Smeddinck, U.; Roßegger, U., 2013: Partizipation bei der Entsorgung radioaktiver Reststoffe – unter besonderer Berücksichtigung des Standortauswahlgesetzes. In: Natur+Recht (NuR) 35 (2013), S. 548–556

Voßkuhle, A., 2012: Neue Verwaltungsrechtswissenschaft. In: Hoffmann-Riem, W.; Schmidt-Aßmann, E.; Voßkuhle, A. (Hg.): Grundzüge des Verwaltungsrechts I. München

Winter, G., 2012: Aufstieg und Fall der Kernenergie in Deutschland. Verläufe, Erklärungen und die Rolle des Rechts. In: Zeitschrift für Umweltpolitik und Umweltrecht 2 (2012), S. 209–246; http://www-user.uni-bremen.de/~gwinter/kernenergieausstieg.pdf (download 4.10.13)

Kontakt

PD Dr. Ulrich Smeddinck
Institut für Rechtwissenschaften
TU Braunschweig
Bienroder Weg 87, 38106 Braunschweig
E-Mail: u.smeddinck@tu-braunschweig.de

« »

Security of eGovernment Systems

by Arnd Weber, ITAS, Linda Kool and Geert Munnichs, Rathenau Institute, and Anders Jacobi, Danish Board of Technology

European governments, as well as the European Union, aim at cost-efficient, convenient "electronic government", designing new processes, such as un-staffed border controls using electronic passports, public procurement with digitally signed bids and contracts, or trans-border usability of medical reports and prescriptions. A project conducted on behalf of the European Parliament on the *Security of eGovernment* addressed whether such transactions, often done on the Internet, are secure and efficient enough. The project report showed (1) that there is no comprehensive strategy for securing eGovernment against advanced threats, (2) that citizens' privacy could be better protected, and (3) that the possibilities of ICT are often overestimated by policy makers. The study was conducted between 2011 and 2013 on behalf of the Science and Technology Options Assessment Panel (STOA) by the Danish Board of Technology and its sister organisations, the Dutch Rathenau Institute and ITAS, members of the European Technology Assessment Group (ETAG). In this article, we introduce the approach used, highlight some findings from case studies, review some discussions from a workshop at the Parliament's premises, draw conclusions, and finally present some of the policy options identified.

1 Introduction, Objectives, and Approach

Digitisation of administrations is supposed to save money and to lead to greater convenience for citizens and businesses. Doing processes electronically can save costs for labour or the handling of paper documents. Moreover, citizens and business can use online services cheaply at anytime from anywhere, and, in the case of electronic delivery, can obtain a service within seconds.

Objectives of the project were to identify the security and privacy issues that emerge from the implementation of eGovernment, to identify whether the design of such electronic services is efficient, and to make policy makers aware of the problems and threats, in order to prepare for well-informed decisions on the future implementation of eGovernment in Europe. The project partners investigated three cases: electronic public procurement, electronic patient records and the biometric passport.

2 Case Studies

Biometric passport: The technical implications of the EU-wide introduction of biometric passports were underestimated. The expectation that the ePassport would significantly simplify border control could not be realised. For example, there are no EU-wide standards for the quality of passport photos and fingerprints. All too frequently EU member states opted for quick, user-friendly procedures, at the cost of the quality of biometric data. This led to high error margins at border controls. In practice, the fingerprints used in the passports prove difficult to use because not all member states wish to exchange their security system keys. As a consequence, the current system does not function well. In addition, a number of member states decided to use the data they collected also for investigations and fighting terrorism. The idea that this could all be done at once illustrates the lack of insight into the technological requirements. The present quality of the data collected for the biometric passport is too low for investigational purposes.

Electronic Procurement: Companies and public procurers must be able to be sure that operation-sensitive information is not accessible to anyone. The European Commission wants to require all bids above certain thresholds to be submitted in digital form by 2016. This is one more example of high political ambitions. It appears to be asking too much: a mere five per cent of bids are already digital. It is unclear whether complete digitisation is sufficiently reliable, with attacks on networks and computers becoming ever more ingenious. Various organizations, including NATO, have therefore decided to continue working with final contracts on paper. So one wonders whether full digitisation is always the best solution.

Electronic Health Data: The analysis of trans-border use of electronic health data revealed problems with the identification of health professionals and with the proper translation of electronic patient records and prescriptions. Another challenge is that of using health data for research purposes, which should be anonymous, but too often allows re-identification of individuals. On a different level, it was recommended that national ID cards should be kept separate from health systems. A baseline security for protecting health systems should be agreed on and implemented in all member states.

Please see the Case Study Report (Jacobi et al. 2012) for details.

3 Workshop, Discussions, and Conclusions

In an expert workshop, a number of overarching issues were discussed.

Security: Recent attacks showed that attackers can intrude even professionally managed systems, such as those of the security company RSA or those of the Coca-Cola Company. Therefore, systems must meet minimum security requirements, and system managers should follow extensive check-lists. As the above mentioned attacks have shown, crafted attacks are very difficult to protect against. What would help would be to isolate sensitive, internal data from arbitrary, potentially malicious data which may arrive in infected e-mail attachments. Gernot Heiser produced a White Paper for the project workshop to indicate how such isolation could be built in a provably secure way (see Jacobi et al. 2013a). Provably secure systems, protecting against attacks on confidentiality, availability or integrity of data, would even help against advanced attacks, such as those made by large organisations or those made with insider knowledge.

The US armed forces already have such a system available. European governments could make the use of similar systems mandatory. The Snowden revelations show that a European, open approach to highly secure computers would be beneficial in order to have a European base of computers free of backdoors.

On a different level, government IT data bases may contain errors, therefore it was concluded that citizens need more legal means to correct such errors.

Privacy: Governments should apply "Privacy by Design" in its ICT systems as a standard procedure. This might involve minimisation techniques (where only the data that is relevant for a specific goal is provided) or techniques that prevent data from anonymous files being traceable to individuals through "data mining". One example is the use of "attribute based credentials" whereby only parts of the identity of a person are exchanged (such as "over 18" or "nationality Dutch"). At present, often complete identity data are requested. "Privacy by Design" could be strongly stimulated by the establishment of a knowledge base with examples of system architectures and programs, in a European context or otherwise.

Feasibility: Policy makers are often too ambitious when it comes to ICT projects. A feasibility study in the draft phase of ICT projects is to show whether the various design requirements such as system security, user convenience, interoperability and last but not least cost efficiency are indeed compatible. Different system variants, with different interpretations of the design requirements involved, must be weighed against one another. This forces critical reflection on the actual goal that an ICT system is to serve and requires checks even after system roll-out.

Summarising, it can be said that the STOA study focused on the complex connection between system design, policy goals, and user risks. The different requirements set for an ICT system can clash. This demands careful weighing of the goal that a system is to serve, the data required for this – which means, as well, which data are *not* required – and the proper degree of system security, privacy protection, user convenience, and interoperability. The study showed that such weighing is still being insufficiently done. Independent experts and stakeholders should be involved in this. Members of Parliament, be it on national or EU level, must obtain insight into the results and the necessary considerations. A list of more detailed options is available in the project's report on policy options (Jacobi et al. 2013b).

References

Jacobi, A.; Folker, M.; Kool, L. et al., 2012: Security of eGovernment Systems. Case Study Report; http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Security%20of%20eGovernment%20-%20Case%20Study.pdf (download 14.11.13)

Jacobi, A.; Jensen, M.; Kool, L. et al., 2013a: Security of eGovernment Systems. Conference Report; http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Sec%20of%20eGovernment%20-%20Conference%20Report.pdf (download 14.11.13)

Jacobi, A.; Jensen, M.; Kool, L. et al., 2013b: Security of eGovernment Systems. Policy Options Assessment and Project Conclusions; http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Security%20of%20eGovernment%20Final%20Report.pdf (download 14.11.13)

Contact

Dr. Arnd Weber
Institute for Technology Assessment and Systems Analysis (ITAS)
Karlsruhe Institute of Technology (KIT)
Karlstraße 11, 76133 Karlsruhe, Germany
Phone: +49 721 608-23737
Email: arnd.weber@kit.edu

« »