1. Introduction

A substantial part of the information that we create and process in everyday life exists in digital form only. The major difference between such information, e.g. represented in data stored on a hard drive, and the information embodied in the text on the printed page of a book, is that the latter information is directly accessible for us as human beings.[1] In order to perceive the information represented in the digital object, however, we are in need of additional means. For the correct rendering of a book stored in the PDF format, for instance, it will first of all be necessary to be in possession of the right software. The execution of that software presupposes the corresponding operating system, which then in turn necessitates a certain hardware configuration to run properly.

Over time, all of these layers are prone to errors that can lead to the loss of data and thus information.[2] One reason for data loss is the obsolescence or destruction of data carriers or reader devices.[3] As technological progress in this area moves at a particularly rapid pace, another cause that can render the content of a digital object inaccessible is the obsolescence of the corresponding software or data format.[4] The loss of information represented in data might, moreover, occur despite of the availability of a functioning data carrier and reader device, when context that is needed to interpret the data properly is not (or no longer) available. In the case of text documents, the context information regarding the alphabet, text direction or character encoding used (e.g. Unicode) might not be available when trying to recover information from the document in the future. Encryption can constitute a further obstacle, if the decryption information is lost.[5]

---

[1] Cf. Borghoff, Rödig, Scheffczyk and Schmitz 2006: 489.

[2] For an introduction to the threats to the preservation of digital objects see Kuny 1998: 8–13.

[3] E.g. the example of the BBC's problems with the recovery/loss of data stored on contemporarily obsolete videodisk technology in the course of the Domesday Book project. For more detail see Charlesworth 2012: 19.

[4] Becker and Rauber 2007.

[5] Risak 2003: 238.

The first of the two most promising approaches towards keeping electronically stored information safe for the future is being referred to as *migration*, which can be defined as: 'A means of overcoming technological obsolescence by transferring digital resources from one hardware/software generation to the next'.[6] The second means of overcoming such technological obsolescence is *emulation*, which focuses on 'developing techniques for imitating obsolete systems on future generations of computers'.[7]

It is one of the goals of the TIMBUS project to take digital preservation into the business domain, whereby existing digital preservation knowledge[8] is applied to business processes. These efforts serve the goal of being able to recover, for instance, a production process at any given time in the future without the loss of either time or information. The phases that are necessary to preserve and later on recover information represented in business processes and digital objects, respectively, can be summarized into three gross categories: expediency, execution and exhumation. In the course of the *expediency* or preservation planning phase, the feasibility of digital preservation for a concrete entity is evaluated. A risk management approach is taken, whereby the critical business processes, but also the boundaries to the envisioned preservation solution, set, inter alia, by intellectual property rights or data protection laws, are identified. Furthermore, the significant characteristics of the identified business processes that need to be maintained over time are defined. The *execution* phase refers to the actual implementation of the previously developed preservation plan. It also encompasses the setting up and optimizing of IT contracts needed to balance the interest of the stakeholders involved in the preservation efforts. Lastly, the *exhumation* or redeployment phase comprises all steps necessary to rerun business processes in a new environment in the future. The verification of the correct behaviour of the redeployed processes forms an integral part thereof.

---

[6] Jones and Beagrie 2008: 26.

[7] *Ibid*. 25.

[8] For an overview of current research projects dealing with digital preservation issues, see Strodl, Petrov and Rauber 2011.