Enforced Disappearances, adopted in 2010. *Recommendation No. R (2000) 13 of the Committee of Ministers to member states on a European policy on access to archives* explains "that a country does not become fully democratic until each one of its inhabitants has the possibility of knowing in an objective manner the elements of their history." Good archival description enables the right to truth and supports democracy.

8. ***Archivists and records managers should provide timely arrangement and description of the archives in the holdings to ensure equal, fair and effective access for users, giving priority to organizing and describing archival holdings documenting gross human rights violations.***

   Archival institutions may not have a sufficient number of archivists to provide timely description of all archival holdings. When deciding the priorities for description of archival holdings, human rights concerns should be a key element to consider.

9. ***Governments should ensure that access is provided to their archives concerning violations of human rights and humanitarian law.***

   Article 19.2 of the *International Covenant on Civil and Political Rights* establishes that everyone "shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information."

   The December 2004 *Joint Declaration* by the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Cooperation in Europe's Representative on Freedom of the Media, and the Organization of American States' Special Rapporteur on Freedom of Expression states, "The right to access information held by public authorities is a fundamental human right."

   The *Global Principles on National Security and the Right to Information* (the *Tshwane* Principles) set out guidelines on how to guarantee, to the extent possible, public access to government information while protecting legitimate national security concerns; Principle 10.A.1 states, "There is an overriding public interest in disclosure of information regarding gross violations of human rights or serious violations of international humanitarian law, including crimes under international law, and systematic or widespread violations of the rights to personal liberty and security. Such information may not be withheld on national security grounds in any circumstances." The Council of Europe's Parliamentary Assembly endorsed the *Tshwane Principles* in Resolution 1954 (2013): *National security and access to information.*

10. ***Archivists and records managers should advocate for and support the right of access to government archives and encourage non-governmental institutions to provide similar access to their archives, in accordance with the Principles of Access to Archives adopted by the International Council on Archives.***

    The ten ICA *Principles of Access* are the foundation for this Principle. In addition, Principle 6 of the International Council on Archives' *Code of Ethics* states, "Archivists should promote the widest possible access to archival material and provide an impartial service to all users," and the *Universal Declaration on Archives*, endorsed by the General

Conference of UNESCO in 2011, declares, "Archives are made accessible to everyone, while respecting the pertinent laws and the rights of individuals, creators, owners and users."

A special requirement for access is found in Principle 16, "Cooperation between Archives Departments and the Courts and Non-judicial Commissions of Inquiry," of the United Nations High Commissioner for Human Rights' *Updated Set of Principles to Combat Impunity* which states: "The courts and non-judicial commissions of inquiry, as well as the investigators reporting to them, must have access to relevant archives. This principle must be implemented in a manner that respects applicable privacy concerns, including in particular assurances of confidentiality provided to victims and other witnesses as a precondition of their testimony. Access may not be denied on grounds of national security unless, in exceptional circumstances, the restriction has been prescribed by law; the Government has demonstrated that the restriction is necessary in a democratic society to protect a legitimate national security interest; and the denial is subject to independent judicial review."

11. ***Institutions, archivists and records managers should ensure that safeguards are in place to protect personal information from unauthorized access, in order to ensure respect for rights, fundamental freedoms and the dignity of persons to whom the information relates.***

In addition to the provisions of the *Principles of Access*, Principle 7of the International Council on Archives' *Code of Ethics* states, "Archivists should take care that corporate and personal privacy as well as national security are protected without destroying information, especially in the case of electronic records where updating and erasure are common practice. They must respect the privacy of individuals who created or are the subjects of records, especially those who had no voice in the use or disposition of the materials." Uncritical opening of archives may result in violations of the privacy of individuals and may result in retaliation against them. Archivists and records managers balance the right to truth with the need to protect the privacy of identifiable persons.

12. ***Archivists should provide reference service without discrimination that is proscribed by the Universal Declaration of Human Rights. All persons are entitled to call upon the assistance of an archivist to help them locate and retrieve archives that may enable them to establish their rights.***

As stated above in Principle 3, Article 2 of the *Universal Declaration of Human Rights* states that everyone is entitled to rights and freedoms "without distinction of any kind, such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."

Principle 15, "Measures for Facilitating Access to Archives," of the United Nations High Commissioner for Human Rights' *Updated Set of Principles to Combat Impunity,* states in part: "Access to archives shall be facilitated in order to enable victims and persons related to claim their rights. . . . Access to archives should also be facilitated in the interest of historical research, subject to reasonable restrictions aimed at safeguarding the privacy and security of victims and other individuals. Formal requirements governing access may not be used for purposes of censorship."

This Principle does not prohibit institutional rules on who may use the archives (such as a requirement that a person must be of a certain age to use the archives or that a person may see his own file but the public may not), but it does require institutions to set those rules with a conscious effort to make access as fair and equal as possible.

13. ***Archivists should ensure that persons seeking to defend themselves from charges of violations of human rights are afforded access to archives.***

Included in Principle 15 of the United Nations High Commissioner for Human Rights' *Updated Set of Principles to Combat Impunity* is "Access should also be facilitated, as necessary, for persons implicated, who request it for their defence." Archivists and records managers should not make distinctions between prosecutors and defendants when providing access to archives.

14. ***Institutions, professional associations of archivists and records managers and individuals should promote programs to inform the public about their right of access to archives and the important role of archivists in protecting their fundamental freedoms. Special attention should be given to ensuring that disadvantaged persons know that they may call upon archivists to locate and retrieve archives that may enable them to assert their rights.***

Principle 3 of the *Principles of Access to Archives* adopted by the International Council on Archives, states, "Institutions holding archives adopt a pro-active approach to access." Special needs of archives' users should be accommodated. In particular, the *United Nations Convention on the Rights of Persons with Disabilities* declares that persons with disabilities are entitled to the "freedom to seek, receive and impart information and ideas on an equal basis with others and through all forms of communication of their choice" and that information intended for the general public should be provided "to persons with disabilities in accessible formats and technologies appropriate to different kinds of disabilities in a timely manner and without additional cost." Similarly, the *United Nations Declaration on the Rights of Indigenous Peoples* affirms that indigenous peoples have the right to maintain, protect and develop the past, present and future manifestations of their cultures, including their archives; to obtain these goals, assistance in locating and copying archives may be required.

III. Special Safeguards

15. ***Archivists or records managers who, in the course of their professional activity, discover archives that they in good faith and on reasonable grounds believe contain evidence of gross violations of internationally recognized human rights that (a) are ongoing or (b) for which victims might seek compensation, should inform pertinent authorities about the existence of such archives.***
    a. ***Governments should provide government employees with channels to report such violations, either internally or to oversight bodies.***
    b. ***Non-governmental institutions may provide channels for their employees to report human rights violations; if such channels do not exist, governments may provide channels for reporting by persons who are not government employees.***

Information which shows wrongdoing, whether or not it is currently available to the general public, should be disclosed to appropriate authorities. The *Global Principles on National Security and the Right to Information,* Principle 37, suggests that information related to the following categories of wrongdoing should be considered for "public interest disclosures":

(a) "criminal offenses;
(b) "human rights violations;
(c) "international humanitarian law violations;
(d) "corruption;
(e) "dangers to public health and safety;
(f) "dangers to the environment;
(g) "abuse of public office;
(h) "miscarriages of justice;
(i) "mismanagement or waste of resources;
(j) "retaliation for disclosure of the any of the above listed categories of wrongdoing; and
(k) "deliberate concealment of any matter falling into one of the above categories."

While the *Global Principles* speak specifically to government information, it is clear that this information can also be present in the archives of non-government institutions and archives of individuals.

The question of appropriate channels for reporting is difficult. If the institution has a formal reporting channel and if using it does not put the archivist or records manager at risk of retaliation, that channel should be used first. Independent oversight bodies or judicial authorities are alternate reporting channels. If no institution within the state can be trusted with the information, the archivist or records manager can turn to international bodies such as the staff of the United Nations High Commissioner for Human Rights or the International Committee of the Red Cross.

16. ***Archivists and records managers who make disclosures of information showing violations of human rights or international humanitarian law, regardless of whether the information is classified or otherwise confidential, have the right to report to an appropriate authority any measure of retaliation or the threat of retaliation in relation to the disclosure; provided that (a) at the time of disclosure the archivist had reasonable grounds to believe that the information disclosed shows wrongdoing, and (b) the archivist previously tried to use any existing internal reporting mechanism, so long as doing so did not increase the risk of retaliation.***

Governments should have laws that protect from retaliation persons who make disclosures of information concerning wrongdoing as defined in Principle 15 above. The Council of Europe's Parliamentary Assembly Resolution 1954 (2013) on *National security and access to information* states, "A person who discloses wrongdoings in the public interest (whistle-blower) should be protected from any type of retaliation, provided he or she acted in good faith and followed applicable procedures." The Council of Europe's Committee of Ministers made a similar point in its *Recommendation CM/Rec (2014)7 to member States on the protection of whistleblowers.*

As the *Global Principles on National Security and the Right to Information* suggest in Principle 40, "if contested, the person may need to defend the reasonableness of his or her belief and it is ultimately for an independent court or tribunal to determine whether this test has been satisfied so as to qualify the disclosure for protection." As with Principle 15, the reporting of retaliation should first be to national authorities but may be to international authorities if no national protection is believed to be available or secure.

17. ***Institutions, archivists and records managers should respect the cultural and legal patrimony of countries and communities and not acquire archives which do not fall with their jurisdiction. Institutional acquisition policies should respect the right of communities to write their own histories.***

The Executive Committee of the International Council on Archives, at its spring 1995 meeting, adopted a Position Paper, "The view of the archival community on the settling of disputed claims." It states, "Archival doctrine, which is founded on the principle of provenance . . excludes, on the one hand, the possibility of dismembering fonds, and on the other hand, the acquisition by any archive institution of fonds which do not fall within its jurisdiction." This is particularly important for indigenous peoples; as noted in Principle 14 above, the *United Nations Declaration on the Rights of Indigenous Peoples* affirms that indigenous peoples have the right to maintain their cultural property, including archives.

18. ***Institutions and archivists should cooperate with institutions and individuals in other countries to manage and settle claims about disputed displaced archives in a spirit of fairness and mutual respect. If returning displaced archives is likely to risk their destruction, their use for repressive purposes, or will place at risk persons whose actions are reflected in the archives, return should be postponed.***

In order to ease international conflicts on archives, UNESCO recommended the use of the concept of "common heritage," and the International Council on Archives endorsed it in the Position Paper cited in Principle 17 above. The first *Protocol to the Convention for the Protection of Cultural Property in the Event of Armed Conflict* (The Hague, 1954) requires parties "to prevent the exportation, from a territory occupied by it during an armed conflict, of cultural property," including archives. If, nonetheless, during armed conflicts cultural properties have been exported, the Convention requires parties to return them at the end of the conflict.

The UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects, signed in 1995, addresses the return of cultural materials, specifically including "archives, including sound, photographic and cinematographic archives." UNIDROIT provides time periods within which restitution can be sought and provides for "a claim for restitution of a sacred or communally important cultural object belonging to and used by a tribal or indigenous community in a Contracting State as part of that community's traditional or ritual use." Notwithstanding the Position Paper referenced in Principle 17 above and the UNIDROIT provisions, if returning the archives may endanger the life or fundamental freedoms of persons or lead to the destruction of the archives, then priority must be given to the protection of the rights of the persons mentioned in the archives and defer the return of the archives at the present time.

19. Institutions provide access to archives, including displaced archives, for transitional justice institutions and for persons, including victims and survivors of gross violations of human rights—regardless of their citizenship--who need them to seek compensation for previous damage to their human rights or to protect their fundamental rights.

Principle 15, "Measures for Facilitating Access to Archives," of the United Nations High Commissioner for Human Rights' *Updated Set of Principles to Combat Impunity* states in part: "Access to archives shall be facilitated in order to enable victims and persons related to claim their rights." Principle 16 "Cooperation between Archives Departments and the Courts and Non-judicial Commissions of Inquiry," of the United Nations High Commissioner for Human Rights' *Updated Set of Principles to Combat Impunity* reads in full: "The courts and non-judicial commissions of inquiry, as well as the investigators reporting to them, must have access to relevant archives. This principle must be implemented in a manner that respects applicable privacy concerns, including in particular assurances of confidentiality provided to victims and other witnesses as a precondition of their testimony. Access may not be denied on grounds of national security unless, in exceptional circumstances, the restriction has been prescribed by law; the Government has demonstrated that the restriction is necessary in a democratic society to protect a legitimate national security interest; and the denial is subject to independent judicial review."

IV. Education and Training

20. Governments, professional associations of archivists and records managers, archival and educational institutions and individual professionals engaged in archival education should ensure that archivists have appropriate education and training and are aware of the ethical duties of archivists with regard to human rights and fundamental freedoms recognized by national and international law.

The International Council on Archives' *Code of Ethics,* Principle 9, states, "Archivists should pursue professional excellence by systematically and continuously updating their archival knowledge, and sharing the results of their research and experience." It explains that archivists should "ensure that those whose training or activities they supervise are equipped to carry out their tasks in a competent manner." Because human rights and international humanitarian law evolve continuously, continued training in this area is essential.

21. Governments, professional associations of archivists and records managers, and archival and educational institutions should ensure that there is no discrimination against a person with respect to entry into or continued practice within the archival profession.

Discrimination as defined in the commentary to Principle 3, based on the areas proscribed by the *Universal Declaration of Human Rights,* may not be used in the employment of archivists.

22. ***In countries where there exist groups, communities or regions whose needs for archival services are not met, particularly where such groups have distinct cultures, traditions or languages or have been the victims of past discrimination, governments, professional associations of archivists and records managers, archival and educational institutions and individual professionals should take special measures to provide opportunities for persons from these groups to enter the archival profession and should ensure that they receive training appropriate to the needs of their groups.***

Many groups, communities and regions have insufficient archival services. The *United Nations Convention on the Rights of Persons with Disabilities* and the *United Nations Declaration on the Rights of Indigenous Peoples* underscore the need to provide opportunities to these specific groups.

V. Freedom of Expression and Association

23. ***Archivists and records managers, like other persons, are entitled to freedom of expression, belief, association and assembly. In particular, they have the right to take part in public discussion of matters concerning the promotion and protection of human rights and the professional responsibilities therefor. In exercising these rights, archivists do not divulge information that they obtained in the course of their professional responsibilities that has not been released by authorized officials for public use.***

Article 19 of the *Universal Declaration of Human Rights* states, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to see, received and impart information and ideas through any media and regardless of frontiers." Principle 8 of the International Council on Archives' *Code of Ethics* warns that archivists "should not reveal or use information gained through work with holdings to which access is restricted." This responsibility to maintain confidentiality continues after the archivist leaves archival employment. Principle 23 does not conflict with Principle 16 above, which refers to disclosure to limited pertinent authorities for the purposes of bringing wrongdoing to light, not to public discussion of such information.

24. ***Archivists and records managers are entitled to form and join self-governing professional associations to represent their interests, promote their continuing education and training, and protect their professional integrity. The executive body of the professional association should be elected by its members and should exercise its functions without external interference. Governments should recognize professional associations of archivists and records managers as civil society organizations that represent the interests of the profession and its practitioners.***

Article 20 of the *Universal Declaration of Human Rights* states, "Everyone has the right to freedom of peaceful assembly and association. No one may be compelled to belong to an association."

25. Professional associations of archivists and records managers should provide guidance and support for archivists handling archives with human rights aspects.

Principle 10 of the International Council on Archives' *Code of Ethics* states, "Archivists should promote the preservation and use of the world's documentary heritage, through working co-operatively with the members of their own and other professions." Providing assistance in handling the complex tasks associated with archives with human rights aspects is one area where working co-operatively surely is essential.

Annex 1. Definitions

In these *Principles*, the following definitions apply:

Archives. The documents created or received and accumulated by a person or institution in the course of the conduct of affairs, and preserved because of their continuing value. If the Principle means an institution whose primary work is the acquisition and preservation of historical archives, the Principle says "archival institution." The term is meant to include records.

Displaced archives. Archives that have been transferred to and are in the custody of a person or institution not legally entitled to them. They include archives that have been removed from the country in which they were originally accumulated and captured archives.

Institution. Any corporate body, public or private, governmental or non-governmental, including, for example, commercial businesses, faith-based organizations, national or sub-national governments, international and inter-governmental organizations, and organized political parties. This is equivalent to the ISAAR (CPF) definition of "corporate body," i.e., "an organization or group of persons that is identified by a particular name and that acts, or may act, as an entity." If the Principle refers to "government" it means to exclude other types of institutions; if a particular type of institution is meant, the Principle says "archival institution" or "educational institution."

Records. Recorded information in any form or medium, created or received and maintained, by an organization or person in the transaction of business or the conduct of affairs (definition from ISAD(G)). In the body of the *Principles*, "record" is used only in quotations; the preferred term in the Principles is "archives" and is meant to include records.

Transitional justice institutions. Entities created following a change in government from a more repressive to a more democratic regime. Transitional justice institutions may include special courts, truth commissions, and vetting and compensation panels.

Annex 2. Resources and References

Note: The following documents are available on line, generally in more than one language, with the exception of the proceedings of the ICA 1993-95 CITRA conferences (published only in paper, in English and French).

ASSOCIATION OF SOUTHEAST ASIAN NATIONS (ASEAN). *Human Rights Declaration (AHRD)* (2012)

COUNCIL OF EUROPE.

_____. *Convention for the Protection of Human Rights and Fundamental Freedoms* (also known as *European Convention on Human Rights*) (adopted in 1950).

_____. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (adopted in 1981)

_____. *Recommendation No. R (2000) 13 of the Committee of Ministers to member states on a European policy on access to archives* (adopted in 2000)

_____. *Recommendation Rec(2002)2 of the Committee of Ministers to member states on access to official documents* (adopted in 2002)

_____. *Convention on Access to Official Documents (2009, not yet in force).*

_____. *Recommendation CM/Rec(2014)7 of the Committee of Ministers to member States on the protection of whistleblowers* (adopted in 2014)

COUNCIL OF EUROPE'S PARLIAMENTARY ASSEMBLY (PACE). *Resolution 1954 (2013): National security and access to information* (2013)

INTERNATIONAL COUNCIL ON ARCHIVES.

_____. *The View of the Archival Community on Settling Disputed Archival Claims* (Position Paper adopted by the Executive Committee. Guangzhou, 10-13 April 1995).

_____. *Reference dossier on Archival Claims.* Documents collated by Hervé BASTIEN (1995).

_____. *Code of Ethics* (adopted in 1996)

_____. *CITRA 1993-1995. Interdependence of Archives. Proceedings of the Twenty-Ninth, Thirtieth and Thirty-First International Conference of the Round Table on Archives: XXIX Mexico 1993, XXX Thessaloniki 1994, XXXI Washington 1995*. Dordrecht: 1998 (special issue of *Janus*).

_____. *Universal Declaration on Archives* (adopted in 2010, endorsed by UNESCO in 2011)

_____. *Principles of Access to Archives* (adopted in 2012)

INTERNATIONAL INSTITUTE FOR THE UNIFICATION OF PRIVATE LAW (UNIDROIT). *Convention on Stolen or Illegally Exported Cultural Objects* (1995)

INTERNATIONAL MECHANISMS FOR PROMOTING FREEDOM OF EXPRESSION. *Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression* (2004)

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION.

_____. 15489. *Information and documentation – Records management* (2001)

_____. 16175. *Principles and Functional Requirements for Records in Electronic Office Environments* (2011)

_____. 30300. *Management systems for records* (2011)

ISLAMIC COUNCIL OF EUROPE. *Universal Islamic Declaration of Human Rights* (adopted in 1981).

LEAGUE OF ARAB STATES. *Arab Charter on Human Rights* (adopted in 2004)

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *G20, Whistleblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation* (2011)

ORGANISATION OF AFRICAN UNITY.

_____. *African Charter on Human and Peoples' Rights* (also known as the *Banjul Charter*) (adopted in 1981)

_____. *Declaration of Principles on Freedom of Expression in Africa*, adopted by the African Commission on Human and Peoples' Rights (2002).

_____. *Guidelines and Principles on Economic, Social and Cultural Rights in the African Charter on Human and Peoples' Rights* (2011)

ORGANIZATION OF AMERICAN STATES.

_____. *American Convention on Human Rights* (also known as *Pact of San Jose, Costa Rica*) (adopted in 1969)

_____. *Additional Protocol to the American Convention on Human Rights in the Area of Economic, Social and Cultural Rights* (also known as *Protocol of San Salvador*) (adopted in 1988).

_____. *Inter-American Convention on Forced Disappearance of Persons* (adopted in 1994)

_____. *Declaration of Principles on Freedom of Expression* (2000)

_____. *Inter-American Democratic Charter* (adopted in 2001).

_____. *Inter-American Convention against All Forms of Discrimination and Intolerance* (adopted in 2013)

_____. *Promotion and Protection of Human Rights in Business* (General Assembly Resolution, adopted at the second plenary session, held on June 4, 2014)

UNITED NATIONS.

Treaties

_____. *Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations the Laws and Customs of War on Land.* The Hague, 18 October 1907

_____. *Convention (IV) relative to the Protection of Civilian Persons in Time of War*. Geneva, 12 August 1949.

_____. *International Convention on the Elimination of All Forms of Racial Discrimination* (adopted in 1965)

_____. *International Covenant on Civil and Political Rights* (adopted in 1966); *Optional Protocol* (adopted in 1966); *Second Optional Protocol* (adopted in 1989)

_____. *International Covenant on Economic, Social and Cultural Rights* (adopted in 1966)

_____. *Convention on the Elimination of All Forms of Discrimination against Women* (adopted in 1979)

_____. *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* (adopted in 1984)

_____. *Convention on the Rights of the Child* (adopted in 1989)

_____. *International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families* (adopted in 1990)

_____. *Convention on the Rights of Persons with Disabilities* (adopted in 2006)

_____. *International Convention for the Protection of All Persons from Enforced Disappearance* (adopted in 2006)

United Nations General Assembly

_____. *Universal Declaration of Human Rights* (adopted 1948)

_____. *Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms* (adopted 1998)

_____. *Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law* (adopted 2005)

_____. *United Nations Declaration on the Rights of Indigenous Peoples* (adopted 2007)

United Nations Congress on the Prevention of Crime and the Treatment of Offenders. *Basic Principles on the Role of Lawyers* (adopted in 1990)

UNITED NATIONS HUMAN RIGHTS BODIES

_____. Commission on Human Rights. *The Administration of Justice and the Human Rights of Detainees Question of the impunity of perpetrators of human rights violations (civil and political).* Revised final report prepared by Mr. Joinet pursuant to sub-commission decision 1996/119 (1997)

_____. Commission on Human Rights. *Updated Set of Principles for the Protection and Promotion of Human Rights through Action to Combat Impunity.* E/CN.4/2005/102/Add.1. (2005)

_____. Office of the United Nations High Commissioner for Human Rights, *Rule of Law Tools for Post-Conflict States: Reparations Programmes* (2008)

_____. Human Rights Committee, *General comment No. 34 Article 19: Freedoms of opinion and expression* (2011)

_____. *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework* (endorsed by the Human Rights Council in 2011)

_____. *Report of the Office of the United Nations High Commissioner for Human Rights on the seminar on experiences of archives as a means to guarantee the right to the truth* (2011)

_____. Human Rights Council. *Report of the independent expert in the field of cultural rights, Farida Shaheed* (2011)

_____. Human Rights Council. *Resolution 21/7 Right to the Truth* (2012)

_____. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (2013)

_____. *The Right to Privacy in the Digital Age. Report of the Office of the United Nations High Commissioner for Human Rights* (2014)

_____. Office of the United Nations High Commissioner for Human Rights, *Rule of Law Tools for Post-Conflict States: Archives* (2015)

_____. Human Rights Council. *Report of the Special Rapporteur on the promotion of truth, justice, reparation and guarantees of non-recurrence, Pablo de Greiff* (2015)

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION (UNESCO)

Conventions

_____. *Convention for the Protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention* (The Hague, 14 May 1954) - *First Protocol*, The Hague, 14 May 1954; - *Second Protocol*, The Hague, 26 March 1999

_____. *Convention against Discrimination in Education Paris*, 14 December 1960

_____. *Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property* (1970)

_____. *Convention concerning the Protection of the World Cultural and Natural Heritage* (1972)

_____.*Convention for the Safeguarding of the Intangible Cultural Heritage* (2003)

_____. *Convention on the Protection and Promotion of the Diversity of Cultural Expressions* (2005)

Other UNESCO resources

KECSKEMÉTI Charles. *Archival claims. Preliminary study on the principles and criteria to be applied in negociations. / Les contentieux archivistiques: Étude préliminaire sur les principes et sur les critères à retenir lors des négociations*. Paris: UNESCO, 1977

GONZALEZ QUINTANA, Antonio, et al. *Archives of the security services of former repressive regimes: report prepared for UNESCO on behalf of the International Council of Archives.* Paris: UNESCO, 1995; revised by GONZALEZ QUINTANA as *Archival Policies in the Protection of Human Rights.* Paris: ICA, 2009

UNESCO. *Charter on the Preservation of Digital Heritage* (2003)

_____. *Declaration Concerning the Intentional Destruction of Cultural Heritage* (2003)

CIVIL SOCIETY STATEMENTS.

Johannesburg Principles on National Security, Freedom of Expression and Access to Information (1995)

*Global Principles on National Security and the Right to Information (*Tshwane Principles) (2013)

FRANCÉS 6)

HRWG ica
human rights working group
international council on archives
groupe de travail sur les droits de l'homme
conseil international des archives

CONSEIL INTERNATIONAL DES ARCHIVES

GROUPE DE TRAVAIL SUR LES DROITS DE L'HOMME

PRINCIPES DE BASE RELATIFS AU ROLE DES ARCHIVISTES ET DES GESTIONNAIRES DE DOCUMENTS POUR LA DEFENSE DES DROITS DE L'HOMME

Un document de travail du Conseil international des Archives

Septembre 2016

INTRODUCTION

Les archives sont utiles pour la défense des droits de l'Homme. Un grand nombre de ces documents sont essentiels pour garantir des droits et des prestations : dossiers de personnel, archives de programmes d'assurances sociales, dossiers de santé et de sécurité du travail, dossiers de service militaire. D'autres documents d'archives servent à prouver des droits civils : listes électorales, titres de propriété, dossiers de citoyenneté. D'autres encore constituent les preuves de violations des droits de l'Homme, comme les archives des unités militaires et policières et celles des services de renseignement des périodes de dictature, et même celles des prisons, des morgues et des cimetières.

Les archivistes et les gestionnaires de documents qui traitent des archives ayant des implications pour les droits de l'Homme ont à régler des problèmes juridiques concrets, des questions ayant trait à la politique sociale au sens large et des points de déontologie professionnelle personnelle. Dans beaucoup de pays, c'est un sujet complexe mais qui peut être traité en utilisant les bonnes pratiques professionnelles. Toutefois les archivistes et les gestionnaires de documents dans différentes situations et organismes peuvent subir des pressions quand ils essaient de gérer de telles archives. Ils peuvent se voir refuser l'accès aux documents à des fins de gestion ou d'évaluation, ils peuvent subir des pressions pour approuver l'élimination d'archives dont ils considèrent qu'elles ont des implications sur les droits de l'Homme, ils peuvent recevoir des instructions pour ne pas signaler l'existence de ces archives dans les instruments de travail, ils peuvent ne pas être en mesure d'entreprendre les actions de préservation nécessaires pour ces archives, ils peuvent ne pas être autorisés à prendre des décisions concernant l'accès public à ces archives ou à les communiquer à des chercheurs qualifiés. Et ils peuvent craindre des représailles s'ils cherchent à suivre les principes professionnels.

Tous les archivistes et les gestionnaires de documents cherchent à être soutenus par l'ensemble de la profession parce qu'ils s'efforcent de montrer la profession sous son jour le meilleur et le plus compétent quand ils traitent des archives importantes pour les droits de l'Homme. Le Conseil international des Archives a adopté un *Code de déontologie* en 1996, qui fournit un ensemble de paramètres éthiques conformément auxquels les archivistes effectuent leurs tâches professionnelles. La *Déclaration universelle des Archives*, adoptée par l'UNESCO en 2011, a proclamé l'intérêt des archives et du travail des archivistes et des gestionnaires de documents pour les peuples du monde. Ces documents importants fournissent un cadre général pour les responsabilités de la profession : cependant, le lien étroit entre archives et droits de l'Homme rend important le fait de clairement se concentrer sur les problèmes éthiques et pratiques qui ne sont mentionnés que d'une façon générale dans le Code et la Déclaration cadres.

Les *Principes de base relatifs au rôle des archivistes et des gestionnaires de documents pour la défense des droits de l'Homme* sont organisés en deux parties : un préambule et un ensemble de principes. Le préambule donne le contexte conceptuel des principes. Chaque principe est accompagné d'un texte explicatif qui n'en fait pas partie. Les principes sont regroupés en cinq sections. Les deux premières couvrent les fonctions archivistiques de base ; la troisième concerne la situation particulière du travail sur des archives susceptibles de documenter des actes répréhensibles et sur des archives déplacées ; les quatrième et cinquième sections sont consacrées au rôle et aux droits des archivistes et des gestionnaires de documents en tant que professionnels.

A la suite des *Principes* vient la définition des termes employés dans les *Principes* ainsi qu'une liste des traités internationaux, conventions, accords, opinions et autres textes qui servent de fondement aux *Principes*.

Principes de base relatifs au rôle des archivistes et des gestionnaires de documents pour la défense des droits de l'Homme

Préambule

Attendu que la mise en œuvre des droits de l'Homme et des libertés fondamentales auxquels chacun a droit conformément à la *Déclaration Universelle des droits de l'Homme,* au *Pacte international relatif aux droits civils et politiques* et à ses deux protocoles facultatifs, au *Pacte international relatif aux droits économiques, sociaux et culturels* et aux autres traités et instruments juridiques internationaux est renforcée par la préservation des archives et la capacité de chacun à y accéder,

Attendu que l'*Ensemble de principes actualisé pour la protection et la promotion des droits de l'homme par la lutte contre l'impunité* du Haut-Commissariat des Nations Unies aux droits de l'Homme affirme qu'il est de la responsabilité de l'Etat « de préserver les archives relatives aux violations des droits de l'Homme et du droit humanitaire et de permettre l'accès à ces archives », proclame que le droit de savoir, y compris de savoir ce qu'il y a dans les archives, est un droit individuel aussi bien que collectif et que l'Etat a un devoir de mémoire, et souligne l'importance des archives pour assurer que les personnes devront rendre des comptes tout en garantissant la défense équitable de toute personne inculpée d'une infraction pénale,

Attendu que les pouvoirs publics ont la responsabilité de promouvoir et de protéger le droit de chercher et de recevoir les informations comme condition fondamentale de la participation du public à la gouvernance,

Attendu que la protection adéquate des droits de l'Homme et des libertés fondamentales auxquels chacun a droit, qu'ils soient économiques, sociaux et culturels, ou civils et politiques, exige que chacun ait un accès effectif aux services archivistiques procurés par des professionnels indépendants,

Attendu que les associations professionnelles d'archivistes et de gestionnaires de documents ont un rôle vital à jouer en faisant respecter les normes et la déontologie professionnelles, en offrant des services archivistiques à tous ceux qui en ont besoin et en coopérant avec les organismes publics et autres pour poursuivre les objectifs de justice et d'intérêt général,

Attendu que la préservation des archives et l'accès aux archives ne peuvent être garantis que si toutes les parties concernées – institutions et particuliers – contribuent à de tels objectifs, selon leurs responsabilités respectives ;

Les *Principes de base sur le rôle des archivistes et des gestionnaires de documents pour la défense des droits de l'Homme*, énoncés ci-dessous, ont été formulés pour:

- aider les services qui conservent des archives à assurer le rôle spécifique des archivistes pour la défense des droits de l'Homme ;

- donner des lignes directrices aux archivistes et aux gestionnaires de documents qui, dans l'exercice de leur travail quotidien, doivent prendre des décisions qui pourraient affecter la mise en œuvre et la protection des droits de l'Homme ;
- apporter un soutien aux associations professionnelles d'archivistes et de gestionnaires de documents ;
- aider les responsables internationaux qui ont à traiter de questions liées aux droits de l'Homme à comprendre l'importance des questions couvertes par les *Principes* et la contribution que les archivistes et les gestionnaires de documents professionnels peuvent apporter à la protection des droits de l'Homme
-

Les Principes

I. Sélection et conservation des archives.

1. ***Les institutions, les archivistes et les gestionnaires de documents doivent mettre en place et maintenir des systèmes d'archivage qui protègent les archives documentant les droits de l'Homme et ils doivent faire en sorte que la gestion de ces archives préserve leur intégrité et leur valeur probatoire.***

Quel que soit leur format, les archives sont indispensables pour défendre les droits et les prérogatives ou pour permettre aux personnes de protester de façon efficace quand leurs droits sont violés, et elles doivent être gérées de façon rigoureuse depuis leur création pour assurer leur accessibilité et leur fiabilité. L'Organisation internationale de normalisation (ISO) a publié un certain nombre de normes qui répondent à ces exigences. ISO 15489, "Information et documentation – Records management", par exemple, établit les concepts et les principes clés pour la création, la capture et la gestion des archives.
En accord avec ISO 15489, la série des ISO 30300 constitue une approche systématique de la création et de la gestion des archives, centrée sur la mise en œuvre et le fonctionnement d'un système de gestion des documents d'activité effectif. Dans l'environnement numérique, ISO 16175 "Principles and Functional Requirements for Records in Electronic Office Environments" fournit les principes et les exigences fonctionnelles approuvés au niveau international pour les logiciels utilisés pour créer et gérer l'information numérique dans l'environnement de bureau. Les systèmes qui créent et gèrent les archives en rapport avec les droits de l'Homme doivent assurer que la preuve de l'authenticité de ces archives puisse être apportée, qu'elles sont exactes et fiables, complètes et sans altération, protégées contre un accès, une modification ou une destruction non autorisés, peuvent être trouvées en cas de besoin, et sont reliées à d'autres archives pertinentes. Les *Principes de tenue des enregistrements* d'ARMA International donnent des points de référence pour la gestion d'archives dans les secteurs public et privé.

2. ***Les institutions, les archivistes et les gestionnaires de documents doivent empêcher la destruction des archives qui sont susceptibles de contenir des preuves de violations des droits de l'Homme ou du droit humanitaire.***

Le principe n° 14, « Mesures pour la préservation des archives » de l'*Ensemble de principes actualisé pour la lutte contre l'impunité* du Haut-Commissariat des Nations Unies aux droits de l'Homme affirme que « Le droit de savoir implique que soient préservées les archives. Des mesures techniques et des sanctions pénales devraient être prises pour s'opposer à la soustraction, la destruction, la dissimulation ou la falsification des archives, notamment dans le but d'assurer l'impunité d'auteurs de violations des droits de l'homme et/ou du droit humanitaire. » Même s'il est possible qu'un archiviste ou un gestionnaire de documents ignore qu'un fonds d'archives contient des preuves de violations , cet archiviste ou ce gestionnaire de documents peut être capable de supposer, sur la base de la provenance des archives, qu'elles peuvent contenir de telles informations et ne doivent pas être détruites.

3. ***Les archivistes et les gestionnaires de documents doivent assurer la sélection, la collecte et la conservation des archives qui entrent dans le champ d'activités et le mandat de leur service d'archives, sans discrimination, conformément aux prescriptions de la Déclaration universelle des droits de l'Homme.***

L'article 2 de la *Déclaration universelle des droits de l'Homme* affirme que « Chacun peut se prévaloir de tous les droits et de toutes les libertés sans distinction aucune, notamment de race, de couleur, de sexe, de langue, de religion, d'opinion politique ou de toute autre opinion, d'origine nationale ou sociale, de fortune, de naissance ou de toute autre situation. » Les archivistes doivent s'assurer qu'ils collectent des archives qui couvrent de façon pertinente les activités de tous les groupes sociaux. Quelques services d'archives sont spécialisés, par exemple sur les archives d'organismes confessionnels, de communautés indigènes ou sur celles qui documentent des mouvements sociaux. Dans leurs programmes de collecte ces services font de la discrimination, conformément à leur mandat, mais, indépendamment de leur objectif particulier au sein de leur mandat, ils ne pratiquent pas d'exclusive.

4. ***Les archivistes et les gestionnaires de documents doivent examiner dans chaque décision d'évaluation l'utilité du fonds d'archives pour défendre ou identifier une revendication concernant des droits de l'Homme, aider à identifier les auteurs de violations de droits de l'Homme, permettre l'identification des personnes qui ont exercé des responsabilités qui pourraient les avoir impliquées dans des violations des droits de l'Homme, clarifier les événements qui ont conduit à la violation des droits de l'Homme, aider à connaître le sort de personnes disparues ou permettre à des particuliers de chercher à obtenir réparation pour des violations des droits de l'Homme commises dans le passé.***

Conformément aux concepts développés par l'*Ensemble de principes actualisé pour la lutte contre l'impunité* du Haut-Commissariat des Nations Unies aux droits de l'Homme, il est entendu que la justice transitionnelle exige de tenir les auteurs de violations pour responsables, d'assurer que les personnes qui ont commis des abus sous l'ancien régime ne soient pas en position de pouvoir dans le nouveau, de déterminer la vérité sur ce qui est arrivé à la société dans son ensemble, aux groupes au sein de la société et aux individus, et d'obtenir restitution et réparation. Des demandes similaires sont faites dans les états démocratiques à la suite d'activités de l'Etat qui ont provoqué des traumatismes pour les citoyens et, de plus en plus, des activités d'organismes privés qui violent les droits. Les archives sont essentielles dans ces processus.

Beaucoup d'autres fonds d'archives permettent de défendre les droits de l'Homme, depuis les registres d'état civil jusqu'aux titres de propriété, aux dossiers personnels du clergé, aux archives qui montrent les vérifications préalables (la diligence raisonnable) faites par une entreprise quand elle passe un contrat pour des marchandises, conformément aux exigences des *Principes directeurs relatifs aux entreprises et aux droits de l'Homme* des Nations Unies adoptés en 2011. Les archivistes et les gestionnaires de documents doivent être conscients des droits qui peuvent être défendus par les archives qu'ils gèrent.

5. ***Les pouvoirs publics doivent assurer la préservation des archives concernant les violations des droits de l'Homme et du droit humanitaire. Les pouvoirs publics et les organismes privés garantissent l'affectation des financements suffisants et des autres ressources permettant la gestion professionnelle des archives.***

Le principe n° 3, « Le devoir de mémoire » de l'*Ensemble de principes actualisé pour la lutte contre l'impunité* du Haut-Commissariat des Nations Unies aux droits de l'Homme affirme que « La connaissance par un peuple de l'histoire de son oppression appartient à son patrimoine et, comme telle, doit être préservée par des mesures appropriées au nom du devoir incombant à l'État de conserver les archives et les autres éléments de preuve se rapportant aux violations des droits de l'homme et du droit humanitaire et de contribuer à faire connaître ces violations. Ces mesures ont pour but de préserver de l'oubli la mémoire collective, notamment pour se prémunir contre le développement de thèses révisionnistes et négationnistes. »

Le principe ne dit pas que l'Etat ne doit préserver que les archives publiques ; il parle des « archives ». Un Etat a le choix entre plusieurs mesures pour encourager la préservation et l'accès aux archives privées, comme de faire des déclarations publiques convaincantes sur la préservation et l'accès, d'adopter une législation exigeant la préservation de ce type d'archives, d'obtenir des décisions de justice qui obligent à préserver des archives spécifiques, de donner des aides financières à des archives privées, de mener des enquêtes et de créer des bases de données pour permettre au public de savoir où se trouvent les archives pertinentes, d'accepter des donations d'archives du secteur privé ou de fournir un dépôt numérique fiable en lieu sûr pour les archives numériques menacées.

6. ***Les institutions, les archivistes et les gestionnaires de documents doivent assurer la protection et la préservation des archives des organismes temporaires établis pour assister la justice transitionnelle, pendant la durée de vie de l'organisme et après sa dissolution; toute élimination d'archives produites par ces organismes doit faire l'objet d'une information préalable.***

Le principe n° 5, « Garanties destinées à rendre effectif le droit de savoir » de l'*Ensemble de principes actualisé pour la lutte contre l'impunité* du Haut-Commissariat des Nations Unies aux droits de l'Homme dit notamment que : « Les sociétés qui ont connu des crimes odieux à grande échelle ou systématiques peuvent avoir intérêt notamment à ce qu'une commission de vérité ou qu'une commission d'enquête soit créée pour établir les circonstances entourant ces violations afin de faire jaillir la vérité et d'empêcher la disparition d'éléments de preuve. Qu'il se dote ou non d'un tel organe, un État doit être capable de préserver les archives relatives aux violations des droits de l'homme et du droit humanitaire et de permettre l'accès à ces archives. »

Les archives des institutions de la justice transitionnelle, qu'elles soient créées par les pouvoirs publics ou par des organisations privées, concernent les violations des droits de l'Homme et relèvent clairement de ce champ. Informer le public avant de détruire une partie de ces archives est une pratique établie dans des états tels que l'Espagne et les Etats-Unis, et donne au public l'occasion de s'opposer à l'élimination de certains fonds, ce qui est particulièrement important quand les archives sont le produit de ces institutions sensibles de la justice transitionnelle.

II. Donner accès à l'information dans les archives

7. ***Les archivistes doivent inclure dans la description de leurs fonds d'archives les informations qui, à leur connaissance, permettent aux usagers de comprendre si ces archives pourraient contenir des informations qui seraient utiles pour faire valoir une revendication en matière de droits de l'Homme, en particulier des informations qui concerneraient des violations graves***

des droits de l'Homme, qui aideraient à connaître le sort de personnes disparues ou pourraient permettre à des particuliers d'obtenir une indemnisation pour des violations des droits de l'Homme commises dans le passé.

Le principe n° 2 « Le droit inaliénable à la vérité » de l'*Ensemble de principes actualisé pour la lutte contre l'impunité* du Haut-Commissariat des Nations Unies aux droits de l'Homme affirme que, « Chaque peuple a le droit inaliénable de connaître la vérité sur les événements passés relatifs à la perpétration de crimes odieux, ainsi que sur les circonstances et les raisons qui ont conduit, par la violation massive ou systématique des droits de l'homme, à la perpétration de ces crimes. L'exercice plein et effectif du droit à la vérité constitue une protection essentielle contre le renouvellement des violations. » Le droit de connaître la vérité est aussi reconnu explicitement par la *Convention internationale pour la protection de toutes les personnes contre les disparitions forcées,* adoptée en 2010. La *Recommandation n° R (2000) 13 du Comité des ministres aux états membres sur une politique européenne en matière de communication des archives* explique "qu'un pays n'accède pleinement à la démocratie que lorsque chacun de ses habitants dispose de la possibilité de connaître de manière objective les éléments de son histoire." Une bonne description des archives favorise le droit à la vérité et renforce la démocratie.

8. ***Les archivistes et les gestionnaires de documents doivent organiser et décrire rapidement les archives figurant dans leurs fonds, afin de garantir aux usagers un accès égal, équitable et effectif ; ils organisent et décrivent en priorité les fonds d'archives qui documentent les violations graves des droits de l'Homme.***

Les services d'archives peuvent ne pas avoir un nombre suffisant d'archivistes pour donner une description rapide de tous leurs fonds d'archives. Quand ils décident quels fonds d'archives ils vont décrire en priorité, la question des droits de l'Homme doit être un élément clé à prendre en considération.

9. ***Les pouvoirs publics doivent assurer que les archives concernant les violations des droits de l'Homme et du droit humanitaire sont accessibles.***

L'article 19.2 du *Pacte international relatif aux droits civils et politiques* dit que « Toute personne a droit à la liberté d'expression; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations. »

La *Déclaration conjointe* de décembre 2004 du Rapporteur spécial des Nations Unies sur la liberté d'opinion et d'expression, du Représentant de l'Organisation pour la Sécurité et la Coopération en Europe chargé de la liberté des médias et du Rapporteur spécial sur la liberté d'expression de l'Organisation des Etats américains affirme que « Le droit d'accès à l'information détenue par les pouvoirs publics constitue un droit de l'Homme fondamental. »

Les *Principes globaux sur la sécurité nationale et le droit à l'information* (*Principes de Tshwane*) énoncent des lignes directrices sur la façon de garantir, dans la mesure du possible, l'accès public aux informations administratives tout en protégeant les intérêts légitimes de la sécurité nationale. Le Principe 10.A.1 affirme qu'« Il y a un intérêt primordial à révéler les informations concernant les violations flagrantes des droits de l'Homme ou les violations graves du droit international humanitaire, y compris les crimes de droit international, et les violations systématiques ou courantes des droits à la liberté et à la sécurité personnelles. La rétention de telles informations pour

des raisons de sécurité nationale, ne peut se justifier en aucun cas. » L'Assemblée parlementaire du Conseil de l'Europe a approuvé les *Principes de Tschwane* dans sa Résolution 1954 (2013) sur *La sécurité nationale et l'accès à l'information.*

10. Les archivistes et les gestionnaires de documents doivent défendre et soutenir le droit d'accès aux archives publiques et encourager les organisations non gouvernementales à offrir un accès similaire à leurs archives, conformément aux Principes d'accès aux archives adoptés par le Conseil international des archives.

Les dix *Principes d'accès* de l'ICA sont le fondement de ce principe. En outre, le principe n° 6 du *Code de déontologie* du Conseil international des Archives affirme que « Les archivistes facilitent l'accès aux archives du plus grand nombre possible d'utilisateurs et offrent leurs services avec impartialité à tous les usagers, » et la Déclaration universelle des Archives, approuvée par la Conférence générale de l'UNESCO en 2011, énonce que, « Les archives soient rendues accessibles à tous, dans le respect des lois en vigueur et des droits des personnes, des créateurs, des propriétaires et des utilisateurs. »

On trouve une exigence particulière en matière d'accès dans le principe n° 16: « Coopération des services d'archives avec les tribunaux et les commissions non judiciaires d'enquête » de l'*Ensemble de principes actualisé pour la lutte contre l'impunité* du Haut-Commissariat des Nations Unies aux droits de l'Homme qui affirme : « Les tribunaux et les commissions non judiciaires d'enquête, ainsi que les enquêteurs travaillant sous leur responsabilité, doivent avoir accès aux archives pertinentes. Ce principe doit être appliqué de façon à respecter les obligations qui conviennent en matière de respect de la vie privée, particulièrement les garanties de confidentialité données à des victimes ou à des témoins comme condition préalable à leur témoignage. L'accès ne peut être refusé pour des raisons de sûreté nationale à moins que, dans des circonstances exceptionnelles, cette restriction ait été prévue par la loi, que l'État ait démontré que cette restriction était nécessaire dans une société démocratique pour protéger un aspect légitime de la sûreté nationale et que le refus fasse l'objet d'un contrôle judiciaire indépendant. »

11. Les institutions et les archivistes doivent assurer que des garanties sont en place pour protéger les informations personnelles contre tout accès non autorisé, afin d'assurer le respect des droits, des libertés fondamentales et de la dignité des personnes auxquelles les informations se rapportent.

En plus des dispositions des *Principes d'accès*, le principe n° 7 du *Code de déontologie* du Conseil international des archives établit que « Les archivistes veillent à ce que la vie des personnes morales et des individus, ainsi que la sécurité nationale soient protégées sans qu'il soit besoin de détruire des informations, surtout dans le cas des archives informatiques où l'effacement des données et la réinscription sont pratique courante. Les archivistes veillent au respect de la vie privée des personnes qui sont à l'origine ou qui sont le sujet des documents, surtout pour celles qui n'ont pas été consultées pour l'usage ou le sort des documents. » L'ouverture sans réserve des archives peut entraîner la violation de la vie privée des individus et des représailles à leur égard. Les archivistes et les gestionnaires de documents cherchent à concilier le droit à la vérité avec le besoin de protéger la vie privée des personnes identifiables.

12. Les archivistes doivent offrir leurs services de références sans discrimination, conformément à la Déclaration universelle des droits de l'Homme. Chacun a le droit de demander l'assistance d'un archiviste pour l'aider à localiser et retrouver les documents qui peuvent lui permettre d'établir ses droits.

Comme il est affirmé ci-dessus par le principe n° 3, l'article 2 de la *Déclaration universelle des droits de l'Homme* énonce que chacun peut se prévaloir de tous les droits et de toutes les libertés « sans distinction aucune, notamment de race, de couleur, de sexe, de langue, de religion, d'opinion politique ou de toute autre opinion, d'origine nationale ou sociale, de fortune, de naissance ou de toute autre situation. »

Le principe n° 15, « Mesures facilitant l'accès aux archives" de l'*Ensemble de principes actualisé pour la lutte contre l'impunité* du Haut-Commissariat des Nations Unies aux droits de l'Homme affirme notamment que : « L'accès aux archives doit être facilité dans l'intérêt des victimes et de leurs proches pour faire valoir leurs droits… L'accès aux archives devrait également être facilité dans l'intérêt de la recherche historique, sous certaines restrictions raisonnables visant à préserver la vie privée et la sécurité des victimes et d'autres personnes. Les formalités d'autorisation régissant l'accès ne peuvent cependant pas être détournées à des fins de censure. »

Ce principe n'interdit pas les dispositions réglementaires concernant les personnes autorisées à utiliser les archives (telle que l'obligation d'avoir un certain âge ou la possibilité de voir son propre dossier sans que le public le puisse), mais il oblige les services à établir ces règles en s'efforçant de rendre l'accès aussi équitable et égal que possible.

13. Les archivistes doivent garantir l'accès aux archives aux personnes qui cherchent à se défendre contre des accusations de violations de droits de l'Homme.

Le principe n° 15 de l'*Ensemble de principes actualisé pour la lutte contre l'impunité* du Haut-Commissariat des Nations Unies aux droits de l'Homme prévoit aussi que l'accès aux archives doit être facilité « en tant que de besoin, pour les personnes mises en cause qui le demandent en vue d'assurer leur défense. » Les archivistes et les gestionnaires de documents ne doivent pas faire de distinction entre les accusateurs et les accusés quand ils donnent accès aux archives.

14. Les institutions, les associations professionnelles d'archivistes et de gestionnaires de documents, et les particuliers doivent promouvoir des programmes d'information du public sur le droit d'accès aux archives et le rôle important que jouent les archivistes pour la protection de leurs libertés fondamentales. Il faudra veiller particulièrement à informer les personnes défavorisées qu'elles peuvent demander l'assistance des archivistes pour localiser et retrouver les archives qui peuvent leur permettre de faire valoir leurs droits.

Le principe n° 3 des *Principes relatifs à l'accès aux archives* adoptés par le Conseil international des Archives, affirme que « Les institutions d'archives ont une attitude proactive en ce qui concerne l'accès aux archives. » Les besoins particuliers des usagers des archives doivent être pris en compte. En particulier, la *Convention des Nations Unies relative aux droits des personnes handicapées* déclare que les personnes handicapées ont droit à « la liberté de demander, recevoir et communiquer des informations et des idées, sur la base de l'égalité avec les autres et en recourant à tous moyens de communication de leur choix » et que les informations destinées au grand public doivent être communiquées aux personnes handicapées « sans tarder et sans frais supplémentaires

pour celles-ci, sous des formes accessibles et au moyen de technologies adaptées aux différents types de handicap. » De la même façon, la *Déclaration des Nations Unies sur les droits des peuples autochtones* affirme que les peuples autochtones ont le droit de conserver, de protéger et de développer les manifestations passées, présentes et futures de leur culture, y compris leurs archives ; pour atteindre ces objectifs , ils peuvent demander à être aidés pour localiser et reproduire ces archives.

III. Garanties spéciales

15. Les archivistes et les gestionnaires de documents qui, dans l'exercice de leurs activités professionnelles, découvrent des archives qu'ils croient, en toute bonne foi et pour des motifs raisonnables, contenir des preuves de violations graves des droits de l'Homme reconnus internationalement, qui (a) sont en cours ou (b) pour lesquelles des victimes pourraient rechercher des compensations, doivent informer les autorités compétentes de l'existence de ces archives.

a.) Les pouvoirs publics doivent fournir aux agents de l'Etat des canaux pour signaler de telles violations, soit de façon interne soit à des organes de contrôle.

b.) Les organisations non gouvernementales doivent fournir à leurs employés des canaux pour signaler des violations des droits de l'Homme ; si de tels canaux n'existent pas, les pouvoirs publics en mettent en place pour que les personnes qui ne sont pas agents de l'Etat puissent les signaler.

Les informations qui font apparaître des actes répréhensibles, qu'elles soient ou non disponibles actuellement pour le grand public, doivent être révélées aux autorités appropriées. Le principe n° 37 des *Principes globaux sur la sécurité nationale et le droit à l'information* suggère que les informations relatives aux catégories suivantes d'actes répréhensibles doivent être considérées comme relevant d'une « divulgation d'intérêt général » :

(a) crimes;
(b) violations des droits de l'Homme;
(c) violations du droit humanitaire international;
(d) corruption;
(e) menaces pour la santé et la sécurité du public ;
(f) danger pour l'environnement ;
(g) abus de pouvoir à un office public ;
(h) erreur judiciaire ;
(i) mauvaise gestion ou gaspillage des ressources ;
(j) représailles suite à la divulgation de l'une des catégories d'actes répréhensibles ci-dessus ;
(k) dissimulation délibérée d'un cas entrant dans l'une des catégories ci-dessus. »

Bien que les *Principes globaux* parlent spécifiquement d'informations publiques, il est clair que ces informations peuvent aussi se trouver dans les archives d'organisations non gouvernementales et dans celles de particuliers.

La question des canaux appropriés pour le signalement est difficile. Si l'organisme a un canal officiel de signalement et si l'archiviste ou le gestionnaire de documents ne risque pas de subir des représailles en y recourant, ce canal doit être utilisé en premier. Les organismes de contrôle indépendants ou les autorités judiciaires sont des canaux de signalement alternatifs ; si l'information ne peut être confiée à

aucun organisme au sein de l'Etat, l'archiviste ou le gestionnaire de documents peut s'adresser à des organisations officielles telles que le Haut-Commissariat aux droits de l'Homme des Nations Unies ou le Comité international de la Croix Rouge.

16. Les archivistes et les gestionnaires de documents qui révèlent des informations faisant apparaître des violations des droits de l'Homme ou du droit humanitaire international, que ces informations soient classifiées ou confidentielles pour d'autres raisons, ont le droit de signaler à une autorité appropriée toute mesure de représailles ou menace de représailles en relation avec la divulgation, pourvu que a) au moment de la divulgation, il ait eu des motifs raisonnables de penser que l'information révélée montrait des actes répréhensibles et b) qu'il ait au préalable essayé d'utiliser tout mécanisme interne de signalement existant, pour autant que cet acte n'ait pas augmenté le risque de représailles.

Les pouvoirs publics doivent avoir des lois qui protègent contre les représailles les personnes qui divulguent des informations concernant des actes répréhensibles tels que définis dans le principe n° 15 ci-dessus. La résolution 1954 (2013) de l'Assemblée parlementaire du Conseil de l'Europe sur *la sécurité nationale et l'accès à l'information* affirme que « Toute personne qui signale des abus dans l'intérêt général (donneur d'alerte) doit être protégée de tout type de représailles, dans la mesure où il ou elle a agi de bonne foi et a suivi les procédures applicables. » Le comité des ministres du Conseil de l'Europe est allé dans le même sens dans sa Recommandation aux Etats membres CM/Rec (2014)7 sur la *protection des lanceurs d'alerte.*

Comme le suggère le principe n° 40 des *Principes globaux sur la sécurité nationale et le droit à l'information*, « En cas de contestation, la personne peut être amenée à défendre le caractère raisonnable de sa conviction et, en dernier recours, il revient à un tribunal indépendant de déterminer si ce critère est satisfait et permet donc de considérer la divulgation comme protégée. » Comme dans le cas du principe n° 15, le signalement des représailles doit être fait d'abord aux autorités nationales mais il peut être porté à la connaissance des autorités internationales si l'on croit qu'il n'y a pas de protection nationale disponible ou sûre.

17. Les institutions, les archivistes et les gestionnaires de documents doivent respecter le patrimoine culturel et juridique des nations et des communautés, et ne collectent pas d'archives qui n'entrent pas dans leur champ de compétences. Les politiques d'acquisition des institutions doivent respecter le droit des communautés à écrire leur propre histoire.

Le comité exécutif du Conseil international des archives a adopté, lors de sa réunion du printemps 1995, un document de principe sur le point de vue de la communauté des archivistes concernant le règlement des contentieux. Il affirme que la doctrine archivistique, qui est fondée sur le principe de provenance, exclut, d'une part, la possibilité de démembrement des fonds, et, d'autre part, la collecte par tout service d'archives de fonds qui ne relèvent pas de ses compétences. Cela est particulièrement important pour les peuples autochtones ; comme il est noté dans le principe n° 14 ci-dessus, la *Déclaration des Nations Unies sur les droits des peuples autochtones* affirme que les peuples autochtones ont le droit de conserver leurs biens culturels, y compris les archives.

18. Les institutions et les archivistes doivent coopérer avec les institutions et les particuliers d'autres pays pour gérer et régler les revendications concernant des contentieux portant sur des archives déplacées, dans un esprit d'impartialité et de respect mutuel. Si le retour de ces archives déplacées risque d'entraîner leur destruction, leur utilisation à des fins répressives

ou la mise en danger des personnes dont les activités sont reflétées dans les archives, le retour devra être différé.

Afin de faciliter le règlement des conflits internationaux sur les archives, l'UNESCO a recommandé d'utiliser le concept de « patrimoine commun » et le Conseil international des Archives l'a retenu dans son document de principe cité au principe n° 17 ci-dessus. Le premier *Protocole à la Convention pour la protection des biens culturels en cas de conflit armé* (La Haye, 1954) exige de chacune des parties « d'empêcher l'exportation de biens culturels d'un territoire occupé par elle lors d'un conflit armé », y compris les archives. Si, néanmoins, les biens culturels ont été exportés pendant les conflits armés, la Convention exige des parties leur restitution à la fin du conflit.

La Convention d'UNIDROIT sur les biens culturels volés ou illicitement exportés, signée en 1995, traite de la restitution des biens culturels, et inclut spécifiquement « les archives, y compris les archives phonographiques, photographiques et cinématographiques ». UNIDROIT prévoit des périodes pendant lesquelles on peut chercher à obtenir leur restitution et prévoit « l'action en restitution d'un bien culturel sacré ou revêtant une importance collective appartenant à, et utilisé par, une communauté autochtone ou tribale dans un Etat contractant pour l'usage traditionnel ou rituel de cette communauté. » Malgré le document de principe référencé au principe n° 17 ci-dessus et les dispositions d'UNIDROIT, si le retour des archives peut mettre en danger la vie ou les libertés fondamentales de personnes ou entraîner la destruction des archives, la priorité doit alors être donnée à la protection des droits des personnes mentionnées dans les archives et le retour des archives doit être différé pour le moment.

19. Les institutions rendent les archives, y compris les archives déplacées, accessibles aux organismes de la justice transitionnelle et aux personnes, y compris les victimes et les rescapés de graves violations des droits de l'Homme, qui, quelle que soit leur nationalité, en ont besoin pour obtenir compensation pour des atteintes antérieures à leurs droits de l'Homme ou pour protéger leurs droits fondamentaux. I

Le principe n° 15, « Mesures pour faciliter l'accès aux archives » de l'*Ensemble de principes actualisé pour la lutte contre l'impunité* du Haut-Commissariat des Nations Unies aux droits de l'Homme dit notamment : « L'accès aux archives doit être facilité dans l'intérêt des victimes et de leurs proches pour faire valoir leurs droits. » Le principe n° 16, "Coopération des services d'archives avec les tribunaux et les commissions non judiciaires d'enquête de l'*Ensemble de principes actualisé pour la lutte contre l'impunité* du Haut-Commissariat des Nations Unies aux droits de l'Homme dispose en totalité que : « Les tribunaux et les commissions non judiciaires d'enquête, ainsi que les enquêteurs travaillant sous leur responsabilité, doivent avoir accès aux archives pertinentes. Ce principe doit être appliqué de façon à respecter les obligations qui conviennent en matière de vie privée, particulièrement les garanties de confidentialité données à des victimes ou à des témoins comme condition préalable à leur témoignage. L'accès ne peut être refusé pour des raisons de sûreté nationale à moins que, dans des circonstances exceptionnelles, cette restriction ait été prévue par la loi, que l'Etat ait démontré que cette restriction était nécessaire dans une société démocratique pour protéger un aspect légitime de la sûreté nationale et que le refus fasse l'objet d'un contrôle judiciaire indépendant. »

IV. Formation initiale et continue

20. Les pouvoirs publics, les associations professionnelles d'archivistes et de gestionnaires de documents, les services d'archives et les établissements d'enseignement, ainsi que les professionnels engagés dans la formation archivistique doivent assurer que les archivistes ont une formation initiale et continue appropriée et ont connaissance des devoirs déontologiques des archivistes en ce qui concerne les droits de l'Homme et les libertés fondamentales reconnus par le droit national et international.

Le principe n° 9 du *Code de déontologie* du Conseil international des Archives établit que « Les archivistes cherchent à atteindre le meilleur niveau professionnel en renouvelant systématiquement et continuellement leurs connaissances archivistiques et en partageant les résultats de leurs recherches et de leur expérience. » Il explique que les archivistes doivent « veiller à ce que les personnes qu'il leur appartient de former et d'encadrer exercent leurs tâches avec compétence. » Etant donné que les droits de l'Homme et le droit humanitaire international évoluent en permanence, la formation continue dans ce domaine est essentielle.

21. Les pouvoirs publics, les associations professionnelles d'archivistes, les services d'archives et les établissements d'enseignement doivent garantir l'absence de discrimination envers une personne en ce qui concerne son admission ou l'exercice permanent de ses fonctions au sein de la profession des archivistes.

La discrimination telle qu'elle est définie dans le commentaire du principe n° 3, sur la base des domaines proscrits par la *Déclaration universelle des droits de l'Homme*, ne doit pas être utilisée dans l'emploi des archivistes.

22. Dans les pays où il existe des groupes, communautés ou régions dont les besoins en services archivistiques ne sont pas satisfaits, en particulier là où de tels groupes ont des cultures, des traditions ou des langues différentes ou ont été victimes de discriminations dans le passé, les pouvoirs publics, les associations professionnelles d'archivistes et de gestionnaires de documents, les services d'archives et les établissements d'enseignement ainsi que les professionnels doivent prendre des mesures spéciales pour donner la possibilité aux personnes de ces groupes d'entrer dans la profession des archivistes et ils doivent leur assurer la formation répondant aux besoins de leurs groupes.

De nombreux groupes, communautés et régions ont des services d'archives insuffisants. La *Convention des Nations Unies relative aux droits des personnes handicapées* et la *Déclaration des Nations Unies sur les droits des peuples autochtones* soulignent le besoin d'ouvrir des possibilités à ces groupes spécifiques.

V. Liberté d'expression et d'association

23. Les archivistes et les gestionnaires de documents ont, comme les autres personnes, droit à la liberté d'expression, de croyance, d'association et de réunion. Ils ont en particulier le droit de prendre part à des discussions publiques sur des questions concernant la promotion et la protection des droits de l'Homme et les responsabilités professionnelles qui en découlent. En exerçant ces droits, les archivistes ne divulguent pas les informations obtenues dans l'exercice

de leurs responsabilités professionnelles qui n'ont pas été rendues publiques par les responsables autorisés à le faire.

L'article 19 de la *Déclaration universelle des droits de l'Homme* dispose que, « Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit. » Le principe n° 8 du *Code de déontologie* du Conseil international des Archives prévient que les archivistes « ne révèlent ni n'utilisent les informations qu'ils ont pu obtenir par leur travail dans les fonds d'archives dont l'accès est limité. » Cette obligation de confidentialité continue à s'imposer après que l'archiviste a quitté son emploi dans les archives. Le principe n° 23 n'entre pas en conflit avec le principe n° 16 ci-dessus qui se réfère à la divulgation d'informations à un petit nombre d'autorités pertinentes dans le but de révéler des actes répréhensibles, et non de discuter en public de telles informations.

24. Les archivistes et les gestionnaires de documents ont le droit de former des associations professionnelles autonomes et d'y adhérer pour représenter leurs intérêts, promouvoir leur formation continue et leur perfectionnement, et protéger leur intégrité professionnelle. L'organe exécutif de l'association professionnelle doit être élu par ses membres et exercera ses fonctions sans interférence extérieure. Les pouvoirs publics doivent accepter les associations professionnelles d'archivistes et de gestionnaires de documents en tant qu'organisations de la société civile qui représentent les intérêts de la profession et de ses praticiens.

L'article 20 de la *Déclaration universelle des droits de l'Homme* affirme que « Toute personne a droit à la liberté de réunion et d'association pacifiques. Nul ne peut être obligé de faire partie d'une association. »

25. Les associations professionnelles d'archivistes et de gestionnaires de documents doivent fournir des lignes directrices et apporter leur soutien aux archivistes qui traitent des archives concernant les droits de l'Homme.

Le principe n°10 du *Code de déontologie* du Conseil international des archives affirme que « Les archivistes travaillent en collaboration avec leurs collègues et les membres des professions voisines afin d'assurer universellement la conservation et l'exploitation du patrimoine documentaire. » Fournir de l'aide dans le traitement des tâches complexes induites par les archives qui concernent les droits de l'Homme est un domaine dans lequel le travail en collaboration est sans aucun doute essentiel.

Annexe 1. Glossaire

Dans ces *Principes*, les définitions suivantes s'appliquent :

Archives*. Documents créés ou reçus et accumulés par une personne ou une institution dans l'exercice de ses activités, et conservés en raison de leur valeur permanente. Si le principe vise une institution dont la tâche de base est la collecte et la préservation d'archives historiques, le principe parle de « service d'archives. »

Archives déplacées. Archives qui ont été versées et qui sont sous la garde d'une personne ou d'une institution qui ne sont pas juridiquement habilités à le faire. Cette définition comprend les archives qui ont été emportées du pays dans lequel elles ont été originellement accumulées et saisies.

Institution. Tout organisme, public ou privé, gouvernemental ou non gouvernemental, y compris, par exemple, les entreprises commerciales, les organisations confessionnelles, les autorités publiques nationales ou locales, les organisations internationales et intergouvernementales et les partis politiques organisés. C'est l'équivalent de la définition de « collectivité » de l'ISAAR (CPF), c'est-à-dire, « Toute organisation ou groupe de personnes identifié par un nom particulier ou qui agit ou peut agir en tant qu'entité. » Si le principe se réfère aux « pouvoirs publics », il vise à exclure les autres types d'institutions; s'il veut désigner un certain type d'institution, le principe parle de « service d'archives » ou « d'établissement d'enseignement ».

Institutions de la justice transitionnelle: Instances créées après un changement de gouvernement et passage d'un régime plus répressif à un régime plus démocratique. Les institutions de la justice transitionnelle peuvent inclure des tribunaux spéciaux, des commissions de vérité et des instances de criblage (*vetting*) et de compensation.

*Le terme «Records» de la version anglaise n'a pas été traduit car, la langue française n'a pas de mot équivalent. Quand ce terme est utilisé dans la version anglaise, il est traduit par les mots «archives», «documents» ou «dossiers» selon le contexte de la phrase.

Annexe 2. Ressources et références

Note: Les documents suivants sont accessibles en ligne, généralement dans plus d'une langue, à l'exception des actes des conférences de la CITRA 1993-1995 de l'ICA (publiés uniquement sur papier, en anglais et en français).

ASSOCIATION DES NATIONS DES PAYS DE L'ASIE DU SUD-EST (ASEAN). *Déclaration des droits humains (AHRD)* (2012)

CONSEIL DE L'EUROPE.

_____. *Convention pour la protection des droits de l'Homme et des libertés fondamentales (*connue aussi comme *Convention des droits de l'Homme)* (adoptée en 1950).

_____. *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* (adoptée en1981).

_____. *Recommandation n° R (2000) 13 du Comité des ministres aux états membres sur une politique européenne en matière de communication des archives* (adoptée en 2000).

_____. *Recommandation Rec(2002)2 du Comité des ministres aux états membres sur l'accès aux documents publics* (adoptée en 2002)

_____. *Convention sur l'accès aux documents publics (*2009, pas encore en vigueur).

_____. *Recommandation CM/Rec(2014)7 du Comité des ministres aux états membres sur la protection des lanceurs d'alerte* (adoptée en 2014)

ASSEMBLÉE PARLEMENTAIRE DU CONSEIL DE L'EUROPE (PACE). *Résolution 1954 (2013): Sécurité nationale et accès à l'information* (2013)

CONSEIL INTERNATIONAL DES ARCHIVES.

_____. *The View of the Archival Community on Settling Disputed Archival Claims* (Document de principe adopté par le Comité exécutif, Guangzhou, 10-13 avril 1995).

_____. *Dossier de référence sur les contentieux archivistiques.* Documents rassemblés par Hervé Bastien (1995).

_____. *Code de déontologie* (adopté en 1996)

_____. *CITRA 1993-1995. Interdépendance des Archives, Actes des vingt-neuvième, trentième et trente et unième Conférences internationales de la Table Ronde des Archives: XXIX Mexico 1993, XXX Thessalonique1994, XXXI Washington 1995*. Dordrecht: 1998 (numéro spécial de *Janus*).

_____. *Déclaration universelle des Archives* (adoptée en 2010, approuvée par l'UNESCO en 2011)

_____. *Principes d'accès aux archives* (adoptés en 2012)

INSTITUT INTERNATIONAL POUR L'UNIFICATION DU DROIT PRIVÉ (UNIDROIT). *Convention sur les biens culturels volés ou illicitement exportés* (1995)

ISLAMIC COUNCIL OF EUROPE. *Universal Islamic Declaration of Human Rights* (adoptée en 1981).

LIGUE DES ETATS ARABES. *Charte arabe des droits de l'Homme* (adoptée en 2004)

MÉCANISMES INTERNATIONAUX POUR LA PROMOTION DE LA LIBERTÉ D'EXPRESSION. *Déclaration conjointe du Rapporteur spécial des Nations Unies sur la liberté d'opinion et d'expression, du Représentant de l'OSCE chargé de la liberté des medias et du Rapporteur spécial de l'OEA sur la liberté d'expression* (2004)

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ECONOMIQUES (OCDE). *G20, Whistleblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation* (2011)

ORGANISATION INTERNATIONALE DE NORMALISATION.

_____. 15489. *Information et documentation – Records management* (2001)

_____. 16175. *Principles and Functional Requirements for Records in Electronic Office Environments* (2011)

_____. 30300. *Management systems for records* (2011)

ORGANISATION DE L'UNITÉ AFRICAINE.

_____. *Charte africaine des droits de l'Homme et des peuples* (connue aussi comme *Charte de Banjul*) (adoptée en 1981)

_____. *Déclaration de principes sur la liberté d'expression en Afrique*, adoptée par la Commission africaine des droits de l'Homme et des peuples (2002).

_____. *Directives et principes sur les droits économiques, sociaux et culturels dans la Charte africaine des droits de l'Homme et des peuples* (2011)

ORGANISATION DES ETATS AMÉRICAINS.

_____. *Convention américaine des droits de l'Homme* (connue aussi comme *Pacte de San José, Costa Rica*) (adoptée en 1969)

_____. *Protocole additionnel à la Convention américaine relative aux droits de l'Homme traitant des droits économiques, sociaux et culturels,* (connu aussi comme *Protocole de San Salvador*) (adopté en 1988).

_____. *Convention interaméricaine sur la disparition forcée des personnes* (adoptée en 1994)

_____. *Déclaration de principes sur la liberté d'expression* (2000)

_____. *Charte démocratique interaméricaine* (adoptée en 2001).

_____. *Convention interaméricaine contre toutes les formes de discrimination et d'intolérance* (adoptée en 2013)

_____. *Promotion et protection des droits de l'Homme dans les entreprises* (Résolution de l'Assemblée générale, adoptée à la seconde séance plénière, tenue le 4 juin 2014)

NATIONS UNIES.

Traités.

_____. *Convention (IV) concernant les lois et coutumes de la guerre sur terre et son Annexe: Règlement concernant les lois et coutumes de la guerre sur terre.* La Haye, 18 octobre 1907

_____. *Convention (IV) relative à la protection des populations civiles en temps de guerre*. Genève 12 août 1949.

_____. *Convention internationale sur l'élimination de toutes les formes de discrimination raciale* (adoptée en 1965)

_____. *Pacte international relatif aux droits civils et politiques* (adopté en 1966); *Protocole facultatif* (adopté en 1966); *Second Protocole facultatif* (adopté en 1989)

_____. *Pacte international relatif aux droits économiques, sociaux et culturels* (adopté en 1966)

_____. *Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes* (adoptée en 1979)

_____. *Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants* (adoptée en 1984)

_____. *Convention sur les droits des enfants* (adoptée en 1989)

_____. *Convention internationale sur la protection des droits des travailleurs migrants et des membres de leur famille* (adoptée en 1990)

_____. *Convention relative aux droits des personnes handicapées* (adoptée en 2006)

_____. *Convention internationale pour la protection de toutes les personnes contre les disparitions forcées* (adoptée en 2006)

Assemblée générale des Nations Unies.

_____. *Déclaration universelle des droits de l'Homme* (adoptée en1948)

_____. *Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnus* (adoptée en 1998)

_____. *Principes fondamentaux et directives des Nations Unies concernant le droit à un recours et à réparation des victimes de violations flagrantes du droit international des droits de l'homme et de violations graves du droit international humanitaire* (adoptés en 2005)

_____. *Déclaration des Nations Unies sur les droits des peuples indigènes* (adoptée en 2007)

Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants.

_____. *Principes de base sur le rôle du barreau* (adoptés en 1990)

ORGANISMES DES DROITS DE L'HOMME DES NATIONS UNIES

_____. Commission des droits de l'Homme. *L'administration de la justice et les droits de l'Homme des détenus. Question de l'impunité des auteurs de violations des droits de l'Homme (civils et politiques).* Rapport final établi par M. L. Joinet, en application de la décision 1996/119 de la Sous-Commission (1997)

_____. Commission des droits de l'Homme. *Ensemble de principes actualisé pour la protection et la promotion des droits de l'Homme par la lutte contre l'impunité.* E/CN.4/2005/102/Add.1. (2005)

_____. Haut-Commissariat aux droits de l'Homme, *Rule of Law Tools for Post-Conflict States: Reparations Programmes* (2008)

_____. Comité des droits de l'Homme, *Observation générale n° 34. Article 19: Libertés d'opinion et d'expression* (2011)

_____. *Principes directeurs relatifs aux entreprises et aux droits de l'Homme : mise en œuvre du cadre de référence «protéger, respecter et réparer» des Nations Unies* (adoptés par le Conseil des droits de l'Homme en 2011)

_____. *Rapport du Haut-Commissariat des Nations Unies aux droits de l'Homme sur le séminaire concernant différentes expériences en matière d'archives en tant que moyen de garantir le droit à la vérité* (2011)

_____. Conseil des droits de l'Homme. *Rapport de la Rapporteuse spéciale dans le domaine des droits culturels, Farida Shaheed* (2011)

_____. Conseil des droits de l'Homme. *Résolution 21/7 Le droit à la vérité* (2012)

_____. *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression* (2013)

_____. *The Right to Privacy in the Digital Age. Rapport du Haut-Commissariat des Nations Unies aux droits de l'Homme* (2014)

_____. Haut-Commissariat aux droits de l'Homme, *Rule of Law Tools for Post-Conflict States: Archives* (2015)

_____. Conseil des droits de l'Homme. *Rapport du Rapporteur spécial sur la promotion de la vérité, de la justice, de la réparation et des garanties de non-répétition, Pablo de Greiff,* (2015)

ORGANISATION DES NATIONS UNIES POUR L'EDUCATION, LES SCIENCES ET LA CULTURE (UNESCO)

Conventions

_____. *Convention pour la protection des biens cuturels en cas de conflit armé avec Règlement d'exécution* (La Haye, 14 mai 1954) – *Protocole*, La Haye, 14 mai 1954; - *Second Protocole*, La Haye, 26 mars 1999

_____. *Convention concernant la lutte contre la discrimination dans le domaine de l'enseignement,* Paris, 14 décembre *1960*

_____. *Convention concernant les mesures à prendre pour interdire et empêcher l'importation, l'exportation et le transfert de propriété illicites des biens culturels* (1970)

_____. *Convention concernant la protection du patrimoine mondial culturel et naturel* (1972)

_____. *Convention pour la sauvegarde du patrimoine culturel immatériel* (2003)

_____. *Convention sur la protection et la promotion de la diversité des expressions culturelles* (2005)

Autres ressources de l'UNESCO

KECSKEMÉTI Charles. *Archival claims. Preliminary study on the principles and criteria to be applied in negociations. / Les contentieux archivistiques: Étude préliminaire sur les principes et sur les critères à retenir lors des négociations*. Paris: UNESCO, 1977

GONZALEZ QUINTANA, Antonio, et al. *Archives of the security services of former repressive regimes: report prepared for UNESCO on behalf of the International Council of Archives.* Paris: UNESCO, 1997; révisé par Antonio GONZALEZ QUINTANA sous le titre *Politiques archivistiques pour la protection des droits de l'Homme.* Paris: ICA, 2009

UNESCO. *Charte sur la préservation du patrimoine numérique* (2003)

_____. *Déclaration concernant la destruction intentionnelle du patrimoine culturel* (2003)

DECLARATIONS DE LA SOCIÉTÉ CIVILE

Principes de Johannesburg sur la sécurité nationale, la liberté d'expression et l'accès à l'information (1995)

Principes globaux sur la sécurité nationale et le droit à l'information (Principes de Tshwane) (2013)