Chapter 8
Erosion of Civil Rights in a Digital Society—Maintaining the Democratic Society

Jimmy Schulz

Vigilance Is Required

A Democratic, Federal and Free State Under the Rule of Law

After the Second World War, Germany was in need of a new constitution that would protect the people from the state and guarantee their fundamental rights. Therefore, the Basic Law for the Federal Republic of Germany was promulgated on 23 May 1949 in Bonn, Germany. At the same time, the Federal Republic of Germany was founded. This constitution substantiates the nature of the Federal Republic of Germany as a democratic, federal and free state under the rule of law. The essential characteristics are the Fundamental Rights, named in Article 1 to Article 19, which guarantee freedom and equality to German citizens. They are binding for all three powers: legislative, judiciary and executive power. Article 19, Paragraph 2 says: "*In no case may the essence of a basic right be affected*" (Tomuschat and Currie 2014). With this important paragraph, the German constitution protects itself from over-ambitious politicians. The authors of the Basic Law for the Federal Republic of Germany surely had no idea how digital transformation would affect our society. But that does not matter. Fundamental Rights are always valid, regardless of whether we need protection from the state in analogue life or in cyberspace.

With the progress of digital transformation, more and more decision-makers recognize challenges and possibilities of increased networking. But possibilities are not always positive, some of the new opportunities even have the power to destroy. To be able to focus on the positive ones and to avoid temptation, staunchness and conscience are the key required characteristics of decision makers.

J. Schulz (✉)
Committee on the Digital Agenda of the National Parliament of the Federal Republic of Germany, Berlin, Germany
e-mail: jimmy.schulz@bundestag.de

D. Feldner (ed.), *Redesigning Organizations*,
https://doi.org/10.1007/978-3-030-27957-8_8

The Big Eavesdropping Operation

Twenty years ago, in 1998, politicians in Germany decided to change one of the Fundamental Rights with the purpose of improving police work. Technical developments led to new possibilities, which brought forth a change in Fundamental Rights. This change affected Article 13: Inviolability of the home. The paragraphs 3–6 were added. These additions empowered executive authorities to use measures of acoustical surveillance in any home in which the suspect is supposedly staying, but only "pursuant to judicial order" and only under strict conditions. Furthermore, the idea of checks and balances is clearly reflected in this change. The executive power gets the right of acoustical surveillance, but only in consideration with the judiciary power. Additionally, the legislative power has to be informed regularly, which is specified in Article 13, paragraph 6.

Nevertheless, 20 years ago, this issue caused a huge controversy. A leading figure of the opponents of this Fundamental Right change was the former Federal Minister of Justice from the Liberal Democratic Party FDP, Sabine Leutheusser-Schnarrenberger. She tried to prevent the change of the law in her role as Federal Minister. When she realized she could not stop the law from passing, she consequently resigned from her post. But she did not stop fighting and brought an action before the Federal Constitutional Court (*GE: Bundesverfassungsgericht*) in Germany. With her liberal supporters—Gerhart Baum, the former Federal Minister of the Interior and Burkhard Hirsch, the former Vice-President of the German Federal Parliament—she finally succeeded in 2004, when the court delivered the judgment that large parts of the law violated human dignity and were therefore unconstitutional. The judges did not declare the changes in Article 13 themselves as unconstitutional, but numerous regulations in the Code of Criminal Procedures based on the changes of Article 13. Furthermore, surveillance should only be ordered on the suspicion of particularly serious crimes. Additionally, conversations between close relatives may only be intercepted if all involved parties are suspects and the conversation has criminally relevant content. If these conditions are not fulfilled, the corresponding records are not only worthless as evidence, but are not allowed to be made at all. In order to establish constitutionality in the conduct of surveillance, surveillance must be actively pursued by an official who, if necessary, stops monitoring as soon as the conditions specified by the court cease to exist. Any form of automatically recorded surveillance is considered non-constitutional. In summary, the right of the state to intrude into citizens' privacy is limited to situations that may pose significant risks for the community (1 BvR 2378/98 2004).

We can summarize that 20 years ago, when the process of digital transformation was still at its very beginning, politicians' ideas for using new technology for surveillance found fertile ground. It was the beginning of a steadily increasing number of comprehensive proposals to limit freedom.

But the plans from 20 years ago might seem kind of innocent compared to today's ideas. This development shows that we are still at the beginning of a revolution that might cause a huge impact on our free and democratic society. The following examples will underline this concern.

The Basic Law in Times of Digital Transformation—Under Constant Fire

Digital transformation is speeding up. New technologies like autonomous driving, hybrid humans, smart living and smart homes, new applications to simplify life, artificial intelligence in general and even digitized clothing are booming. A new generation of people, the so-called digital natives, are growing up with all these things, taking them for granted. But will this new generation also consider their civil rights as important, or will they become used to the fact that they are "transparent"? What is our duty now?

Data Retention

One of the key terms is data retention. For years, experts have emphasized that storing all communication without links to terrorism or even an involvement in crime is absolutely the wrong way to go. This does not lead to greater safety, but only to less privacy. With these data, it is possible to create a detailed profile of people. The state has access to information about the websites that citizens visit, who they called and where they were called from. Data retention can be used to identify social relationships and to provide a comprehensive background about people's private lives. Politicians who support this procedure consider every citizen a suspect.

In cooperation with supporters of civil rights, several politicians from the liberal party brought an action before the Federal Constitutional Court in Germany to stop data retention. At the moment, due to an unclear jurisdiction and several constitutional complaints, the law was put on hold until there is a judgment from the Federal Constitutional Court. Maybe it is easy to store all these data and then just look for what is needed to fight crime. It would even be easier to have a saliva sample of every person in a database and install surveillance software in every smartphone or computer (and car). Just because it is easy and possible, does not make it the right way to go. Unfortunately, the right way to go is complicated and expensive. Many people believe this is a price we should be willing to pay. About 40% of the German citizens are concerned that the state has steadily increased monitoring them as a result of technological development (Statista 2016).

Governmental Malware—Spyware Made by the Government

Another issue is a disturbing new law that was passed by the Conservatives and the Social Democrats in 2017 with regards to online searches and surveillance of telecommunication. The way this extension of state power passed the legislative process was considered controversial by many citizens and media: Two unrelated draft laws were in the middle of the normal legislative process when the Committee on Legal Affairs and Consumer Protection of the German Bundestag silently included (Deutscher Bundestag 2017) these far-reaching surveillance instruments into these draft laws. The "Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens" (BT-Drucksache 18/11277) (*EN: Law on the more effective and practicable design of criminal proceedings*) and the "Gesetz zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze" (BT-Drucksache 18/11272) (*EN: Law amending the Criminal Code, the German Juvenile Court Act, the Code of Criminal Procedure and other laws*) normally would not be associated with online searches and surveillance of telecommunications. However, following the decision of the Committee on Legal Affairs and Consumer Protection (BT-Drucksache 18/12785) adopted by the plenary, the amendments had been incorporated into the laws. Therefore, the legal foundation has been extended to allow the so-called "Quellen-TKÜ" (*GE: Quellen-Telekommunikationsüberwachung*), which means lawful interception at the device-level by malware, before any end-to-end encryption can be applied. Also, online searches were added, which provides the executive powers the right to search computers and smartphones by installing malware.

By pursuing this legislative procedure, silently including far-reaching restrictions on privacy in the middle of the legislative process, a public debate nearly failed to appear. The government avoided the standard process, which consists of three readings in plenary and the involvement of the German Bundesrat. In the German Bundesrat, the federal states participate in the legislation of the federation. The Federal Data Protection Commissioner was also not involved (cf. Beuth and Biermann 2017; Grunert 2017).

With this new law, the state granted itself the right to use spy software on smartphones and computers of suspects—not only to prevent terrorism, but also to detect, for example, counterfeiting of documents or tax evasion. Nevertheless, online searches should only be applied if the alleged offense is particularly serious. But this is not the case with the use of spy software for the purpose of telecommunication surveillance. The problem is that the software used for telecommunication surveillance is able to monitor much more information than lawfully permitted.

The "Quellen-TKÜ" has the goal of lawfully intercepting encrypted communication. The other part, the online searches, goes a significant step further and implies the ability to search through all data—for example, data that is stored on a smartphone (or accessible via the cloud). The Quellen-TKÜ is supposed to be similar to the interception of a telephone call, and the online search is comparable to the search of an apartment. However, this important separation, which the legislator has envisaged, is extremely difficult to implement from a technical point of view. Unfortunately,

past reports have shown that the state has been using software that was not covered by the legal framework, because the trojan used had significantly more capabilities than permitted by law.

In addition, the installation of this malicious software obviously requires the exploitation of existing vulnerabilities in IT systems. This constitutes a weak point for overall IT security, as the state participates in the trade and the dissemination of IT security vulnerabilities and prevents their effective remediation. This can lead to major collateral damages to innocent citizens, as well as companies. The use of backdoors and the participation of the state in digital black and grey markets in order to acquire knowledge about security vulnerabilities or so-called zero-day exploits from third parties are incompatible with the basic values of our liberal-democratic order.

What's Next? Public Surveillance Ideas

Data retention and governmental malware are two examples of these kind of ideas that should make "evil" cyberspace safer, better or less complicated. But in the end, they restrict the freedom of citizens. There are many other suggestions, such as face recognition in public, which has already been tested by the federal government at Berlin-Südkreuz, a heavily frequented train station in the middle of Germany's capital city. Another suggestion is the possibility of recognizing emotions via software. Some politicians think that terror attacks could be prevented—for example, at an airport—by identifying potential terrorists via monitoring of "dangerous" facial expressions. One can imagine many different reasons that a person might look stressed, angry or in any other form "dangerous" at an airport, such as if a flight is cancelled at the last minute. Such a surveillance of emotions would significantly curtail citizen liberties and constitute a huge loss of freedom.

Freedom of Speech—Online and Offline

In a democratic society, freedom of speech is fundamental. In Germany, it is written down in Article 5 of the constitution: Freedom of expression, arts and sciences. It says in paragraph 1: "*Every person shall have the right freely to express and disseminate his opinions in speech, writing and pictures, and to inform himself without hindrance from generally accessible sources. Freedom of the press and freedom of reporting by means of broadcasts and films shall be guaranteed. There shall be no censorship*" (Tomuschat and Currie 2014). Today, many people get their information through social media platforms. They use them to get updates and news from their friends or to share their thoughts and opinions. This novelty that allows everybody to express him- or herself online through a blog or a social media profile has advantages for a great majority of people. But some people use this chance to distribute lies, hate speech and even illegal content. This has led German politicians to propose the rules to require that social media companies like Facebook and Twitter quickly remove this kind of

content from their sites, or face having to pay high fines. This model is now also being discussed on the European level. About 45% of the German citizens believe the so-called German Netzwerkdurchsetzungsgesetz or "NetzDG" (*EN: Network Enforcement Act*) constitutes a serious threat to the freedom of expression of the public (Civey 2018). It therefore should not become a role model. The concern about this model is that there is a risk that, in case of doubt, the companies concerned will opt for deletion of online content in order to avoid paying high fines.

Moreover, it is unacceptable to allow companies to act like judges and decide which content is covered by the right to freedom of expression and which is not. This is primarily a governmental task and will cost money, because more judges with a special training are needed.

Some European politicians even promote the idea of obligating online services to monitor and filter content, even before it's uploaded, by introducing so-called "Upload Filters". This would mean that private companies decide which content is allowed to be distributed online—taking a significant step towards censorship.

Bavarian Surveillance Fantasies Threatening a Whole Country

The past has shown that many ideas curtailing civil rights came from the conservative side of the political spectrum. Many of these ideas have their origin in Bavaria. The conservative party, called CSU (*DE: Christlich Soziale Union*), has governed Bavaria since 1957. This is a local Bavarian party, which builds a union with the CDU (*DE: Christlich Demokratische Union Deutschlands)* on the federal level. The CSU had a majority in the Bavarian Parliament in 2018, meaning they could easily make far-reaching political decisions. Furthermore, a new party appeared and gained strength against the background of the refugee crisis in 2015 in Germany. The AfD (*Alternative für Deutschland*) is another very conservative and nationalistic party that seems to be attractive to very conservative, perhaps some of them former CSU, voters. Therefore, the CSU had to regain their attention, especially with regard to the Bavarian State Elections on 14 October 2018. Additionally, the former Bavarian Prime Minister was nominated as German Federal Interior Minister half a year before the elections. In his first speech in the German Bundestag as Federal Interior Minister, he announced the desire to make Bavaria a role model for Germany as a whole.

Police with Secret Service Tasks

In 2018, the Bavarian government (CSU-led) drafted a law for the Bavarian parliament (CSU majority) that many have equated with turning the police force into an intelligence service. The plans of the so-called "Gesetz zur Neuordnung des bayerischen Polizeirechts" (BayLT-Drucksache 17/20425) (*EN: Law on the reorganization of the Bavarian police law*) lead to a weakening of judiciary power. As was the

case 20 years ago, surveillance only was permitted "pursuant to judicial order" under strict conditions. The CSU wants to change this. Additionally, the law would allow the police to make videos while people participate in peaceful assemblies, butting up against Article 8 of the Federal Constitution, which guarantees the "Freedom of assembly". The draft law includes additional controversial ideas. It would allow police to spy on computers and smartphones if they think there is an imminent danger. The police could also change and delete information on these computers under special circumstances. Since the foundation of the Federal Republic of Germany and, thereby, the establishment of the German Basic Law, no police force ever had similar powers. Additionally, Members of the Bavarian Parliament submitted amendments to make this law even stricter—for example, by obligating IT companies to implement vulnerabilities in their products that could be used by the state. People all over Germany (more than 30,000 citizens in Munich, the capital of Bavaria) demonstrated against this law (Süddeutsche Zeitung 2018).

Recommended Steps to Protect Civil Rights

Transforming Possibilities into Chances

New technologies offer many possibilities to make police work more efficient but also to restrict the civil rights of a country's citizens. There are many controversial ideas popping up that are discussed, decided upon, implemented, concretized and sometimes even withdrawn. Without a doubt, the digital transformation has the potential to lead people to another age of democracy, with another view on civil rights and transparency—this is already happening.

The previous explanations focused on the dangers to civil rights while a democratic digital transformation is happening. But citizens should not be scared when it comes to the future and technical innovations. There is a lot of power in this digital transformation, along with many positive ideas that can help save and improve lives. Politicians and citizens would do well to focus more on these beneficial ideas. The question is: How can they succeed?

Investing in Education—Sensitizing People—Enlightening Politicians

To seize the full potential the digital transformation has to offer for society, there are three tasks that can be focused on: providing a better (also digital) education, raising awareness and being persistent. The future generations must be prepared to handle new technologies at school and older generations should never stop learning. In particular, multipliers like politicians or teachers should refresh their knowledge of history and explain the reasons and the importance of fundamental rights to everyone. Furthermore, today's stakeholders have the responsibility to deal with the

consequences of their decisions. There need to be social debates about civil rights in the digital world, and multipliers need to be able to counter the attitude of people who say, "Surveillance is ok. I can accept it because I have nothing to hide".

A Right to Encryption

One of the basic rights in a digitized society is online privacy. On the one side, Article 10, paragraph 1 of Germany's Fundamental Rights states that "*the privacy of correspondence, posts and telecommunications shall be inviolable*" (Tomuschat and Currie 2014). If people send letters, they regularly use an envelope. But emails are often sent unencrypted, which is comparable to a postcard—anyone could read it. For that reason, a right to encryption is needed. This implies that all providers of telecommunication services should be obligated to offer the standard version of their communication service (end-to-end) encrypted.

Good Ideas from Politics

Luckily, there are also many positive political initiatives. Two of them are particularly noteworthy. As early as April 2016, the European General Data Protection Regulation (GDPR) (EU 2016/679) was adopted, and it became effective on 25 May 2018 after a two-year transition period. It establishes a harmonized data protection framework in all 28 Member States of the European Union. This regulation enables all individuals in the European Union to have control over their personal data via several instruments. The GDPR is based on several principles. One is the principle of explicit consent as the foundation for data collection and processing (opt-in), which also strengthens the data protection authorities as it provides for the possibility to impose severe sanctions in the case of data protection infringements—such as fines of up to €20 million, or 4% of the annual worldwide turnover of a company, depending on which sum is higher.

Furthermore, negotiations of the so-called ePrivacy Regulation, are taking place on the European level. The regulation's goal is to ensure "*the protection of fundamental rights and freedoms […] in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data*" (COM/2017/010 final—2017/03 (COD), Article 1). It will complement the GDPR with regard to electronic communications data. The ePrivacy Regulation could ensure that the same high privacy standards apply for so-called Over-the-Top communications services (e.g., widely used messenger services), as well as "traditional" telecom operators in the future.

The GDPR and the ePrivacy Regulation are important steps to ensure that all over Europe, people and businesses profit from a harmonized set of rules that strengthen the sovereignty over their own data. Data sovereignty is fundamental, if we want to ensure the autonomy of each citizen in the digital world.

Courage First—Concerns Second

"Digital first—Bedenken second" (*EN: digital first, concerns second*)—this claim was used by the Free Democratic Party (FDP) to promote innovative ideas for the digital sphere in the campaign for the Federal Elections in 2017 in Germany. This is the attitude toward new technologies that leads to great innovation. There is not a contradiction between this claim and the former explanations, as long as the fundamental rights of all people are guaranteed, and they are empowered to profit from the opportunities offered by digital transformation.

This is the guiding principle on which an international ethical fundament could be built on. The internet is a good thing after all!

References

BayLT-Drucksache 17/20425 vom 30.01.2018, Gesetzentwurf der Staatsregierung für ein Gesetz zur Neuordnung des bayerischen Polizeirechts (PAG-Neuordnungsgesetz), URL: http://www.bayern.landtag.de/www/ElanTextAblage_WP17/Drucksachen/Basisdrucksachen/0000013000/0000013038.pdf Accessed May 08, 2018.

Beuth, P., & Biermann, K. (2017). Staatstrojaner. Dein trojanischer Freund und Helfer, DIE ZEIT online, 22.06.2017, URL: https://www.zeit.de/digital/datenschutz/2017-06/staatstrojaner-gesetz-bundestag-beschluss Accessed May 08, 2018.

BT-Drucksache 18/11272 vom 22.02.2017, Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jungendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze, URL: http://dip21.bundestag.de/dip21/btd/18/112/1811272.pdf Accessed May 08, 2018.

BT-Drucksache 18/11277 vom 22.02.2017, Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, URL: http://dip21.bundestag.de/dip21/btd/18/112/1811277.pdf Accessed May 08, 2018.

BT-Drucksache 18/12785 vom 20.06.2017, Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz, URL: http://dip21.bundestag.de/dip21/btd/18/127/1812785.pdf. Accessed May 08, 2018.

BVerfG, Urteil des Ersten Senats vom 03. März 2004, 1 BvR 2378/98—Rn. (1-373), bverfg.de, URL: http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html Accessed May 08, 2018.

Commission proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final—2017/03 (COD), 10.01.2017, URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:10:FIN Accessed May 08, 2018.

Deutscher Bundestag, Bundestag gibt Strafermittlern neue Instrumente in die Hand, Deutscher Bundestag, 2017, URL: https://www.bundestag.de/dokumente/textarchiv/2017/kw25-de-aenderung-stgb/511182 Accessed May 08, 2018.

Grunert, M. (2017). Bundestrojaner. Durch die Hintertür zur Online-Überwachung, faz, 22.06.2017, URL: http://www.faz.net/aktuell/politik/online-durchsuchung-quellen-tkue-bundestrojaner-wird-gesetz-15071053.html Accessed May 08, 2018.

NetzDG: Einschränkung der Meinungsfreiheit? - Umfrageeregebnisse 03.08.2018, Civey 2018. URL: https://civey.com/umfragen/netzdg-einschraenkung-der-meinungsfreiheit.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 27.04.2016, URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32016R0679 Accessed May 08, 2018.

Menschen demonstrieren gegen Polizeigesetz, Süddeutsche Zeitung, 10.05.2018, URL: https://www.sueddeutsche.de/muenchen/massenproteste-in-muenchen-menschen-demonstrieren-gegen-polizeigesetz-1.3974427 Accessed August, 08 2018.

Tomuschat, C., & Currie, D. P. (2014). (translators), Basic Law for the Federal Republic of Germany, Juris. URL: https://www.gesetze-im-internet.de/englisch_gg/index.html Accessed May 08, 2018.

Umfrage in Deutschland zur Befürchtung, dass der Staat die Bürger überwacht, Statista/ IfD Allensbach (ACTA 2016), 2016, URL: https://de.statista.com/statistik/daten/studie/282285/umfrage/staatliche-ueberwachung-der-buerger–befuerchtung-in-deutschland/ Accessed: August 08, 2018.

Jimmy Schulz is a German internet entrepreneur and politician of the Free Democratic Party (FDP) from the district of Munich, Bavaria. After finishing his secondary education at the Ottobrunner Gymnasium, he studied political science at the University of Texas at Austin and in Munich, Germany. His passion for IT started at school, during which he worked at various IT companies and later, in 1995, founded CyberSolutions GmbH, which entered the stock market in 2000. He is currently CEO of CyberSolutions Ltd., which has its company seat in Riemerling/Hohenbrunn. Jimmy Schulz has been actively fighting for civil rights and internet freedom for more than 20 years. From 2009 to 2013, he was a member of the German Parliament. He was spokesperson for the FDP in the commission of enquiry: “Internet and digital society”. From 2014 to 2016, he was a member of the ICANN At-large Advisory Committee (ALAC) and Vice Chairman of the Internet Society ISOC Germany (2015–2017). Since 2018, he has been a member of the Presidium of ISOC Germany. In 2017, he was again elected as a member of the German Parliament and is now chairing the Committee on the Digital Agenda.