



NEDERLANDSE VERENIGING VOOR RECHTSVERGELIJKING
NETHERLANDS COMPARATIVE LAW ASSOCIATION

The Status of eGovernment in the Netherlands

S. van der Hof*

Readers are reminded that this work is protected by copyright. While they are free to use the ideas expressed in it, they may not copy, distribute or publish the work or part of it, in any form, printed, electronic or otherwise, except for reasonable quoting, clearly indicating the source. Readers are permitted to make copies, electronically or printed, for personal and classroom use.

1. Introduction

eGovernment has been high on the policy agenda since the mid 90s. Since then, the Dutch central government launched several programmes and issued a number of policy documents in the area of or related to eGovernment. This paper, first, provides a chronological overview of the most important government policy initiatives on eGovernment.¹ Subsequently, the paper addresses issues with legal implications or issues touching on legal matters, which have been addressed in these policy documents. Then, eGovernment practice in the Netherlands will briefly be described to show the impact of the policy initiatives, and eGovernment projects and programmes, so far. Finally, the paper addresses the regulatory framework for eGovernment, the remaining legal challenges and ends with a short conclusion.

2. Policy Initiatives

2.1. 1998 Electronic Government Action Programme

With the '1994 National Action Programme on Electronic Highways: From Metaphor to Action' the Dutch government launched its first ICT policy initiative. This action programme aimed at stimulating the development of 'electronic highways', but did not as yet address the provision of online public services. After an evaluation of the results achieved under the '1994 National Action Programme' in 1997, the Ministry of the Interior and Kingdom Relations launched the '1998 Electronic Government Action Programme'. This programme envisaged a more active role of the government by developing a more efficient and effective government through the use of ICTs. The programme revolved around three overall themes:

* S. van der Hof is Senior Lecturer in Private International Law and ICT-law at Tilburg University.

¹ Based upon information provided by the E-government knowledge centre (<<http://www.elo.nl>>) and in the IDABC Report 'eGovernment in the Netherlands', June 2005, online available at: <<http://www.europa.eu.int/idabc/en/document/4370/254>>.

1. Good electronic access to government – The starting point here was that government information, which is fundamental in a democratic constitutional state, such as legislation, court decisions, parliamentary information, should be online accessible to citizens. As a result of this objective, for instance, the government portal www.overheid.nl and the project Government-Citizen Communications (e.g. resulting in PC's with internet connections in public libraries) were established.
2. Better service to the public – One of the actions here included the continuation of the Programme OL2000, which was launched in 1996. This project aimed at the development of an electronic counter ('one-stop shop') for the provision of public services to citizens, in addition to existing traditional means of communication (multi-channel delivery). Also the use of chip cards for public services was studied.
3. Improving the back-office of national government – This action line purported an improved data exchange within the government with a view to use data already available with the government, one-time data provision by citizens and business, and a reduction in administrative burdens and cost efficiency for companies.

2.2. 1998 Legislation for the Electronic Highway

In 1998, the Ministry of Justice also launched the policy document 'Legislation for the electronic highway'. Although it is not specifically focused at eGovernment as such, it deals with the influence of the dematerialization tendency on administrative law as well as the confidentiality (PETs, anonymous biometrics) and reliability (e-identification, digital signatures, TTPs) of electronic communications and, thus, affects eGovernment developments.

2.3. 1999 Dutch Digital Delta

In 1999, the policy document 'The Dutch Digital Delta' (D3) saw the light of day and introduced five pillars, amongst which the regulation and use of ICT in the public sector, which were considered essential for the 'the future position of the Netherlands as a world leader in ICT'. D3 further builds upon earlier policy documents and, therefore, to a great extent overlaps with issues already mentioned before.

2.4. 2000 Contract with the Future

D3 was shortly thereafter followed by another policy document, titled 'Contract With The Future', in 2000. This document envisaged a new and more balanced relationship between citizens and government through ICTs and recognised that in order to achieve that goal government had to become more approachable to citizens, amongst others, by improving accessibility and citizen participation and by providing citizens with more choices on how to structure their informational relationship with the government. Several pilot projects, studies and surveys were initiated accordingly, which intended to complement the activities already started under the '1998 Action Programme Electronic Government' and take them a step further.

2.5. 2003 Modernising Government

After a change of government, the 'Better Government For Citizens And Business Action Plan' was launched in 2002,² but did not serve a long life. A year later already, the '2003 Action Plan Modernising Government' replaced the 2002 Action Plan due to, again, a change of government. 'Modernising Government' aims at a more

² *Kamerstukken II 2002/03*, 28 755, nr. 1.

reserved government with respect to regulation and concentration on tasks that are vital for a constitutional state as well as more responsibility for society at large. One of the lines of action includes the improvement of public service, including eServices. 'Modernising Government' has been further elaborated in the '2004 National ICT Agenda 'Better Performance With ICT' and the '2005 Follow-Up on National ICT Agenda 'Better Performance With ICT'.

3. Legal and Regulatory Issues in eGovernment Policy

The policy documents of the previous paragraph address several persistent key issues that have legal implications or touch upon legal matters in Dutch eGovernment policy. The most important of which are: privacy, dematerialization of government communications, confidentiality and reliability of eGovernment communications, efficient eGovernment communications and service provision, interoperability of eGovernment data exchange, and access to and re-use of public sector information. This paragraph will further elaborate on these issues by addressing relevant developments in each category.

3.1. Privacy

Most policy documents clearly recognize that the privacy of citizens should be adequately guaranteed.³ Personal data of citizens must be kept confidential and the collection of such data must be transparent. Citizens should, e.g., be protected against datamining and the use of their personal data by third parties. More concrete plans mentioned are an opt-out system through self-regulation and the use of privacy-enhancing technologies (PETs) and anonymous biometrics. The latter will, however, be necessarily restricted by higher interests, such as state security and criminal investigations. Moreover, the '2000 Contract With The Future' policy document initiates a study on control over and transparency of personal data. The study led to research projects, such as on legal and technical aspects of controlling own personal data and periodic reports to citizens on recorded own personal data.⁴ Results of the first project were published in 2001.⁵ In the same year, a special commission recommended the introduction of a voluntary digital safe (*digitale kluis*), which provides citizens with access to their personal data and allows them to manage and supply personal data. The proposal was strongly criticized mostly for privacy and security reasons by the Dutch Data Protection Authority and several politicians.⁶ The proposal seems to have been abandoned since then. In 2003, the outcome of the second project is that a periodic survey of personal data of citizens should only be provided at their request. The establishment of a central register is unnecessary, but the government must provide sufficient help for citizens to be able to find out about registered personal data. Presently, the Ministry of the Interior works out whether

³ A policy document on personal information is expected soon, see: <http://www.minbzk.nl/ict_en_de_overheid/ict_en_de_overheid/blindgangers/ict_binnen_de/documenten_en_links_0#PrivacyEnhancingTechnologies>.

⁴ See also (in Dutch): <http://www.minbzk.nl/ict_en_de_overheid/ict_en_de_overheid/blindgangers/ict_binnen_de_0/beveiliging_en#Regieentransparantiepersoonsgegevens>.

⁵ Holvast 2001.

⁶ Forse kritiek op plan 'digitale kluis', Netkwesties June 2001, <<http://www.netkwesties.nl/editie16/artikel1.html>>.

such a service can be integrated with the Citizen Service Number (see further section 5.1.4).

Privacy is a thread in many of the other issues mentioned hereafter as well, most notably with respect to confidentiality, reliability, efficiency of eGovernment communication and service provision.

3.2. Dematerialization of eGovernment Communications

The '1998 Legislation for the electronic highway' policy document recognizes that administrative communication and decision-making processes, at that time, contained writing requirements, which needed to be adapted to electronic communications by changing of the General Administrative Law Act. The policy document, initially, advises the introduction of an experimental provision in this Act, which gives electronic decisions an equal status to written ones. This idea of an experimental provision was, however, soon abandoned again and in 2004 the General Administrative Law Act was permanently changed to accommodate electronic communications with(in) the government (see further section 5.1.1). Furthermore, the '1999 D3' policy document addresses electronic tax declarations, which over the years have been successfully introduced for businesses and private persons, as well as electronic procurement as relevant eGovernment issues.

3.3. Confidentiality and Reliability of eGovernment Communications, Service Provision and Procedures

The '1998 Electronic Government Action Programme' first mentions the importance of reliable and confidential eGovernment communications, including issues such as identification and authentication. The policy document points at the relevance of information security and specific technologies, such as TTPs, digital signatures and chip cards. It also mentions explicit goals, such as ensuring sustainability with respect to digital government records. A project on digital longevity ([http://www.digitale duurzaamheid.nl](http://www.digitale-duurzaamheid.nl)) had started already in 1996. Within this programme, knowledge and experiences of government organisations on digital information management and quality control have been made available over the years (so-called digital toolbox). Moreover, research experiments with respect to long-term digital preservation were performed. Recommendations on technical and preservation strategies are being made available on the programme's web site.

The '1998 Legislation for the electronic highway' policy document, moreover, points out that government legislation is necessary with respect to the use of biometrics, electronic identification, digital signatures, and TTPs. In the latter case, the document also anticipates self-regulation, which led to a trustmark for Certification Service Providers (i.e., TTPs that issue digital certificates for digital signing and encrypting purposes) (TTP.NL). With respect to electronic signing, the Electronic Signature Act 2003 was issued to implement Directive 93/9/EC (see section 5.1.1). In order to allow the use of biometrics in passports, legislation amending the Passport Act (*Paspoortwet*) is pending in the second chamber of parliament.⁷

Moreover, a government PKI (*PKIoverheid*, <http://www.pkioverheid.nl>) has been established and several private companies were admitted as certified Certification Service Providers (i.e., TTPs that issue digital certificates for digital

⁷ *Kamerstukken II* 2001/02, 28 342, nr. 1-5.

signing and encrypting purposes) under the TTP.NL scheme.⁸ In 2004, the Dutch government embraced the newly established national authentication service (DigiD, <<http://www.digid.nl>>), which overrules the many authentication initiatives which existed in the Netherlands at the time. DigiD means a step forward in the field of e-identification and a more efficient eGovernment. The authentication scheme provides three security levels dependent on the service concerned: basic (user name and password), middle (Internet-banking mechanisms, software certificates), and high (*PKIoverheid* and electronic national identity card, expected to be introduced in 2006).

Finally, several quite recent incidents, such as a denial-of-service attack at the <<http://www.overheid.nl>> website, have shown that information security within the government is, however, still worrying. In 2002, the Ministry of the Interior and Kingdom Relations started Govcert.nl (<<http://www.govcert.nl>>), the Dutch government's computer emergency response team, and 'waarschuwingsdienst.nl' (<<http://www.waarschuwingsdienst.nl>>) (a computer security alert service for citizens and SMEs) to increase information security.

3.4. *Efficient eGovernment Communications and Service Provision*

The policy documents address several recurring topics on the efficiency of eGovernment communications and services. First of all, the idea of the reduction in the administrative burden led to the 'streamlining of key data' project (<<http://www.stroomlijningbasisgegevens.nl>>). A system of initially 6 key registers (i.e., registers on natural persons, companies, plots, addresses, buildings, and geographic maps) is being established, in which key data need to be provided only once and can, subsequently, be used by the public sector as a whole. For the future, an expansion of the systems with further registers is intended (probably including key registers for income and wealth, vehicle registrations, non-residents, social-security records and the large-scale basic map of the Netherlands). Within the project a study addressing, among other things, privacy, liability, intellectual property rights, and archiving has been performed to map and clarify the legal issues involved.⁹ Meanwhile, legislation is pending or drafted to regulate the different registers (see further section 5.1.5).

Another project, which aims at a reduction of the administrative burden for government and businesses, is the Government Transaction Gate (*Overheids-transactiepoort* (OTP), <<http://www.ictal.nl>>). OTP is a digital post office which supports and facilitates standardized electronic communication between government and companies. In 2004, a study into the legal aspects of OTP, such as liability, evidence and security, was performed to map the legal environment in which such a service operates.¹⁰

Second, the '2003 Modernising Government' action plan announces the introduction of a Citizen Service Number, expected in January 2006, to improve service provision and enforcement (e.g., of fraud) by the government (<<http://www.programmabsn.nl>>). The Citizen Service Number is a unique identification number used in relationships with the Dutch government and to some, as yet uncertain, extent in relationships with non-governmental bodies, and will

⁸ An evaluation of government TTP policy was carried out in 2004: Zouridis *et al.* 2004.

⁹ Schreuders & Prins 2002.

¹⁰ Van der Hof *et al.* 2004.

correspond with and replace the National Insurance Number. Legislation regulating this personal number is currently pending in Parliament. The Citizen Service Number is criticized from several sides (amongst others, the Dutch Data Protection Authority and the Council of State) for a number of reasons. First, worries exist with respect to the integrity and security of the system. Currently, the quality of data available in the government back offices leaves much to be desired and an improvement as a result of the introduction of a Citizen Service Number is doubted. Second, better public service provision to citizens is an important argument for the introduction of the Citizen Service Number. However, the citizen is addressed rather as an object than as a customer and the actual interested parties seem to be the users of the system. Another important argument *pro* a Citizen Service Number is the fight against identity fraud. Yet, some feel that an extended use of this number will rather reinforce identity fraud risks.¹¹ So far, the Dutch government has neglected to address the risks of identity fraud. Finally, a special facility, a so-called roadmap, is intended to provide more transparency to citizens concerning the uses of the Citizen Service Number amongst public bodies and the legal basis for such uses. However, non-public bodies using the number are not included in the map. Moreover, an unsettled issue is the responsibility with respect to the quality of the information on the website concerned. In addition, the roadmap may provide more transparency so as to provide the government with more ideas and opportunities to exchange personal data.¹²

Third, pro-active service provision is a persistent issue in Dutch eGovernment policy and research into legal and other barriers to pro-active service provision was felt to be necessary. In 2001, the government issued a practical guide on the development and implementation of pro-active service provision for the public sector.¹³ This handbook addresses the legal implications of using citizen information, more specifically personal-data protection. In pilot projects, pro-active services are further being developed. In a 2002 Research report on Electronic government and privacy, the Dutch Data Protection Authority also addresses the data-protection rules applicable to pro-service provision and stresses that personal data should be sufficiently up-to-date and appropriate for linking purposes to prevent problems with linking of files.¹⁴

Finally, the '2003 Modernising Government' document addresses the problem of adequate and timely replies to e-mails addressed to the government. Research of the National Ombudsman had shown that the central government lacked considerably in this respect. The policy document states that the government organization must be adjusted such that statutory deadlines can be met. Moreover, uncomplicated correspondence should have priority and in the case of delays and complex correspondence the procedure and final deadline must be announced to the sender. In 2000, a code of conduct on dealing with e-mail messages was issued for the Dutch ministries. In October 2005, 'Burger@overheid', a forum that stimulates eGovernment from a citizen perspective (<<http://www.burger.overheid.nl>>), concludes on the basis of a study into government communication, however, that many municipalities still do not respond at all or late to e-mails, especially in the case of difficult questions and irrespective of an acknowledgement of receipt, some of

¹¹ See also Prins 2003, p. 2-3.

¹² Prins 2006.

¹³ Naar een pro-actief werkende overheid, Een handreiking voor gemeenten die hun burgers pro-actief van dienst willen zijn, available at: <<http://www.elo.nl>>.

¹⁴ Versmissen & De Heij 2002, p. 35-39.

which contained promises about further procedures and deadlines. This forum issued a code of conduct, based on the 2000 Code of Conduct for ministries, which has now been adopted by a small number of municipalities. In addition, the forum operates a complaints service on this issue.

3.5. *Interoperability of eGovernment Data Exchange*

The '2003 Modernising Government' policy document briefly mentions the use of (open) standards for electronic data exchange with and between public bodies. In order to encourage the use of open standards and of open-source software, the OSOSS programme (<<http://www.ososs.nl>>) was started in 2003. Meanwhile, a national standardization council has been established to stimulate interoperability between governments and between government and citizens/business. Moreover, a knowledge centre for open-source software has been set up to meet the needs for expertise and support in this area.¹⁵

3.6. *Access to and Re-use of Public-sector Information*

The '1998 eGovernment Action Programme' states that fundamental information of a constitutional state, such as legislation, court decisions and parliamentary information, as well as other government information must be made widely accessible through the Internet. Such information is currently available at different websites (e.g., <<http://www.overheid.nl>>, <<http://www.rechtspraak.nl>>, <<http://www.eerstekamer.nl>>, <<http://www.tweedekamer.nl>>). In 2000, the Advisory Commission on 'Fundamental Rights in the Digital Era', which was established by the Dutch government, recommended the introduction of a constitutional right of access to public-sector information as well as an obligation for the government with respect to the accessibility of fundamental information of a constitutional state. Although the government initially made a proposal mainly in lines with the recommendations of this commission, it was finally decided to leave any decision-making with respect to this particular constitutional right until after an evaluation of the Government Information (Public Access) Act 1991 (*Wet openbaarheid van bestuur* 1991) had taken place. This evaluation was carried out in 2004¹⁶ and again recommended the introduction of a constitutional right of access to public-sector information as well as a general law on access to, accessibility and use of public-sector information, which would replace the Government Information (Public Access) Act 1991. Furthermore, the evaluation report recommends making active dissemination of information the rule and access at request the exception. In line with this, the '2000 Contract With The Future' policy document stresses that all government information should be actively made available to the public. In 2003, the 'Modernising Government' policy document announces a project to commence with active dissemination of all information on merely three urgent topics in 2006. In 2005, 8 ministries have, however, established a site with public-sector information that has been made public upon a recent request on the basis of the Government Information (Public Access) Act 1991. According to the evaluation report, the active dissemination rule should, furthermore, be complemented with legal obligations to guarantee actual and intellectual accessibility of public-sector information. In addition, back and front offices of public bodies should be better

¹⁵ *Kamerstukken II* 2003/04, 26 643-29 800XIII, nr. 67.

¹⁶ Van der Hof *et al.* 2004a.

geared to each other and ICTs (including the Internet) should be used more and more effectively to achieve public-sector transparency. So far, however, statements by the government concerning the evaluation report, and the legal future of public access to public-sector information remain forthcoming.

In relation to the re-use of digital government information by companies, the '1998 Government Action Programme' mentions the importance of clear conditions on non-discriminatory access to such information. This topic is, subsequently, addressed in other policy documents as well. Presently, legislation regulating the re-use of public-sector information is pending in parliament (see further section 5.2.2).

4. eGovernment in Practice

The previous sections show an impressive list of policy initiatives. This section will address the Dutch eGovernment situation to establish whether these policy initiatives have led to a productive eGovernment practice. Both the situation of eGovernment in the Netherlands as well as the Dutch situation compared to that in other countries are discussed.

4.1. eGovernment in the Netherlands

The status of eGovernment in practice differs at the national and local level as well as between small and large municipalities. The national level shows important developments, such as in the field of tax and customs administration, car registration, the student loan system and information exchange between social welfare agencies.¹⁷ The local level is not doing as well as the national level, although some distinctions are necessary. Some cities took part in the OL2000 project (see section 2.1) and especially three of them, which were in later on indicated as SuperPilots (i.e., The Hague, Enschede, and Eindhoven/Helmond), show promising results. Moreover, outside the OL2000 project, large cities are doing better than smaller municipalities, because they own the resources to invest in eGovernment and there is a critical mass to use e-services. All in all, the progress at the local level has been rather slow. Not until the end of 2003 did all of the municipalities have a website, and the maturity of e-service delivery on these websites is rather low. To give an example, transactional services are still very few. Again with the smaller municipalities lagging behind the bigger ones. Furthermore, citizens rate off-line services higher than on-line services.¹⁸

More generally with respect to the implementation of ICTs in the public sector, the '1999 D3' policy document observes that lack of central steering and co-operation between public organisations in this respect is felt as a problem.¹⁹ Good examples are the ample e-authentication initiatives in the public sector, which only after years have eventually been covered and replaced by one central facility, called DigiD. Joining such a central initiative makes it easier and financially more worthwhile for municipalities to implement e-authentication mechanisms in their eGovernment services than having to develop their own mechanisms. More and better co-operative action in other areas of developing eGovernment services may prove fruitful as well.

¹⁷ See for an overview: <http://www.elo.nl/elo/english/egov/online_services/index.jsp>.

¹⁸ See all Leenes 2004, p. 8-11.

¹⁹ See also Leenes 2004, p. 12-15.

4.2. *The Netherlands compared to other Countries*

Until 2004, international benchmarks showed that the Netherlands have over the years dropped in rankings on eGovernment services and is no longer at the top. In relation to other EU countries, the number of online public services is low and the progress of getting such services online is slow.²⁰ A recent international benchmark by Accenture measures a combination of service maturity and customers services maturity, which results in an overall maturity score. Service maturity consists of service breadth, the number of national services available online, and service depth, the level of completeness at which the service is offered (publish-, interact- or transact-level service). Customers services maturity is the extent to which government agencies manage interactions with their customers (citizens and businesses). On the 2005 overall maturity index, the Netherlands finds itself in the middle group, scoring only slightly higher than the average of 48% (50%), and being indicated as a follower. Trend-setters and challengers according to this benchmark are: Canada and the United States respectively Denmark, Singapore, Australia, France, Japan, Norway, and Finland.²¹

5. **Regulatory Framework for eGovernment**

An overall regulatory framework for eGovernment, i.e. an eGovernment Law, does not exist in the Netherlands. However, some laws address issues related to eGovernment and other laws that do not specifically address eGovernment may nevertheless be applicable to this area. This section will first deal with the most relevant legislation in both categories respectively and wind up with concluding remarks concerning the regulatory framework for eGovernment.

5.1. *eGovernment-related Laws*

5.1.1. Electronic Government Communications

On 1 July 2004, the Act on Electronic Government Communications (*Wet elektronisch bestuurlijk verkeer*), which amends the General Administrative Law Act (*Algemene Wet Bestuursrecht*), was enacted. The law regulates electronic communications between government bodies on the one hand and between government and citizens/businesses on the other hand. Parties involved must have given express notice of their electronic contactability. The sole availability of an e-mail address does not amount to such contactability. Government bodies can give notice with respect to specific forms of e-communication in different ways, i.e. through a general regulation, an individual e-mail message, on websites, the local paper, etc. Moreover, the law takes a functional approach, i.e. electronic messages should be sufficiently reliable and confidential as regards the nature and the content of the message as well as its purpose. In other words, the security of electronic communications should be as reliable and confidential as conventional communications, and some instances require more security measures (e.g. granting a license) than others (e.g. providing general information). Both the criteria of reliability and confidentiality depend upon the state of the art and may be further defined by technical rules for specific situations. Furthermore, with respect to e-

²⁰ Leenes 2004, p. 11-12.

²¹ The Government Executive Series Leadership in Customer Service: New Expectations, New Experiences, <http://www.accenture.com/xdoc/ca/locations/canada/insights/studies/leadership_cust.pdf>.

signatures this law refers to the section in the Civil Code (Electronic Signature Act 2003), which implements Directive 99/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures,²² and is also based on the functional approach as well as on the distinction between advanced and normal e-signatures as laid down in the Directive. These provisions are applicable to government e-communications, unless the nature of the message concerned opposes such an application. Also, law can impose additional requirements for the use of e-signatures in e-communications with(in) the government. In view of complying with deadlines, this law finally determines the times of dispatch and receipt of e-messages sent to government bodies.

5.1.2. eProcurement

On 1 December 2005, the Regulation on procurement rules for public contracts (*Besluit aanbestedingsregels voor overheidsopdrachten*), which implements Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contract,²³ entered into force. Among other things, the Regulation regulates the possibility of eProcurement. The objectives are to allow for more efficient and timesaving public procurement procedures and to introduce new ways of public procurement, i.e. electronic auctions and dynamic purchasing systems. Electronic auctions function as an automated evaluation method, ranking tenders anonymously depending on new prices revised downwards and other new values concerning certain elements of the tenders. A dynamic purchasing system is a fully electronic system intended for common purchases with characteristics generally available in the market. Before sellers or service providers can subscribe to specific procurement offers, they have to submit an indicative tender to be admitted to the system.

Following the Act on Electronic Government Communications, 'writing' in this Regulation includes electronic documents and is defined in line with the Directive, which states that '(in) writing' is 'any expression consisting of words or figures which can be read, reproduced and subsequently communicated. It may include information which is transmitted and stored by electronic means'.

5.1.3. Electronic Tax Returns and Invoices

Since January 1996, tax legislation allows tax declaration forms to be filed with the Tax Department electronically.²⁴ Since January 2005, companies are legally obliged to electronically file tax declaration forms with respect to, among other things, income, corporation and turnover taxes. With the implementation of Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax, electronic invoicing has been introduced into Dutch law.²⁵

²² OJL 178/1, 17 July 2000.

²³ OJL 134/114, 30 April 2004.

²⁴ Wet van 6 december 1995 tot wijziging van de Algemene wet inzake rijksbelastingen en van enige andere wetten in verband met de invoering van de mogelijkheid tot het doen van aangifte op elektronische wijze, *Staatsblad* 1995, 606.

²⁵ Wet van 18 december 2003, houdende wijziging van de Wet op de omzetbelasting 1968 met het oog op de vereenvoudiging, modernisering en harmonisering van de ter zake van de facturering →

Electronic invoices will be accepted by the tax inspector when the authenticity of the source and the integrity of the contents of the invoice are sufficiently guaranteed, which is, for example, the case when an advanced electronic signature in the sense of Directive 99/93/EC on electronic signatures is used. Under certain conditions, electronic invoicing through EDI and other methods are allowed as well.

5.1.4. Citizen Service Number

Presently, a proposal for a Citizen Service Number Act is pending before parliament, regulating the Citizen Service Number already elaborated upon in section 3.4.²⁶ The proposed law addresses the attribution, use and management of these personal numbers, and more specifically the protection of personal data.

5.1.5. Streamlining of Key Data

Under the 'streamlining of key data' project (see section 3.4) legislation is planned for the beginning of 2007 addressing each of the key registries. These laws will address the terms and definitions used in the registries, management of the registries, the conditions for data exchange, and the obligatory use of registries by public bodies (to actually stimulate more efficient uses of data and one-time data provision). The project also instigates amendment of the Personal Data Protection Act and the General Administrative Law Act. Future legislation is expected with the introduction of additional key registries.

5.1.6. Electronic Crime Reports

In 2005, the Code of Criminal Procedure has been amended to accommodate electronic crime reports and records.²⁷ Further regulations may be issued to set the requirements for such reports and records.

5.2. *General Legislation Relevant to eGovernment*

5.2.1. Personal Data Protection

The Personal Data Protection Act 2000 (*Wet bescherming persoonsgegevens 2000*) implements Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.²⁸ When eGovernment activities encompass the 'processing of personal data', a notion that includes many different activities with respect to data (capable of) identifying an individual, and the processing of such data is not already covered by a more specific Act (e.g., the Municipal Database (Personal Records) Act), this Act applies to such activities. eGovernment services using citizen information are likely to be subject to the Personal Data Protection Act 2000.

geldende voorwaarden op het gebied van de belasting over de toegevoegde waarde, *Staatsblad* 2003, 530.

²⁶ *Kamerstukken II* 2005/06, 30 312, nrs. 1-4.

²⁷ Wet van 15 september 2005 tot wijziging van het Wetboek van Strafvordering (*elektronische aangiften en processen-verbaal*, *Staatsblad* 2005, 470).

²⁸ *OJ L* 281/31, 23.11.1995. See also: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *OJ L* 201/37, 31.07.2002.

5.2.2. Access to and Re-use of Public Sector Information

The Dutch Constitution holds an obligation for both government and the judiciary to observe openness (*openbaarheid*) in the course of their duties. Access to public-sector information has been predominantly regulated in the Government Information (Public Access) Act 1991. According to this Act, any person (including legal persons and public bodies) can request information, which is related to an administrative matter and contained in documents, held by a public body or organisation working on behalf of a public body. Access can be restricted on grounds of unity of the Crown, state security, company secrets, Dutch relations with other states and international organisations, state economic and financial interests, criminal investigations, personal-data protection, etc. In addition, public bodies must provide information relevant to a proper and democratic government of their own accord.

In 1998, access to environmental information has been included in the Government Information (Public Access) Act 1991 (implementation of Directive 90/313/EC of 7 June 1990 on the freedom of access to information on the environment).^{29 30} In 2004, the Aarhus Treaty was directly implemented into Dutch law.³¹ In 2005, two further directives,³² which were issued as a result of the Aarhus Treaty, were implemented in, amongst others, the Government Information (Public Access) Act 1991.³³

Presently, proposed legislation, which implements Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, is pending in the second chamber of parliament.³⁴ This law will, amongst others, add a chapter on re-use to the Government Information (Public Access) Act 1991.

5.2.3. Preservation of Government Information

The 1995 Archives Act (*Archiefwet 1995*)³⁵ and 1995 Archives Decree (*Archiefbesluit 1995*)³⁶ regulate the filing, storage and destruction of public-sector records. The purpose of the 1995 Archives Act is to guarantee the public nature and preservation of public-sector archives. This law does not contain any form requirements with respect to records and is, therefore, also applicable to electronic records and archives. The 2002 Regulation on the Arrangement and Accessibility of Records (*Regeling geordende en toegankelijke staat archiefbescheiden 2002*) does, however, contain complementary requirements for digital records, such as with respect to metadata on content, form and structure, and technical data on conversion, migration and storage.

5.3. Concluding Remarks

The regulatory framework for eGovernment is, on the one hand, made up of eGovernment-related legislation, which amends existing legislation relevant to

²⁹ OJ L 158, 23.06.1990.

³⁰ Wijziging Wet openbaarheid van bestuur ivm implementatie richtlijn nr. 90/313/EG inzake milieu-informatie, *Staatsblad* 1998, 180.

³¹ Wet uitvoering Verdrag van Aarhus, *Staatsblad* 2004, 519.

³² Directives 2003/4/EC (OJ L41/26, 14.2.2003) and 2003/35/EC (OJ L156/17, 25.6.2003).

³³ Implementatiewet EG-richtlijnen eerste en tweede pijler Verdrag van Aarhus, *Staatsblad* 2005, 341.

³⁴ *Kamerstukken II* 2005/06, 30 188, nrs. 1-6.

³⁵ *Staatsblad* 1995, 277.

³⁶ *Staatsblad* 1995, 671.

government communications, services and procedures in order to accommodate electronic equivalents, and, on the other hand, general legislation that applies to these government communications, services and procedures regardless of their electronic nature. In the first case, it is interesting to determine whether the adage ‘online = offline’, which was introduced by the ‘1998 Legislation for the electronic highway’ policy document, was followed by the Dutch legislator. This adage essentially means that the same norms should apply online as are applied offline.³⁷ eGovernment-related legislation, particularly, addresses the dematerialization, reliability and confidentiality, and efficiency of government services and communications. With respect to dematerialization, and reliability and confidentiality, legislation is aimed at providing electronic equivalents to paper and oral services and communications. The idea of functional equivalence, which is adhered to in that respect, clearly shows the intention to endorse the off-line situation. Because of an inherent unreliability of electronic communications, this often leads to supplementary requirements that guarantee authenticity and integrity of such communications, but such requirements do not detract from the essence of this adage. Ultimately, new legislation has in this area merely been introduced to extend legislation to electronic communications. With respect to a more efficient government, the situation is somewhat different, because in that case new systems (e.g., the key register and Citizen Service Number), which as yet do not exist in the off-line world either, are introduced to achieve the goals set by the government. Both systems will, however, impact the offline as well as the online world, although the effect may be more substantial with respect to the latter. Finally, it is worth recalling that recent eProcurement legislation introduces new possibilities (electronic auctions and dynamic purchasing systems) exclusively for the on-line world.

Moreover, it is notable that European law to a great extent influences the regulatory framework, i.e. EU directives, which over the years have been implemented into Dutch legislation, although this is obviously the case more generally and not as such specific to eGovernment issues. The ‘1998 Legislation for the electronic highway’ policy document expresses a preference for international regulatory action with respect to issues concerning the electronic highway, however, so far eGovernment is, regardless the European influence, predominantly still a national issue. Yet, this may change in the future, because a need to attune national eGovernment services and procedures at the European level clearly starts to surface and leads to, e.g., interoperability and standardization issues.

Finally, this section has shown that the regulatory framework for eGovernment consists of government legislation. In the Netherlands, self-regulation, for instance, is not a common means used for regulating eGovernment, although the ‘1998 Legislation for the electronic highway’ shows a preference for self-regulation in the short term to get ICT developments going successfully. Self-regulation is, however, not considered suitable where fundamental values and norms of the constitutional state are at stake, which explains to a large extent why this kind of regulation is omitted in the eGovernment area. Moreover, the interest of the government clearly outweighs the interests of companies and citizens in this respect, making eGovernment predominantly a government issue and not an issue in which the market and more generally non-government stakeholders are expected to take (a part of the) regulatory responsibility. Nevertheless, examples exist where self-regulatory instruments have an impact upon eGovernment. First, the TTP.NL scheme, which

³⁷ Schellekens 2006.

holds criteria for CSPs providing qualified certificates to the private sector (see section 3.3). This scheme is also applicable to those CSPs that wish to join the government PKI (*PKIoverheid*). A second example is the codes of conduct for ministries and municipalities on dealing with e-mail communications (see section 3.4).

6. Remaining Challenges

In view of the actual status of eGovernment in the Netherlands and the position of this country internationally, obviously the further development and sophistication of eGovernment services as such remains a challenge for the near future. More specifically, the persistent key issues that have legal implications or touch upon legal matters in Dutch eGovernment policy elaborated upon in section 3 (i.e. privacy, dematerialization of government communications, confidentiality and reliability of eGovernment communications, efficient eGovernment communications and service provision, interoperability of eGovernment data exchange, and access to and re-use of public sector information) deserve further attention while eGovernment progresses. This section will address the most pertinent remaining challenges for eGovernment for each of the key issues identified earlier.

6.1. Privacy

Data protection remains an important challenge with respect to most of the key issues, since most eGovernment services include the processing of personal data. In order to avoid problems, such as time and money-consuming technical, organizational and policy adjustments, at a later stage, data protection rules must be taken into account and implemented in eGovernment services right from the start. Such timely and correct implementation is not merely relevant in view of complying with data-protection rules, but is also likely to stimulate trust of citizens in eGovernment services.³⁸

Another important issue is progress in the creation of a digital identity infrastructure (including, e.g., the introduction of the Citizen Service Number), in which a digital identity (e.g., electronic signature, biometric passport) is linked to the physical identity of an individual. Such an infrastructure affects the protection of personal data and, more generally, the privacy of citizens, because in time their actions are at risk to become, dependent on fundamental (future) choices to be made, completely transparent within and perhaps outside the government information infrastructure.³⁹ Therefore, the Dutch Data Protection Authority advocates what is called privacy by design: government needs a proper identity infrastructure to be sure of a citizen's identity, however, not in every instance do citizens have to be identifiable within this system. Non-identifiability can in such cases be made part of the design of the identity infrastructure by, e.g., implementing privacy-enhancing technologies (PETs).⁴⁰ The increasing importance of issues such as identity and identity management, including the protection of privacy in that respect, is also evident from substantial European research projects, such as PRIME (Privacy and Identity Management for Europe, <<http://www.prime-project.eu.org>>) and FIDIS

³⁸ Versmissen & De Heij 2002, p. 10.

³⁹ Koops 2001, p. 1555-61.

⁴⁰ Versmissen, & De Heij 2002, p. 10, 13-17.

(Future of Identity in the Information Society, <<http://www.fidis.net>>). In Dutch government policy, these issues so far, however, remain highly underexposed.

Finally, a remaining challenge is citizen control with respect to own personal data. The Dutch Data Authority states that transparency is an important prerequisite for citizen trust in the government and one of the issues (among other issues such as access to public-sector information) in that respect is transparency of personal-data use by the government. The finality principle, i.e. personal data should solely be collected for clearly defined and specific purposes, used as a design principle for the information infrastructure plays a crucial role in stimulating trust.⁴¹ In this respect further monitoring of the development and adequacy of government initiatives, such as the possible integration of a service to provide transparency of personal-data uses with the Citizen Service Number (see section 3.4 on the roadmap to be introduced in draft legislation on this number), is important.

6.2. Dematerialization of Government Communications

The regulatory framework addressing the legal status of electronic communications must be kept up-to-date while technology progresses. Most laws mentioned in section 5.1 currently seem to be formulated sufficiently technology-neutral and, thus, capable of dealing with new technologies. However, technical rules that elaborate on these laws and go into further details on the technical specifics have to be monitored periodically in order to keep up with, for instance, new and updated standards. Also, the strong focus on advanced electronic signatures – and thus the specific technology of digital signatures – in electronic-signature legislation may need revision, when future technologies provide new forms of reliable and authenticated electronic communication. Moreover, while the dematerialization tendency proceeds, some legislation may still need adapting in order to encompass electronic communications and services.

6.3. Confidentiality and Reliability of eGovernment Communications

Besides persistent issues already mentioned in section 6.1, information security will continue to be a crucial point of attention in eGovernment processes because of the inherent vulnerability of ICTs. A recent incident, for instance, where security experts gained access to medical data of 1.2 million individuals in two hospitals as a result of inadequate security arrangements, has alerted the government again to ICT vulnerability and, thus, to the urgency of sufficiently adequate information security mechanisms. The introduction of electronic patient files in January 2006 has now been postponed with at least a year. Moreover, the government announced legislation on such files, which will address security and reliability issues.⁴²

6.4. Efficient eGovernment Communications and Service Provision

The Citizen Service Number to be introduced nationally in 2006 will in view of the criticism of the Dutch Data Protection Authority and the Council of State (see section 3.4) persist as an issue of further attention. The same is true for the way in which the government deals or, rather, does not deal (timely) with e-mail communications by citizens (see section 3.4). Efficiency can be effective only if the government practices what it preaches.

⁴¹ Versmissen, & De Heij 2002, p. 19-23.

⁴² *Kamerstukken II* 2004/05, 27 529, nr. 18.

6.5. *Interoperability of eGovernment Data Exchange*

As was mentioned in section 5.3, interoperability gets more and more important in the European context, as is shown by the IDABC programme (Interoperable Delivery of European eGovernment Services to Public Administrations, Businesses and Citizens, <<http://www.europa.eu.int/idabc>>). This programme aims at improving efficiency and collaboration between European public administrations by establishing pan-European eGovernment services.⁴³ Moreover, at the national level the interoperability of eGovernment services and processes and co-operation within the public sector remain relevant in view of the furtherance of eGovernment.

6.6. *Access to and Re-use of Public Sector Information*

The debate on the modernization of the Government Information (Public Access) Act 1991 as a consequence of, amongst others, ICT developments, and the introduction of a constitutional right of access to public-sector information as well as an accompanying obligation concerning accessibility of fundamental public-sector information as addressed in section 3.6 is still unsettled.

7. **Conclusion**

This status report shows a remarkable list of eGovernment policy initiatives. However, a lot of work still has to be done to bring eGovernment practice to a full and a more sophisticated momentum. To a large extent the regulatory framework is in place; yet some laws are presently still pending in parliament or being drafted by the legislator. Several key issues that have legal implications or touch upon legal matters in Dutch eGovernment policy can be identified, i.e. privacy, dematerialization of government communications, confidentiality and reliability of eGovernment communications, efficient eGovernment communications and service provision, interoperability of eGovernment data exchange, and access to and re-use of public sector information. These issues remain challenges for the future of Dutch eGovernment.

Because this paper has primarily addressed issues from a legal angle, some facets of eGovernment that effect society at large have remained underexposed. To conclude, these aspects will briefly be mentioned here. First, the advance of electronic communications and services increasingly seems to result in an elimination of traditional communication mechanisms (i.e., paper and oral communications).⁴⁴ Although the Act on Electronic Government Communications still optimistically propagates the optional use of e-communications, obligatory electronic tax declarations for business are a fact already. The legitimate question is how soon elimination will penetrate other public-sector areas and services? Second and related to the tendency of elimination, exclusion of citizens may occur as far as access to electronic information and services is concerned. Although a large majority of citizens is online nowadays, part of the population may – in spite of public computers in, e.g., libraries and other projects to win people over – for whatever reasons remain deprived of electronic access. Moreover, eGovernment seems to result in a shift in initiative

⁴³ ‘Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), *OJ* L181/25, 18.5.2004.

⁴⁴ Prins 2005, p. 1.

from citizen to government. Obviously, active service provision will contribute to such a shift, yet also plans by the Tax Authority to automatically fill in tax declarations for citizens. Some feel, however, that such a development will diminish the individual freedom of citizens to be known to the government as a certain person.⁴⁵ Finally, an area where challenges and issues mentioned in this conclusion and earlier in the paper come together is personalization of public service provision, i.e. the use of ICTs to tailor services and information to the individual needs and desires of citizens. Like identity management and identity fraud, this is an increasingly relevant issue not yet addressed (substantially enough) in eGovernment policy.⁴⁶

References

Van der Hof et al. 2004

Van der Hof, S. et al., *Aandachtspunten OTP, Over bestuursrechtelijke en andere juridische consequenties van de Overheidstransactiepoort*, Tilburg/Amsterdam, 2004.

Van der Hof et al. 2004a

Van der Hof, S. et al., *Over wetten en praktische bezwaren, Een evaluatie en toekomstvisie op de Wet openbaarheid van bestuur*, Tilburg: Tilburg University, 2004 (<http://www.rechten.uvt.nl/simone/Wobevaluatie_def.pdf>).

Holvast 2001

Holvast, J., *Mogelijkheden van het regie voeren over de eigen gegevens: juridische en technisch-organisatorische aspecten*. Onderzoek uitgevoerd in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Directie Informatiebeleid Openbare Sector, December 2001.

Koops 2001

Koops, E.J., 'Een nieuwe GBA, digitale kluisjes en identificatiedrang', *Nederlands Juristenblad*, 2001, p. 1555-1561.

Leenes 2004

Leenes, R., *Local e-Government in the Netherlands: From Ambitious Policy Goals to Harsh Reality*, ITA Manuscript, Austrian Academy of Sciences, Vienna, 12/2004.

Prins 2003

Prins, J.E.J., 'Het BurgerServiceNummer en de strijd tegen Identiteitsfraude', *Computerrecht*, 2003, p. 2-4.

Prins 2005

Prins, J.E.J., 'Verdringing: sluipend feit van deze tijd?', *Computerrecht*, 2005, p. 1.

Prins 2006

Prins, J.E.J., 'What's in a number', *Nederlands Juristenblad*, forthcoming 2006.

⁴⁵ Prins 2005, p. 1.

⁴⁶ Lips et al. 2004.

Schellekens 2006

Schellekens, M.H.M., *What holds off-line, also holds on-line?* in: Koops, E.J. *et al.* (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-liners*, Den Haag: T.M.C. Asser Press, forthcoming 2006.

Schreuders & Prins 2002

Schreuders, E. & Prins, J.E.J., *Met recht gestroomlijnd, Juridische normen voor authentieke gegevens, authentieke registraties en het gebruik van de daarin opgenomen gegevens*. Research report commissioned by the Streamlining of Key Data Programme Office, Tilburg: Tilburg University, August 2002 (<<http://www.stroomlijningbasisgegevens.nl/files/sbgmrg.pdf>>).

Versmissen & De Heij 2002

Versmissen, J.A.G. & De Heij, A.C.M., *Elektronische overheid en privacy. Bescherming van persoonsgegevens in de informatie-structuur van de overheid*, Den Haag, College bescherming persoonsgegevens, 2002.

Zouridis et al. 2004

Zouridis, S. *et al.*, *Een open tunnelvisie, Evaluatie van het TTP-beleid*, Tilburg: Tilburg University/Ordina Public Management Consulting, 2004.

Lips et al. 2004

A.M.B. Lips, *et al.*, *Issues of Online Personalisation in Commercial and Public Service Delivery*, Tilburg: TILT – Tilburg Institute for Law, Technology, and Society, Tilburg University, June 2004.

Cite as: S. van der Hof, *The Status of eGovernment in the Netherlands*, vol. 11.1 ELECTRONIC JOURNAL OF COMPARATIVE LAW, (May 2007), <<http://www.ejcl.org/111/article111-13.pdf>>.