AGREE

Good governance between freedom of information and data protection

An interview with Peter Schaar

Freedom of information and data protection are of crucial importance for the information society. The state must meet citizens with a spirit of openness. Transparent governmental actions should be the principle, and secrecy the exception. Being a democratic state also includes protecting the fundamental rights to data protection and information self-determination.

You are an expert for data protection, freedom of information and information self-determination. Where do you see the connection between good governance and the associated demands that should be placed on the government and administration?

Good governance includes transparency of governmental action. In a democracy, citizens have a right to find out how official decisions have been formed, and which arguments were ultimately decisive. Those affected by administrative action have been entitled to inspect the files relating to re relevant processes for years. Pursuant to the data protection laws, the right to information is equally restricted to the data of the of the data subject. However, such a limited claim to information is not enough. That is why almost all democratic states passed freedom of information laws in recent decades that grant every person the right – without proof of being affected themselves – to view files of the administration or obtain relevant information. Yet, good governance also means that state action must protect the fundamental rights of the citizens. Data protection and information self-determination are fundamental rights in Germany, as well as the European Union.

Almost every time good governance is mentioned, transparency comes up. In the context of data protection, good governance tends to relate to areas that should remain untouched. How does that fit together?

Data protection has several dimensions: Ensuring privacy, information self-determination and regulation of technology. As a result of the fast-paced development of information technology, an increasing number of areas in our lives can be examined. All types of devices, from smartphones to loudspeakers, from cars to beverage packaging are increasingly fitted with information technology. This makes it even more important to set legal limits for the collection, collation and analysis of the data. Data protection is not an end in itself; rather, it serves to safeguard free development of personality. If a person has to expect that all their activities are registered, they will not feel free, and forego their rights – such as freedom of expression or the right to demonstrate. The state, in particular, must exercise restraint in the collection of personal data – every-

thing else would be disproportionate and conflict with the constitution. Automated decision-making processes and risk assessment on the basis of big data volumes are of increasing significance. Now, this is where we need rules. It is paramount that the purposes for which data is processed become transparent, as well as the standards and methods employed in this processing. Transparency and data protection go well together in this context.

Freedom of information is crucial in a democratic constitutional state. What are the standards in Germany, and where can we expect changes, triggered on European level?

Above all, freedom of information means that the rule/exception relationship between secrecy and transparency is turned around. Traditional official secrecy is replaced with the entitlement to find out how authorities act, what decisions are made by whom, and which persons and institutions have contributed to the decision-making process. The Freedom of Information Act introduced on federal level around ten years ago fails to adequately satisfy this entitlement. There are still some federal states that have no freedom of information legislation at all. A number of exemption clauses in the existing freedom of information legislation prevent data being disclosed to citizens. Of course, some exemptions are justified: data protection, for example. What is particularly problematic is that business and trade secrets enjoy absolute protection – unlike personal data. The public interest in information must also be balanced with the economic interest of enterprises acting under public mandate. It is crucial that authorities start to actively publish data, rather than limiting data disclosure to instances where citizens request it. Since the administration employs automatic data processing for an increasing range of data, making relevant information available online would only involve manageable effort and expense. The Freedom of Information Act should therefore be advanced to a transparency law. Some federal states – in particular, this refers to the city states – have made more progress than others.

In connection with the new (internal) security requirements – where do you see the greatest threats for the right to freedom of information and data protection?

In recent years, the security agencies have been granted new authorisations of enormous scope for monitoring purposes. The Federal Constitutional Court and the European Court of Justice have both repeatedly objected to relevant laws. In my opinion, collecting data about unsuspicious people is the greatest problem; for instance, in data retention and the increasingly extensive video surveillance that is gradually equipped with face recognition technologies. Clear boundaries must be set here to prevent us ending up with total surveillance irreconcilable with a democratic constitutional state. The freedom of information has its own problems. For instance, intelligence services are exempted from freedom of information legislation in general. Unlike in the USA, there is no right to information access at all here. However, even Germany need more transparency in this area.

What would be your ideal case scenario for handling whistle-blowers?

Whistle-blower protection in Germany is rather poor – even compared to other European states. If someone reports or publicises violations of the law by enterprises or authorities, they have to be protected from being disadvantaged. Whistle-blower hotlines where the caller remains anonymous are of crucial importance.

How can data protection succeed in view of modern information and communication technology and its possibilities? (Why) Is that in the interest of administrations and governmental institutions?

There is no going back to analogue times. That is exactly why it is so important to formulate clear rules for the use of information technology. Data protection and IT security are key requirements for people trusting companies and authorities with their data. Trustworthy systems and responsible treatment of data are not only necessary in a state under the rule of law, they are also strategic factors in the rapidly progressing digitalisation of our society. The rule of law, fundamental and human rights must also be guaranteed under the new guaranteed.

Peter Schaar

Peter Schaar was Federal Commissioner for Data Protection and Freedom of Information (BfDI) from 2003 to 2013, and is now Chairperson of the European Academy for Freedom of Information and Data Protection (EAID) in Berlin.

Contact

European Academy Berlin
46/48 Bismarckallee
14193 Berlin, Germany
+49 30 895951 0
eab@eab-berlin.eu
http://www.eab-berlin.eu