Transparent Government

Parliamentary and Legal Accountability in an Information Age

A.J. Meijer, Transparent government: Parliamentary and legal accountability in an information age, *Information Polity*, Vol. 8, Nrs. 1 & 2, 2003, pp. 67 – 78.

Abstract

There are several indications that the (long-term) memory of electronic government is in danger and that this decline in organizational memory may have important negative effects on accountability. Case study research in the Netherlands, however, highlights the positive effects of the use of information and communication technologies for parliamentary and legal accountability. Although technological safeguards for authenticity may be lacking and data may not always be preserved in a durable way, parliamentary and legal fact-finding is generally facilitated. The use of ICTs leads to more informational and analytical transparency of government organizations: more data is recorded and there are also more ways to retrieve this data. This increased transparency is an unintentional effect of efforts to improve the support and management of business processes.

Transparent Government

Parliamentary and Legal Accountability in an Information Age

1. Government without a (digital) memory?

The (long-term) memory of electronic government may be in danger. For one thing, electronic data cannot be read if required software is no longer available [1]. Furthermore, government organizations may not consider it important to preserve electronic messages [2][3]. Thirdly, the use of databases may lead to an increased focus on up-to-date data at the expense of historical data [4]. Thus there seems to be evidence that digital memories may not function as well as paper memories. This decline in organizational memory may have important negative effects on parliamentary and legal accountability. An example can illustrate these problems.

Databases of the Canadian Forces

In 1996, a Canadian Parliamentary Committee investigated the deployment of Canadian Forces to Somalia. The committee held interviews, studied documents, and also requested access to the National Defence Operation Centre (NDOC) logs. These logs were maintained in an automated database and contained a record of all message traffic coming into National Defence headquarters from Canadian Forces' theatres of operation. This database, however, showed some anomalies, including entries containing no information, missing serial numbers and entries with duplicate serial numbers. The committee was concerned that there might have been deliberate tampering with the data and could not exclude this possibility because of the absence of standard operating procedures with regard to the log, the complete ineffectiveness of the security system in place, and the tendency to bypass the awkward system. The Canadian Parliamentary Committee concluded that the NDOC logs were not a reliable record of transactions at the operations centre and decided not to use the records in the inquiry into the deployment of Canadian Forces to Somalia. [5]

In this example, the use of an ICT negatively affected the availability of data about the actions of the Canadian Forces in Somalia. Thus, the Canadian parliamentary inquiry had difficulties in evaluating the deployment of Canadian Forces. One may ask whether this example is an exception or whether the decrease in the transparency of government organizations is a serious problem for accountability. Literature on electronic record keeping does seem to indicate that the (long-term) transparency of government organizations is at risk in the information age [5][6][7][8].

Although many have warned for the dangers of a loss of digital memory and the problems this would cause, there has been little empirical research concerning the relation between digital memories of government organizations and parliamentary and legal accountability. This paper tries to fill this gap. Case study research is used to analyse the influence of the use of ICTs by Dutch government organizations on parliamentary and legal accountability. This research aims to answer the following question: how does the use of ICTs by government organizations influence parliamentary and legal accountability?

2. Parliamentary and legal accountability

Accountability is a core concept in public administration. In its most fundamental sense accountability refers to answerability to someone for expected performance.[9] For public administration, Romzek & Dubnick distinguish two types of internal accountability systems, bureaucratic and professional accountability, and two types of external accountability, legal and political accountability.[10] Parliamentary accountability is a specific type of political accountability.

Parliamentary and legal accountability are crucial elements of our democratic constitutional state. Parliamentary accountability is important for the democratic control of government organizations and legal accountability plays a crucial role in the protection of individual rights of citizens. This paper focuses on two forms of parliamentary accountability - parliamentary inquiries and efficiency surveys by the National Audit Office and two forms of legal accountability - Administrative Courts and the National Ombudsman. These are all well-established, institutionalised forms of accountability.

Accountability processes consist of three phases: the information phase, the discussion phase and the sanction phase [11]. In the first phase the forum gathers data from various sources and reconstructs what has happened. In the second phase actions are discussed and judged according to certain norms and criteria. In the third phase sanctions can be applied.

The information phase is the central focus of this paper since this is the phase where the availability of (electronic) data is of primary concern. Fact-finding is the goal of this phase. It is assumed that before the Parliament, National Audit Office, Administrative Courts or National Ombudsman can discuss or sanction government actions, they need to make a reconstruction of what has happened. A reconstruction is adequate when the reconstruction is in agreement with reality, the completeness of a reconstruction refers to the part of reality that is reconstructed.

Parliamentary and legal fact-finding depend on the availability of data: the adequacy and completeness of reconstructions may therefore be influenced by the availability of data from government organizations. Traditionally these data were preserved in paper documents. The availability of data, however, is influenced by the use of ICTs by government organizations.

3. ICTs

ICTs can influence the different functions of organizational memory systems. Firstly, ICTs can affect the input functions of these memory systems. The use of ICTs may lead to registering more, less or different data. Secondly, the throughput function may be influenced by the use of ICTs. Organizations may find it difficult to preserve digital data adequately. Thirdly, ICTs can influence the output functions of organizational memory systems. Retrieval of digital data may be easier or, alternatively, more difficult than retrieval of paper data.

To understand the influence of ICTs on organizational memory systems and thus on accountability, in this paper two important elements of the use of ICTs are distinguished: technological characteristics and intentions of ICT-management. Through their technical and social construction ICTs have attained certain characteristics [12][13][14]. These characteristics do no determine the use of ICTs but

create opportunities and risks. Based on an expert survey, Meijer indicates that different ICTs present different opportunities and risks [15]. Typical opportunities and risks for six (groups of) ICTs are:

- E-mail systems are often used both for critical and ephemeral communication. Preservation of ephemeral communication increases the availability of data in a general way but failure to preserve critical communication leads to the loss of highly significant data.
- Database systems generally focus on up-to-date data. Many databases are continuously updated and 'old records' are replaced by new data. In doing so, organizations risk that 'old records' are not preserved.
- Office systems are often controlled by individual employees. The lack of central control over data creation and preservation can lead to the risk that data are not adequately preserved but individual control can also lead to better data management.
- Web technology systems can contain hyperlinks to other documents on other websites. Hyperlinks facilitate access to data but also introduce the risk that, when locations of web documents are changed, data can no longer be retrieved.
- Smart systems are characterized by their encoded 'internal logic'. Organizations risk that this 'internal logic' is no longer accessible and therefore the input and output of these systems cannot be interpreted.

The impact of these opportunities and risks is mediated by the management of ICTs. ICT-management may intend to support personal, organizational and societal functions of organizational memory systems. The intentions of ICT-management influence how organizations use these opportunities and avoid the risks. It is important to keep in mind, however, that the use of ICTs may have unintentional effects. In the prescriptive literature it is emphasized that ICT-management should intend to support not only organizational but also societal functions [6]. However, there is no

empirical research that supports this claim. Unintentional effects have not yet been investigated.

4. Case study research

Digital memory systems of Dutch government organizations and the consequences of these systems for parliamentary and legal accountability were studied through case study research. Thirteen cases were selected according to variation in parliamentary and legal institutions (National Ombudsman, Administrative Judges, National Audit Office and Parliamentary Committees) and variation in ICTs (database management systems, workflow management systems, e-mail systems and an automated telephone system). All cases were studied through interviews with key actors and review of relevant documents. In the end, the final case descriptions were verified by the key actors. Here for each of the four parliamentary and legal institutions the cases are briefly summarized. Later some of the cases will be presented more in depth to illustrate the main findings.

National Ombudsman

In the Netherlands the National Ombudsman is appointed by Parliament but performs his tasks independently. The National Ombudsman's main task is to investigate the actions of administrative authorities and decide whether they were improper or not. The National Ombudsman has about 100 staff to assist him in performing this task. Investigations are usually triggered by formal complaints of citizens. To explore the effects of the use of ICTs by government organizations on fact-findings by the National Ombudsman four of these investigations were studied:

- The National Ombudsman asked the Police in Delft to give him all data concerning the complaints of a citizen about cars parked in front of his house. The police could not meet this demand since the required data had not been registered in a database system. The failure to meet the demands of the National Ombudsman, however, could not be attributed to the use of this ICT. In this case registering activities either on paper or in an automated database system

cost a lot of time and therefore some activities were not registered. Consequently, data were lacking which were required for fact-finding.

- The Police in The Hague used a database system to support primary business processes. In the database system police reports could easily be changed; there were no technical safeguards for the authenticity of these data. In the investigation of the treatment of a citizen by police, the National Ombudsman trusted the digital police report. This report supported the point of view of the citizen and conflicted with arguments of the police officers. In view of the contents of the report the National Ombudsman had no reason to question the reliability of the digital report. In this case the reliability of data did not only depend on the way data were preserved but also on the contents of these data.
- The Central Agency for Motor Vehicle Taxes used an automated telephone application to manage its call centre. When the National Ombudsman investigated whether the agency could have been reached by a citizen, data from the automated telephone application were used to reconstruct the number of telephone calls that were not answered on the day the citizen called. This case shows how the use of an ICT-application could facilitate legal fact-finding because more data were registered.
- The Student Grant Agency used a database systems to support primary business processes. Data from these ICTs were not directly used by the National Ombudsman when investigating the complaint of a student about his debts. Crucial data were still kept in paper files. The database systems, however, supported employees in answering questions posed by the National Ombudsman. In this case ICTs facilitated legal fact-finding because the accountable organization could retrieve information more easily.

Administrative Courts

In the Netherlands citizens can file a complaint with a administrative judge if they do not agree with a government decision. Administrative judges then evaluate whether this decision has been taken in

accordance with legal regulations. To be able to evaluate decisions administrative judges first have to make a reconstruction of the decision-making process. Government information plays an important role is these reconstructions. To explore the effects of the use of ICTs by government organizations on fact-findings by Administrative Courts four cases were studied:

- The Ministry of Environmental Affairs used a workflow system to support the process of permitting the export of waste. This system led to more adequate document management. Therefore it became easier for the Ministry to send a complete file with documents to the Administrative Court that investigated a claim by a company that was not allowed to export waste. In this case ICTs improved document management at the government organization and consequently facilitated legal fact-finding.
- The Provincial Acoustic Agency in the Province of Zeeland used a simple database system to support acoustic surveys. When an Administrative Court investigated a claim by a citizen, it became easy to reconstruct the acoustic survey. The digital data could be used by the Administrative Court to recalculate the acoustic effects of a railway. In this case ICT enhanced the re-usability of data for legal fact-finding.
- The Student Grant Agency used a workflow system to improve workflow and document management. The agency created technological safeguards for the authenticity of data. These safeguards were accepted by the Administrative Court that investigated the claim of a student and trusted the digital data. In this case the government organization implemented a technological system in such a way that the legal institution considered the digital data as reliable as paper data.
- The Student Grant Agency used an e-mail system for external communication. More data were registered since e-mail communication partly replaced communication by telephone. This agency, however, had not found an adequate way to store and retrieve e-mail messages.

When an Administrative Court investigated a claim of a student, the agency could not send a copy of the relevant e-mail messages to the court. This, however, did not lead to problems for legal fact-finding because the student had a copy of the e-mail messages. In this case the introduction of an e-mail-system led to the registration of more data but also inadequate preservation of these data by the government organization. This was compensated by preservation of the data by a citizen and therefore had no direct implications for legal fact-finding.

National Audit Office

The Dutch National Audit Office is an independent body and can set its own agenda. The National Audit Office evaluates the legality, efficiency and affectivity of policies. Reports are presented to Parliament and often form the input for debates between Parliament and the government. Therefore, investigations by the National Audit Office can be considered to be an element of parliamentary control. Two cases were studied to explore the effects of the use of ICTs by government organizations on fact-findings by the National Audit Office:

- The National Audit Office used the authorization tables of the information systems of units of the Tax Department in an enquiry. In these tables, data were registered about authorizations. Preservation of these data, however, was not guaranteed: old authorizations were deleted when new authorizations were entered. This, however, did not lead to problems for fact-finding by the National Audit Office since an overview of recent authorizations was sufficient for the reconstruction it required. In this case the introduction of ICT negatively affected the durability of information but this did not influence parliamentary fact-findings which focused on up-to-date information.

- The Ministry of Finance used a database system for policy analysis. This database system contained data about income taxes in the Netherlands. The National Audit Office could use data from this database system to calculate the effects of certain legal arrangements. Without the digital application this type of fact-finding would be practically impossible. In this case ICTs created many opportunities to analyse data and can therefore facilitated fact-finding.

Parliamentary Committees

The Dutch Parliament increasingly uses its right to conduct an official enquiry. In the last ten years social insurances, police and justice, the airplane crash in Amsterdam, construction fraud and the army operation in Bosnia were investigated. Public hearings play a central role in the enquiries but prior to these hearings documents are reviewed. Three cases were studied to explore the effects of the use of ICTs by government organizations on fact-findings by Parliamentary Committees:

- The National Aviation Agency used an e-mail system for internal and external communication. More data were registered with this system because it partly replaced face-to-face and telephone conversations. The agency did not regard e-mail messages as formal communication and e-mail was informally managed by individual civil servants. When Parliament investigated the airplane crash in the Bijlmermeer, an e-mail message of a civil servant was used to reconstruct facts. However, the e-mail system did not provide guarantees for the preservation of e-mail messages. Possibly, the parliamentary enquiry committee missed other relevant messages. In this case the introduction of e-mail led to the registration of more data but also a shift of control over data from central recordkeeping departments to individual (professional) civil servants. The impact of these changes on parliamentary fact-finding is unclear.
- The Central Information Agency of the Dutch police used a database system to manage data about suspects. These digital data were not directly used by a parliamentary enquiry

committee. The committee used a paper report that showed numbers that were generated with the database system. Additional opportunities to analyse digital data were not used by the parliamentary enquiry committee. In this case ICT created many opportunities for fact-finding but these opportunities were not be used for fact-finding.

- The Ministry of Foreign Affairs used an e-mail system for internal communication. When a parliamentary committee investigated decision-making concerning peace operations, not one e-mail message was found in the departmental records. Possibly, e-mail was only used for unimportant communication. The e-mail system of the Ministry, however, made it impossible for the parliamentary enquiry committee to verify the relevance of these messages. In this case the introduction of an e-mail-system negatively affected the preservation of data. The impact of these changes on parliamentary fact-finding is unclear.

5. Analysis

In the previous section thirteen cases were briefly described. In all cases the use of ICTs influenced organizational memory systems and, consequently, parliamentary or legal accountability. The results of the case studies are summarized in the following table:

[Insert Table 1]

In this table one sees that government organizations register more digital than paper information in ten out of thirteen cases. In the terms used by Davenport, the informational transparency of government organizations increases because digital systems generally register more information about their (internal) business processes [16]. Workflow management systems, for example, register every step in a process whereas before these steps would often not be registered because this cost too much time. Furthermore, the introduction of ICTs can lead to more communication. A good example is the use of e-mail systems: oral communication that would not be registered is partly replaced by e-mail

communication that is registered. The fact that more information is registered does not directly impact upon accountability processes. Some parliamentary or legal institutions may choose to use the extra information whereas other institutions may not be interested.

The preservation of information deteriorated in seven out of thirteen cases. These deteriorations take two forms. In some cases data are preserved as long as paper data but without technical guarantees for the authenticity of the data. In other cases digital data are not preserved as long as paper data. Interestingly enough, these deteriorations did not create problems for parliamentary and legal accountability. When there were no technological safeguards for the authenticity of the data, parliamentary and legal institutions had other ways to assess the authenticity. In the cases where data were not preserved for a long period of time, parliamentary and legal institutions were only interested in recent data.

In nine out of thirteen cases digital data could be accessed more easily than paper data, an increase in the analytical transparency of government organizations [16]. Digital data can be viewed from many different perspectives. Database systems, for example, enable the user to select, aggregate and combine data in many different ways. Furthermore, retrieving data from digital systems is easy since these systems generally offer many search tools. One can search for e-mail messages, for example, using full text search options. The increase in analytical transparency does not directly impact upon accountability processes. Some parliamentary and legal institutions are interested in the opportunities to analyse the data whereas other institutions make no use of these options.

In this analysis, the effects of the use of ICTs on registration, preservation and retrieval of data have been discussed briefly. The relevance of these changes for accountability processes were also founded upon. To arrive at a more thorough understanding of these effects, changes in organizational memory systems and the consequences of these changes for accountability processes will be discussed in more depth using the information from the case studies.

6. Registering digital data: increased informational transparency

The empirical research indicated an increase in the 'informational transparency' of organizations. The transparency of government organizations increases when ICTs are used because more process information is captured [16]. This creates opportunities for fact-finding. The following case concerning an investigation of the National Ombudsman into the Central Agency for Motor Vehicle Taxes demonstrates this mechanism.

More information available

The Central Agency for Motor Vehicle Taxes implemented an automated telephone system to support its call centre. This system directed incoming phone calls to available employees and also generated an enormous amount of data about phone calls and about the work of employees. The management staff of the agency used this data to plan the work of the other employees. The data was also used to introduce targets for employees. Employees had one and a half minutes on average to answer a phone call. If employees took longer to answer phone calls, management could approach them and propose measures to improve their work rate.

With the use of the automated telephone system, the agency had set up an information factory. Work was managed according to guidelines of Frederick Taylor. Every action was measured and consequently employees had to work according to these standards. The use of the telephone system, however, had unintentional side effects. These side effects became clear when the National Ombudsman investigated the agency.

In 1999 a citizen tried to reach the Central Agency for Motor Vehicle Taxes by telephone. He tried for several days but did not get through. In the end he decided to file a complaint with the National Ombudsman. The National Ombudsman investigated the charges and asked the agency to answer questions about the number of incoming phone calls, the average waiting time and the number of calls that were answered. Before the introduction of the automated telephone system, the Central Agency for Motor Vehicle Taxes did not register information about the number of incoming calls and the

average waiting time and thus could not have answered these questions. In the 'paper situation' the National Ombudsman would not have been able to reconstruct facts and evaluate the citizen's complaint. With the use of the automated telephone system, the Central Agency for Motor Vehicle Taxes could give an exact answer to the questions of the National Ombudsman: fact-finding was facilitated by the automated telephone system.

In this case the Central Agency for Motor Vehicle Taxes registered much more data about the answering of its telephones. The informational transparency of the process increases as a result of management efforts to improve the support and steering of the business process of answering phone calls. In its turn, the National Ombudsman could use this informational transparency for fact-finding and thus make a more adequate and complete reconstruction of facts.

7. Preserving digital data: decreased authenticity and durability of data

The case study research indicated that the introduction of ICTs might threaten the authenticity of data. How can parliamentary and legal institutions trust digital data when there are no technological procedures to preserve the authenticity of this data? In the cases, however, other safeguards for the authenticity of data were identified. The following example illustrates how organizational safeguards can render data reliable:

Decreased (technological) authenticity

Information about police suspects is gathered and preserved by the (decentralised) police departments. The Central Information Agency has set up a system to facilitate exchange of information between the regional police departments. Through this information system police departments can find out that a suspect is also suspected by another police department. To this end police departments periodically send information to the automated information system of the Central Information Agency. There the information is preserved in a database. Since the information is only used within the police

organization, the agency did not consider it necessary to introduce technological safeguards for the authenticity of the information.

In 1998 and 1999 the behaviour of the Dutch national police organization was investigated by a parliamentary committee. On of the questions the committee tried to answer was whether the police followed the law and deleted information about persons after a prescribed period of time. The committee used information from the database management system of the Central Information Agency to evaluate policies regarding police suspects. The fact that there were no technological safeguards for the authenticity of the digital information, did not bother the parliamentary committee. They did not question the reliability of the information about police suspects.

Why did the parliamentary committee not question the reliability of the digital information when there were no technological safeguards? To understand this, we need to look at organizational aspects of the management of information about suspects. The Dutch Police kept the same information in two places: at the Central Information Agency and at the separate police departments. Tampering with the digital information would require interorganizational cooperation. This is indeed possible but much harder to accomplish than when the information is kept by one government organization only and, therefore, these organizational safeguards were one of the reasons why the parliamentary committee could trust the information provided to them.

In this example there are no technological safeguards for the authenticity of digital data. Theoretically, it is easy to manipulate digital data and therefore one can argue that the data about police suspects are not reliable. The absence of technological safeguards, however, does not necessarily lead to the conclusion that data are not reliable. Other types of safeguards can protect the authenticity of digital data. In this case study, the Parliamentary Committee could trust the data because there were organizational safeguards for authenticity: management of information was carried out by different actors.

The case studies also indicated that the use of ICTs can decrease the durability of data. Digital data

may not be preserved as long as paper data and, therefore, may not be available for fact-finding by Parliament, National Audit Office, and National Ombudsman of Administrative Judges. However, problems only arise when these parliamentary and legal institutions require old data for the reconstruction of facts. In such cases, lack of durability did not lead to problems, however, as we see below.

Decreased durability

The Tax Department keeps information about citizens and companies to carry out its task of collecting taxes. It needs to protect its data about citizens and companies for reasons of privacy and preventing fraud. Employees at the Tax Department therefore acquire rights to read or change data according to their function within the organization. These rights to read or manipulate data are laid down in databases which do not contain historical components. When the rights of an employee change, the data in these tables are changed. Old data are replaced by new data. Thus, the tables contain no information about the past but only about the present situation.

In 1996 the National Audit Office evaluated the protection of data by the Tax Department. The data in tables were used to check whether employees had the rights they should have according to the policies of the Tax Department. The National Audit Office could not check whether the rights of employees had recently be changed since the databases did not contain historical components. This did not matter to the National Audit Office because the available data already indicated that the Tax Department had not implemented its own policy guidelines.

In this case data are not preserved in a durable way. Old data are replaced by new data and therefore these old data are effectively deleted. The Tax Department did not find it necessary to preserve old data. The National Audit Office did not consider this to be a problem since it could reconstruct relevant facts on the basis of the ‘new data’. The lack of durability had no consequences for fact-finding.

8. Retrieving digital data: increased analytical transparency

The empirical research also demonstrated an increase in analytical transparency. The transparency of government organizations increases when ICTs are used because data may be viewed from different perspectives. Thus, ICTs improve the analysis of information and decision making [16]. An example can illustrate the consequences of the increasing analytical transparency for accountability:

More opportunities for data analysis

In the Netherlands, the Ministry of Finance is responsible for the formulation and implementation of tax policies. To perform this task the ministry requires data about incomes of citizens and taxes. Therefore, the Ministry of Finance has established a database system with tools for the analysis of these data. This system is used for policy analysis and policy development.

In 1998 the National Audit Office investigated the use of taxes as a policy instrument. The National Audit Office wanted to find out how effective various legal arrangements (e.g. concerning green investments and travelling to work using public transportation) were and thus needed data about these arrangements. However, data about these legal arrangements were neither kept by the responsible policy department nor by the Tax Department. This lack of data hampered fact-finding by the National Audit Office.

In the end, the National Audit Office did manage to reconstruct the amounts of money spent on the different arrangements with the use of the database system of the Ministry of Finance. This system offered various facilities to aggregate, query and analyse the data. Thus, the National Audit Office could evaluate the effectiveness of the various legal arrangements. Such a reconstruction of facts would not have been possible without the automated database system of the Ministry of Finance since it would have taken the National Audit Office a very long time to aggregate, query and analyse data in thousands of paper forms and letters.

In this case there are not many differences in the data that were registered in paper and in digital systems. The use of the database system, however, makes it much easier to retrieve the data in various ways. This means that the analytical transparency of government increases. Civil servants at the Ministry of Finance used this transparency for policy analysis. In its turn, the National Audit Office could use this analytical transparency for fact-finding and thus make a more adequate and complete reconstruction of facts.

8. Transparent government

The empirical research seems to indicate that the anomalies in the database of the Canadian Forces were indeed an exception. The most significant finding was that the use of ICTs leads to more informational and analytical transparency of government organizations for parliamentary and legal accountability. More data is recorded and there are also more ways to retrieve this data. The use of ICTs leads to a more 'transparent government'. Interestingly, this increased transparency is an unintentional effect of efforts of ICT-management to improve the support and management of business processes.

Generally, parliamentary and legal fact-finding is facilitated by the increased transparency of government organizations. Often parliamentary and legal fact-findings result in more adequate and more complete reconstructions of facts. The image of 'transparent government', however, needs to be placed in perspective. Firstly, in parliamentary and legal investigations, it remains the case that little use is made of digital data. Most parliamentary and legal institutions still rely heavily upon paper data. It does not seem likely that this situation will change radically within a few years because there still is much uncertainty about the status of digital data. Secondly, the use of ICTs may lead to fewer guarantees for the authenticity of data since data can easily be changed. This shortcoming may not hamper the quality of the reconstruction of facts in parliamentary or legal scrutiny, however, when there are organizational guarantees for authenticity. Thirdly, the use of ICTs may have negative consequences for the durability of data. This only leads to problems for fact-finding when

parliamentary and legal institutions require these data. Such situations may exist but the empirical research yielded no examples.

In general, the empirical research indicated that the use of ICTs by government organizations facilitates parliamentary and legal accountability. In the information age government seem to become more transparent. This transparency can be used in parliamentary and legal fact-finding but also in other types of accountability. Increasingly, government organizations make their information available to the public through their websites. This makes it possible that in the future the transparency could also be used for direct accountability to citizens. We might be heading for Brin's ideal of reciprocal transparency: citizens are transparent to government and government is transparent to the citizens. [17] The gloomy idea of government without a (digital) memory is thus replaced by the perspective of realizing direct citizen/government accountability in the information age.

References

[1] J. Rothenberg, Ensuring the longevity of digital documents, *Scientific American* **272(**1) (1995), 24-29.

[2] T. Blanton (ed.), *White House E-mail: the top secret messages the Reagan-Bush White House tried to destroy*, The New Press, New York, 1995.

[3] D.A. Wallace, *The Public's Use of Federal Recordkeeping Statutes to Shape Federal Information Policy: A Study of the PROFS Case*, Unpublished PhD Thesis, University of Pittsburgh, 1997.

[4] A. Meijer, Geographical information systems and public accountability. Towards a better understanding of long-term public accountability in an information age, *Information Polity* **7(**1) (2002), 39 – 47.

[5] L. Duranti, Concepts, Principles, and Methods for the Management of Electronic Records, *The Information Society* **17(**4) (2001), 271-279.

[6] D. Bearman, *Electronic Evidence. Strategies for Managing Records in Contemporary Organizations*, Archives and Museum Informatics, Pittsburgh, 1994.

[7] S.S. Lukesh, S.S., E-Mail and Potential Loss to Future Archives and Scholarship or The Dog that Didn't Bark, *First Monday* (www.firstmonday.org) **4(**9) (1999).

[8] S. Yorke, The Electronic Recordkeeping Environment. In: *Selected Essays in Electronic Recordkeeping in Australia*, J.A. Ellis (ed.), Australian Society of Archivists, O'Connor , 2000, pp. 5-15.

[9] B.S. Romzek & P.W. Ingraham, Cross Pressures of Accountability: Initiative, Command, and Failure in the Ron Brown Plane Crash, *Public Administration Review* **60**(3)(2000), 240 – 253.

[10] B.S. Romzek & M.J. Dubnick, Accountability in the Public Sector: Lessons from the Challenger Crisis, *Public Administration Review* **47**(3)(1987), 227 – 238.

[11] M.A.P. Bovens, *The Quest for Responsibility: Accountability and Citizenship in Complex Organisations*, Cambridge, Cambridge University Press, 1998.

[12] S. Zuboff, *In the age of the smart machine. The future of work and power*, New York, Basic Books, 1988.

[13] G.P. Huber, A Theory of the Effect of Advanced Information Technologies on Organizational Design, Intelligence, and Decision Making. In: *Organizations and Communication Technology*, J. Fulk & C. Steinfield (eds.), Sage Publications, Newbury Park/London/New Delhi, 1990, pp. 237-274.

[14] W.E. Bijker, T.P. Hughes & T.J. Pinch, *The social construction of technological systems: new directions in the sociology and history of technology*, MIT Press, Cambridge, 1987.

[15] A. Meijer, Electronic Records Management and Public Accountability: Beyond an Instrumental Approach, *The Information Society* **17(**4) (2001), 259 – 270.

[16] Th. D. Davenport, *Process Innovation: Reengineering Work through Information Technology*, Harvard Business School Press, 1993.

[17] D. Brin, *The Transparent Society*, Perseus, Reading. 1998.

Case	ICT	Register[1]	Preserve[2]	Retrieve[3]
National Ombudsman				
Delft Police	Database System	+	-	+
The Hague Police	Database System	+	-	+
Motor Vehicle Taxes	Telephone System	+	-	+
Student Grant Agency	Database System	+	+/-	+
Administrative Courts				
Ministry of Environmental Affairs	Workflow System	+	+/-	+
Provincial Acoustic Agency	Database System	+	+/-	+
Student Grant Agency	Workflow System	+	+/-	+
Student Grant Agency	E-mail System	+	-	-
National Audit Office				
Ministry of Finance	Database System	+/-	+	+
Tax Department	Database System	+	+/-	+/-
Parliamentary Committees				
National Aviation Agency	E-mail System	+	-	+/-
Central Information Agency	Database System	+/-	-	+
Ministry of Foreign Affairs	E-mail System	+/-	-	+/-

Table 1. Changes in organizational memory systems

[1] + more data were registered; +/- no changes; – less data were registered.

[2] + data were preserved for a longer period of time and/or with more guarantees for authenticity; +/- no changes; – data were preserved for a shorter period of time and/or with more guarantees for authenticity.

[3] + data were easier accessible; +/- no changes; – access to data were more difficult.