Martin Rost

Large fires are best fought with large backfires, V2.0 – Data protection as the guardian of functional differentiation

The following text is intended to draw attention to the dramatically increased data protection risk posed by the use of citizen portals, single points of contact, and e-government gateways, as well as by social networks such as Facebook and the activities of Google Analytics and "smart meters." A common thread running through all of this is that the separation of functions, which is an essential feature of a modern constitutional state, is being undermined by organized access to personal data. What the unique personal identification number promises as a central linking symbol for relationships between individuals and organizations is actually being delivered by these current projects: All human data and communication relationships are conveniently accessible in a few centralized locations. Why is this a problem at all? And for whom? The relevant field for analyzing this finding is not data protection law, which is already a reaction to the latent conflicts, but sociology.

According to the epistemological findings of current social science theories, modern society no longer has a logical central attractor. Modern society cannot be adequately understood if everything is analyzed from the perspective of THE economy and THE capital or THE politics or THE science or THE law or even THE religion. It is characterized by a whole series of uncontrollable opacities that cannot be arranged hierarchically. Think of the uncertainties of the separation of powers and checks and balances, as well as those of the market, politically competing agendas and public opinion, changing political leadership at the top of the administration, unsettling scientific discourse, and artistic provocations. This modern society offers the majority of people, predominantly and from a historical perspective, good conditions for living, shaping their lives, and participating.

A person can and must take on different roles, the diversity of which contributes to the development of individuality that is worthy of protection. Freedom is evident, among other things, in the fact that the same roles can or must be shaped independently of one another in different forms and, more importantly, in different contexts. There is currently no central social authority that oversees the entire actions of an individual, orchestrates these actions into a coherent whole, and holds deviant actions accountable.[1]

At present, however, a few observation points are emerging where socially functional and personally desirable opacities can be eliminated through automated access to individual data. For society, this development could mean at least a partial elimination of functional differentiation and thus a relapse into a stratified social structure, which creates a latent pressure to justify oneself that threatens individual freedom.

1. The ongoing industrialization of administration

European authorities are currently working flat out to review their structures and processes with a view to optimizing them in terms of cost reduction, controllability, and technical feasibility. Compliance with legal requirements, which forms the basis of all administrative activities, is increasingly seen as a tiresome obligation that needs to be shaken off, and which is being tackled through harsh reforms such as Federalism Reform II. Laws, regulations, and responsibilities are being merged without further ado, or existing obstacles are being removed and then, like organizational and technical processes, standardized with the aim of industrializing administrative activities to reduce costs.

There is also external pressure to technologize administrative activities, from the economy, citizens, and technical developments. For example, the EU Services Directive requires that businesses be able to submit their business applications centrally to "single points of contact" (SPCs) accessible via the Internet throughout Europe.3 If an authority does not respond with a decision within a short period of time during the application process, approval is to be considered automatically granted.

Further pressure is exerted by the citizen portals designed by the Federal Ministry of the Interior. Citizen portals (CP) are intended to offer citizens, administrations, and companies a secure infrastructure, particularly for e-mail communication via the Internet, which keeps the technical effort for the unavoidable use of security programs low, especially for citizens.

Last but not least, the computer industry's promises are tempting, claiming that its products will make all internal and external communications of administrations more transparent, and thus finally controllable and more cost-effective, despite immensely increasing requirements, via central e-government gateways (GG). At the heart of government gateways are "message brokers" or "enterprise service buses," through which all communications involving a country's administration are centrally controlled, converted into the various formats of different procedures and programs, and then forwarded to recipients, typically via web services.

EAP, BP, and GG thus function as concentrators of functionally separated data sets and data flows for legal and natural persons as well as for machines that control the data streams among themselves. These three technologies completely cover the setup of communicatively accessible entities, namely: organizations interact with administrations via single points of contact, citizens interact with citizens via citizen portals, and machines interact with machines via government gateways.

The bundling of communication flows and data sets for natural and legal persons currently underway as part of administrative modernization through citizen portals and single points of contact, as well as through the message brokers of the e-government gateways in the administrative data centers, is therefore highly problematic from a data protection perspective, because it undermines the above-mentioned constitutional separation of functions in a modern constitutional state, particularly with regard to individuals. It makes a reality of what data protectionists have always fought against, namely the personal identification number, which is $^{\text{pointless}}$ to fight against from a purely technical point of view, but which can be considered a reality at the latest with the introduction of the tax ID number, and which only promised disaster: The portals and central news brokers make the data from the various communication relationships of individual citizens, customers, patients, and people very real, concentrated at only a few access points, and technically easily accessible.[10] They act as central linking entities directly to individuals.[11] Citizen portals, for example, must already encrypt, decrypt, or sign citizens' emails on their servers in order to deliver on the promise of convenience that no one has to deal with security procedures that are considered complicated but indispensable. This exposes this data to access and possible manipulation or malfunction by portal operators, as well as external attacks.

Concentrators for administration, unique users for the economy

The same trend toward concentration and organization can be seen in the private sphere, as demonstrated by Google Analytics and Google Meters (see DER SPIEGEL 2010/02) and social networks.

With the help of Google Analytics, it is often possible to generate so-called "unique users" across servers and organizations among web users. Unique users are profiles of network users whose observer, i.e., an operator of Google Analytics technology, knows many of the user's characteristics in detail, with the possible exception of the user's name and street address. The operator of Google Analytics knows the characteristic clickstream of the unique user and knows which links and servers, i.e., topics, this observed user typically clicks on. In addition, they can geolocate a user quite precisely based on the typical time of network use and the IP address pool used by the Internet provider. And if there is access to the globally unique MAC addresses or timing properties of a PC, the user's PC can even be uniquely identified.[12] The more data that can be collected from a web user in this way, the more detailed the profile of a unique user becomes. And if a unique user authenticates themselves at any point—for example, with Gmail or when placing an order with an operator accessible by Google Analytics—Google then even has the unique user profile assigned to a specific person. Google, which stores and evaluates the data obtained with Google Analytics centrally, may know a great deal about this person because information has been collected in a unique user profile over many years. And the use of the Google Chrome browser and, above all, Google mobile phones will certainly make it much easier to monitor users. So even if a user continues to use the web only passively for reading after the first sin of authentication under data protection law, the longer they continue to browse the web, the more likely it is that they can be identified as a specific user based on their browsing characteristics. They are therefore highly likely to be identifiable not (only) at the level of IP addresses, but also based on their content usage of the internet.

Data protection as the guardian of functional differentiation

What is the social function of data protection? Data protection ensures that communications between organizations (public administrations, private companies, scientific practices and institutes, private interest groups) and their clientele (citizens, customers, patients, people) are malleable. Malleable means that these communications are subject to conditions or can be made subject to conditions. Under data protection law, therefore, all communication must have a legal basis (law, contract, consent) that specifies the purpose and mutual assurances, and must be secured in terms of data protection and data economy.[5] The explicit purpose of the communication serves as a regulatory measure for the purpose of establishing the substantive legal assessability of such communications, which in turn requires the accessibility of the data collected and exchanged and the processes used in the process ("transparency requirement") in order to prove their necessity. The legal assessment of data processing is based on the legality of the communication, which ultimately amounts to a fair relationship in political terms and, in terms of fundamental rights, to respect for the ever-threatened autonomy of citizens, customers, patients, and human beings (as subjects and unique individuals) by organizations that latently imperialistically appropriate their clientele. Enforcing this respect on the part of the organization requires that the state also exert influence on its internal storage and use of information for the purpose of shaping communication. These normative requirements and technical implementations or assurances must therefore be designed in such a way that they can be reviewed by an uninvolved, neutral, external authority—in Germany, specifically, the data protection officers of the federal states and the federal government, as well as the supervisory authorities for the private sector—and sanctioned in the event of violations. Data protection should prevent customers from becoming puppets of private companies, citizens from becoming recipients of orders from public administrations, and people from becoming the disposable masses of practices or scientific institutions, without organizations having to forego the use of efficient information and communication machines.

The social function of data protection highlighted in the previous paragraph – namely that it focuses on the malleability of communications between organizations and their clientele – presupposes that communications and their content and forms are constructively accessible and not unconditionally fixed, for example by cultural and psychologically anchored traditions or technical precautions. Communications can only be subject to legal and operational conditions if data flows can actually be influenced operationally and regulatively, i.e., if different data sets are available and corresponding data streams from different sources cross existing boundaries of the stubborn constitution and processing of information. This in turn presupposes that there are stable communicative boundaries.

And there are already a whole series of such communicative boundaries. On the one hand, there is the communicative boundary between the law-oriented public administration and the capital-oriented private economy; on the other hand, there are the boundaries of the political sphere constituted by the separation of powers into jurisdiction, legislature, and executive, to which journalism can be added. In the current negotiations on the design of the new IT, the boundaries between different local, state, and federal authorities, as well as those with the EU and the United Nations, are also very practical. These discussions are about ensuring that institutions cooperate on an equal footing in terms of mutual access and the imposition of restrictions and claims, rather than being unilaterally subordinated.

The social sciences assert the existence of further social boundaries that ^{generate} communication and thus social systems. Modern sociology distinguishes between a) communities of interaction and b) organizations whose members are involved in the reproduction of decisions from decisions, as well as c) functional systems of society that provide functionally differentiated, specific forms of communicative accessibility.[7] The structurally leading social functional systems are economics, law, politics, and science. These social functional systems are characterized by the fact that they operate functionally separate from one another, meaning that political power, for example, cannot easily and without loss influence law, payments, or discourses on truth. Taxes are only costs in economic terms, but politically they are raw material for opportunities to shape society. There is no overarching functional system to which the other systems must conform. These equally "equal" social systems interfere with each other; they must construct their own forms of information from the disturbances in their environments. In doing so, they reproduce their boundaries as specific systems.

The separation of functional systems in modern times has led to an enormous diversity and complexity of social communications, which media training transforms improbable communicative connections into probable couplings. These systems have, and this is important for the aspect addressed here, first formed the communicative expectation patterns *of the citizen, the customer, and the subject*, which, delivered by society as generalized communicative role patterns, regulate the relationship between organizations and their clientele, on which the concrete role designs with concrete persons and their psychological expectations are then based. Citizens are considered sovereign, but must nevertheless submit to the state's monopoly on the use of force and to the law; customers are considered cost/benefit optimizers whose rational preferences may be influenced by seductive advertising and negotiating tricks; and humans are considered rational but instinct-driven individuals who therefore often act against their own interests. And when it comes to employees, we don't want to know too much about their actual sovereignty as citizens and human beings.[8] It is these contradictions that shape communication between organizations and their clientele in the first place. In this respect, the function of data protection is also to ensure that these contradictions are not resolved unilaterally but are reproduced as such. This is one of the reasons why data protection cannot be appropriated politically in a one-sided manner.

Traditionally, data protection has been suspicious of modern information and communication technologies. These technologies can too easily be used by organizations to misappropriate information for their own specific interests, even across functional boundaries, which can pose a concrete danger to individuals. Around the mid-90 , however, state-institutionalized data protection underwent a paradigm shift. Initial experiences with the internet showed, on the one hand, that certain areas of social reality were at risk of escaping legal control and, on the other hand, that there were improved opportunities to actually enforce fundamental rights. Progressive data protectionists therefore increasingly engaged in a game with the devil, or at least with fire: they sought technical solutions to embed data protection in technology and, once it had solidified in technical infrastructure, to enforce it ("Privacy Enhancing Technologies," PET). The task of designing technology in a manner that complies with data protection requirements is to ensure that data processing, which is itself technically supported, is planned, controlled, transparent, and secure, thereby allowing communications to be subject to conditions at the content level. This raises the question of whether or how the PETs developed over the last ten years can help solve the above-mentioned problems. We will return to this question shortly.

What can be done?

Two important developments in the context of PET should be noted. On the one hand, anonymization techniques and, on the other hand, "user-controlled identity management."

The aim of anonymization is to ensure that neither a web server operator nor an Internet access provider can identify where a user is surfing or what topics the user is interested in. Ambitious anonymization techniques also solve the problem of protecting users from the operators of the anonymization service. The core concept behind anonymization on the internet is to make internet-based communication relationships disappear within the largest possible anonymity group formed by the users of an anonymity service. This means that even a technically well-equipped observer on the Internet cannot establish a causally unambiguous relationship between events on the part of a user and events on the part of technical systems, such as web servers.[13] From a data protection perspective, all Internet use should be anonymous from the outset.[14] Only in the case of certain communications that require authentication, such as communications between citizens and customers with authorities and companies, must the communication partners be authenticated. But even identifying a characteristic of a person, such as whether they are of legal age, have a driver's license, or have health insurance, does not necessarily lead to the disclosure of the name and other data of a specific person. ^{A} great deal of communication can also be conducted under a pseudonym or with "anonymous credentials." However, such techniques cannot be used when users utilize a social web platform such as Facebook, which centrally organizes the removal of these social chains.

And smart meter applications must in turn be designed in such a way that they allow households to

User-controlled identity management is intended to help users employ different pseudonyms for different communication situations and transactions in the background The purpose of pseudonym management is, on the one hand, to prevent organizations from attributing data to individuals when a person only wants to obtain information and the attribution to the person is therefore not functionally necessary. More importantly, however, pseudonyms prevent organizations from linking different events together using the same name or pseudonym. To achieve this, it is necessary to be able to use a different pseudonym for each communication or transaction. Pseudonyms for everyday dealings with organizations must be able to be generated and discarded at will, at negligible cost and under the exclusive control of the user.[18] The occasion-related lifting of a person's anonymity or the disclosure of the assignment rule of a pseudonym to a specific person may only take place under constitutional conditions, e.g., with the approval of a judge. The current draft law on the operation of citizen portals takes a completely different view: Here, a portal operator is to decide for themselves whether it is justified to reveal a pseudonym upon request. The very fact that the pseudonyms of their users should be discoverable by the portal operator is unacceptable. And that is only one indicator of the unacceptable provisions of this draft in terms of security and data protection law

However, anonymization on the internet, which is currently largely based on users appearing under a single, massively used IP address, would have to be supplemented by further precautions that at least make it more difficult to profile unique users at the application level of internet use. For example, the browser could call up random pages in the background and then follow random links in order to level out the click characteristics of users. However, the effort involved is likely to be considerable. And social web platforms can only be used to a very limited extent, if at all, and under a pseudonym, which rather negates their actual purpose, namely the convenient maintenance of interactive, emotionally significant social relationships.

In general, anyone who wants to communicate securely via the Internet using the latest technology must install security programs on their own PC, within their own sphere of control.[20] This is increasingly the case, for example, for lawyers and notaries who want to use the electronic court and administration mailbox (EGVP) of courts or, increasingly, have to do so.[21] They use OSCI Transport security technology to transport data, which is considered a secure and auditable protocol according to the state of the art and is used by authorities for data transfer between themselves. In this form, with the aid of a connected card reader and a chip card, electronic signatures can be provided at a secure technical level and files can be securely encrypted in such a way that only the recipient addressed by the sender can decrypt them.

Instead of an obscure citizen portal, a project should be set up that enables citizens to install such programs, which are conceptually designed for security, on their own private PCs in order to be able to communicate securely and legally. There is a need to develop a truly functional technology that is offered even when demand is sluggish, if only to create the opportunity for a migration path so that in the future, better technology that actually delivers on its security promises can be used more widely. This is also part of a state's responsibility for infrastructure. Otherwise, poor technology will spread due to a lack of alternatives with the normative force of the factual.

The EAP could also be used more intelligently in compliance with data protection regulations. The core idea here is that the EAP models the application process across all administrations as an overall workflow, then formulates this workflow in its technical description, for example in OWL or BPEL[22], and transfers it to the applicant's PC. From then on, communication between the applicant and the administrations can take place directly, based on OSCI transport or a European equivalent. Although the EAP has access to a whole range of personal data and would also monitor the workflow, as required by the EU Services Directive, it does not need to view the content of communications between applicants and authorities· Controlling and operating would in fact be largely separated, in accordance with pure doctrine.

And finally: The technical systems of organizations, especially administrations, must be designed, configured, and operated in such a way that transparency can be established at any time regarding the purpose for which a system is operated, the functions and security levels guaranteed to the user, what the system has currently done with the data, or what the system has done with data in the past. To this end, the systems must be designed from the outset in such a way that they can be automatically verified.[25] In principle, such checks must be able to be carried out by the users themselves and, at a minimum, by experts on the basis of internal and external audits. One conceivable approach would be a technology that enables a user to instruct a proxy agent in the system to provide information about where a person's data was located, when, and to whom it was transmitted, when and for what purpose. Above all, however, independent and sanctionable external supervisory authorities must carry out these checks, supported by machines. Otherwise, under the industrialized conditions of administrations cooperating across Europe, it will simply be impossible to help those affected to exercise their right to informational self-determination.

Progressive data protection aims not only to preserve existing divisions of functions, but also to extend them into the organizations themselves, as required, for example, by the "social secret" for state service providers (cf. SGB I, §35), which, however, is currently not taken into account in any way. To achieve this, however, data protection would need to have a theory that would allow it to be better understood than it has been up to now, namely what social or, perhaps more precisely, what communication-ecological function it fulfills by observing the right to informational self-determination, which is aimed at the individual.[26]

[1] However, there are already some conflicting approaches, for example when health insurance companies begin to determine what they consider to be a healthy lifestyle when pricing their services, or when genetic dispositions restrict the lifestyle choices of individuals (cf. Stockter, Ulrich,2008 : Das Verbot genetischer Diskriminierung und das Recht auf Achtung der Individualität, Duncker & Humblot).

[2] To date, the registration system is the only administrative procedure in Germany that has been largely digitized. The aim of this pioneering project was to learn how to standardize and automate administration in Germany. Since1.1.2007 , almost5200 German registration authorities have been legally obliged to process and transmit registration data records exclusively electronically. This required many changes and adjustments to the registration laws of the federal states, as well as the development of a standard for technical representation ("OSCI-XMeld") and for secure and audit-proof transport ("OSCI-Transport") of data, so that it can also be sent via the insecure Internet.See OSCI Control Center, also for the history of the creation of the "Online Services Computer Interface": http://www1.osci.de/sixcms/detail.php?id=1181 .

[3] Concept: Germany Online Project Report "Blueprint" (as of:05.09.2008): http://www.deutschland-online.de/DOL_Internet/broker. Technical recommendations: von Lucke, Jörn; Eckert, Klaus-Peter; Breitenstrom, Christian,2008 : IT implementation of the EU Services Directive, design options, framework architecture, proposed technical solution – Fraunhofer Institute for Open Communication Systems, version2.0 , August 5, 2008.

[4] On the friendly goal of setting up a citizen portal: http://www.bundesregierung.de/ Content/DE/Magazine/MagazinSozialesFamilieBildung/064/t6-mit-buergerportalen-fuer-sichere-und-verbindliche-elektronische-kommunikation.html; Draft law and debate on the draft: https://www.ekonsultaton.de/buergerportalgesetz/index.php?page=viewcompiler_paragraph_items&id_view=14&menucontext=3&layoutfield=misc3; Explanatory notes on the draft law on citizen portals:https://www.ekonsultation.de/buergerportalgesetz/site/pictures/Erlaeuterungen_ Buergerportalgesetz.pdf; Presentation slides on the technical draft: http://www.eco.de/dokumente/ 080716_BP_Technische_Konzeption_v02.pdf.

[5] The Federal Data Protection Act was formulated under the influence of mainframe technology in a few state computer centers. Nowadays, PCs are on every desk, and computer systems are becoming ubiquitous, even extending into people's bodies. If we then factor in the foreseeable development of service-oriented architectures, according to which it is no longer possible to determine in advance which data will be processed with which process on which machine, it becomes clear that the BDSG expert opinion from2001 , and even the current amendment proposals from the middle of the year2008 (cf. https://www.datenschutzzentrum.de/vortraege/ 20080701-weichert-neuerungen-bdsg.html), must already be considered insufficient in parts.

[6] And thus generate information: Information defined as "a difference that makes a difference" (Gregory Bateson).

[7] See Luhmann, Niklas,1997 : Die Gesellschaft der Gesellschaft, Frankfurt am Main: Suhrkamp.

[8] Appeals such as that of the "citizen in uniform," like other appeals, for example, to the "customer as king," the "citizen as sovereign," or the "human being as an individual," characterize the latent problem, hardly the solution.

[9] Place of birth, time of birth, last name, first name, written together in this way, is operationally a unique personal identification number. It is used in the same way by organizations, with spaces in between.

[10] The providers of citizen portals are already technically perfectly prepared to access this data, namely via the lines through which the stored data is or will be accessible.

[11] The term "linking" is emerging as an attractive concept for a general theory of data protection that is slowly taking shape and spans technology, law, and organization, cf. Hansen, Marit/Meissner, Sebastian,2008 : "Linking digital identities." https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

[12] Which, in turn, could be desirable features in the context of digital rights management or trusted platform modules. For the double-edged nature of this, see Hansen, Markus: "Über die Auswirkungen von Trusted Computing auf die Privatsphäre" (On the effects of trusted computing on privacy). https://www.datenschutzzentrum.de/ allgemein/trusted_computing.htm.

[13] See the list of conceptually trustworthy Anon platforms: http://hp.kairaven.de/ bigb /asurf.html.

[14] Just as people who want to use a sidewalk do not have to identify themselves first. The use of roads with a car, on the other hand, is an application of pseudonymization, whereby the disclosure of the owner's name is strictly reserved for the police.

[15] See the Idemix concept, http://www.zurich.ibm.com/security/idemix/.

[16] Hansen, Marit; Berlich, Peter; Camenisch, Jan; Clauß, Sebastian; Pfitzmann, Andreas; Waidner, Michael,2004 : Privacy-Enhancing Identity Management; Information Security Technical Report (ISTR) Vol. 9, No. 1 (2004); Elsevier Ltd, Cambridge (UK);35-44 ; http://dx.doi.org/10.1016/S1363-4127(04)00014-7.

[17] See the EU project PRIME on user-controlled identity management: https://www.prime-project.eu/.

[18] Pfitzmann, Andreas; Hansen, Marit: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology; http://dud.inf.tu-dresden.de/ Anon_Terminology.shtml.

[19] And once the citizen portal is established, it is likely that citizens and customers will be effectively forced to connect to it, simply because administrations and companies will use this more cost-effective method as standard and make the more secure paper-based method more expensive.

[20] "Cloud computing" is the foreseeable next structurally significant attack on privacy, when not only are files stored on servers instead of on one's own hard drive, but programs are used that are installed somewhere out on the network instead of on a private PC. Users will then have even less control than they currently do over what happens to their data and the processes used to process it.

[21] See http://www.egvp.de/.

[22] OWL (Web Ontology Language) and BPEL (Business Process Execution Language) offer formal semantics that can be used to control organizational events.

[23] Directive2006/123 /EC of the European Parliament and of the Council of December 27, 2006, on services in the internal market: http://eur-lex.europa.eu/LexUriServ/site/de/oj/2006/l_376/l_37620061227en00360068.pdf.

[24] Rost, Martin,2008 : The slightly different model of the single point of contact (EAP), in: Administration and Management,2008/ 04 : 179f.

[25] The policies used to control web services will play a decisive role here. These policies translate legal requirements into technical instructions, which can then be verified for correctness and compliance during use with the aid of machine support.

[26] I would like to thank M. Häuser, M. Kamp, Dr. K. Storf, and W. Zimmermann for their critical discussion of the theses presented here.