The German IT Security Law 2.0: More Shadow than Light?

More Duties and Power Extensions for the Federal Cybersecurity Authority

Dr. Dennis-Kenji Kipker | Wissenschaftlicher Geschäftsführer | Universität Bremen

25. März 2021
LR 2021, Seiten 65 bis 69 (insgesamt 5 Seiten)

On May 5, 2020, a new draft of the IT-Sicherheitsgesetz 2.0 (IT Security Law 2.0, "IT-SiG 2.0") was published, which has already been the subject of several legal discussions. In summary, the legislator intends to make changes and extensions to multiple legal acts, including Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (Federal Cyber Security Authority Law, "BSIG"), Telekommunikationsgesetz (Telecommunications Law, "TKG"), Telemediengesetz (Telemedia Law, "TMG") and Außenwirtschaftsverordnung (Foreign Trade and Payments Ordinance, "AWV"). The commonly discussed amendments include, in particular, the introduction of the KRITIS (critical infrastructure) sector called "disposal" and new categories of "companies in the special public interest" and of "guarantee declarations for critical components". In addition, there are plans to expand the competences and the scope of duties of Bundesamt für Sicherheit in der Informationstechnik (The Federal Cybersecurity Authority, "BSI") and to initiate a national IT security label. The aim of this contribution is to provide an in-depth legal analysis of these newly introduced laws, while also evaluating the major differences between their current drafts and their initial versions from 2019. It is worth mentioning that the official explanatory memorandum for this legal act and its critique discussed in this contribution both lack a secure basis in terms of knowledge and information, due to the fact that – up until now – the "IT-SiG 1.0" did not undergo an appropriate evaluation. This crucial step in the legislative process was also skipped in regard to the newly proposed amendments to Netzwerkdurchsuchungsgesetz (Network Enforcement Act, "NetzDG"), pertaining to the handling of hate speech and right-wing extremism. A proper and broad assessment preceding the legislative process would have been particularly useful in regard to the IT-SiG 2.0, as it could have provided answers to questions concerning the need to introduce some of the planned regulations.

The current draft law provides for several new duties and power extensions for the BSI. These include the activities of the BSI as a conformity assessment body under § 3 I 2 no. 5a BSIG-E (BSIG-draft) and as a national authority for cybersecurity certification under § 3 I 2 no. 5b BSIG-E. The assignment of new duties in connection with the latter function is intended to support Article 58 of Regulation (EU) 2019/881 of 17 April 2019 (EU Cybersecurity Act) and to render it more precise and it generally fits into the cybersecurity strategy of the Federal Government. Additionally, § 3 I 2 no. 19 and 20 BSIG-E provide the BSI with the task of developing and evaluating identification and authentication procedures. Furthermore, the BSI is to be in charge of developing and publishing the new "state of the art" standard for cybersecurity requirements for IT products. These changes initially raised the question of overlapping with Article 42, 32 and 57 EU-GDPR, as well as questions about the scope of application of the EU-eIDAS regulation. The draft itself understands the purpose of § 3 I 2 no. 19 BSIG-E as clarification and specification of the eIDAS-regulation on a national level. Hence, the legislator does not seem to see any legally problematic overlap between the European regulation and the IT-SiG 2.0. However, it remains unclear in the draft law to what extent the BSI is now supposed to support the existing data protection authorities in their work and what the relation is between the new concept of certification and certification within the meaning of Article 42 EU-GDPR.

The development and definition of what the law considers to be the "state of the art" also offers further reasons for criticism. This task is of utmost importance for critical infrastructure operators, since they are obliged to maintain the state of the art standard in their operations, according to § 8a BSIG-E. The explanatory memorandum states that the development of the state of the art – which is seen as linked to the conformity assessment performed by the BSI – is indispensable for consumer protection and necessary to guarantee uniform requirements. However, in its current structure, this prima facie reasonable concept bears some problems. First and foremost, the BSI is not obliged to include critical infrastructure operators in the development process. From a legal-political and economic points of view, it further seems unreasonable to not firmly include the observation and integration of international standards in the decision-making process, either. The same point of view reveals the problem of the fragmentation of IT security regulations within the EU. The above leads to the conclusion that the government would be well advised to involve critical infrastructure operators in this process, as part of the next revision of the draft. Furthermore, the integration of international technical standards into the law should be considered before resorting back to more national efforts. Though the latter does not render the draft act incompliant with the provisions of law, it would be desirable to create a framework that prevents such fragmentation of cybersecurity regulations, as much as possible. The new framework must draw from existing international standardization to avoid duplication of effort.

Furthermore, § 4b BSIG-E intends to expand the BSI's role as the general reporting office for cybersecurity, whereby § 4b III BSIG-E states the BSI's authority to pass on information it receives within its capacity as reporting office. It also provides it with the possibility of filing reports to other federal authorities. Along with this comes the call for greater institutional independence of the BSI, in view of its general key position in the cybersecurity landscape of Germany. In addition, § 4b III BSIG-E has been designed as an "optional" provision; nevertheless, for cybersecurity in Germany to be effectively strengthened by the work of the BSI, the decision to report significant information to the relevant actors should not be left to the discretion of the BSI, but rather constitute its obligation.

Like the first draft, the IT-SiG 2.0 inserts provisions on crisis reaction plans into the BSIG. These are referred to in § 5c BSIG-E as an "overall plan for federal reaction measures" and are developed by the BSI in agreement with Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (The Federal Office of Civil Protection and Disaster Assistance) and with respective supervisory authorities. However, the affected operators of critical infrastructures, companies of special public interest and suppliers of critical components are merely consulted. They do, however, have the opportunity to contribute their own crisis reaction plans to the process and thus make use of their detailed knowledge about their own IT systems in this way. Often times, the operators have by then already drawn up crisis reaction plans in their own economic interest, which is why such consultation will usually not require extraordinary effort on the part of the companies; therefore, good use can be made of existing knowledge. Without sufficient involvement of the operators, the suitability of the crisis reaction plans developed externally by the BSI would be questionable, since the IT systems of such companies are complex by nature and vary from one infrastructure to another. As a result, without such involvement, an efficient design of crisis response plans is hardly conceivable. Attacking this provision as an unnecessary delegation of power to the state isn't convincing, in light of regular cybersecurity incidents, without an adequate reaction of commercial enterprises.

Moreover, the scope of authority of the BSI proposed in § 5c IV BSIG-E significantly interferes with internal company processes. Thereby, the BSI may request that certain (also personal) data be made available in the event of a serious malfunction within the meaning of § 8b BSIG. Furthermore, the BSI is to be authorized to directly intervene in the systems and corporate processes of the operator in order to restore their functionality and security. This provision would only come into effect in the event the affected organization does not or cannot remedy the malfunction itself.

Prima facie, the obligation to surrender the data required to cope with the incident could be criticized to the extent that the wording does not further specify such data and that the explanatory memorandum does not show any consideration for the interests of third

parties. However, such critique is refuted by the wording of the draft act, which supplies the BSI with discretionary powers in this regard. This must – according to the general dogma of the German administrative law – inevitably involve weighing the BSI's decision to request data against the legally protected interests of the subjects concerned by this request.

In contrast, the BSI's right to "take the necessary measures on its own" is controversial, since the response plans already drawn up by the operators are often the subject of successful certification procedures and regularly comply with international standards such as ISO/IEC 27001. In addition, it could be argued that operators of critical infrastructures have a vested interest in the rapid restoration of the operability of their systems and therefore governmental interference should be kept to a minimum. This last argument loses its "firing power" in that the BSI may only issue such orders if a timely reaction by the operator is not possible or cannot be expected; in any case, this law cannot justify a disproportionate response. Operators have further criticized the lack of special liability provisions in the draft act, regarding unlawful damages resulting from intervening measures taken by the BSI. In the event of such damages to the operator's system, compensation can be guaranteed by the instruments of state liability law, which is applied on case-by-case basis, and common law in the German legal system. The absence of an explicit liability regulation may therefore be unfavorable from a business point of view but corresponds to the previous methods of handling of potential state liability cases by the legislator.

In addition, the media has repeatedly referred to § 7b BSIG-E as the so-called "hacker paragraph", which enables the BSI to detect security gaps in publicly accessible systems and which thus colloquially labels the BSI as a "hacker authority". § 7b II BSIG-E indicates the situations when such a system is unprotected; however, the draft does not define the term "public access". This section must be read in combination with § 7a BSIG-E, which provides for the right to investigation and the right to information, enjoyed by the BSI in regard to the respective companies. The interests of these companies and any third parties, also with regard to business secrets, must be protected and considered by the BSI when making its discretionary decision. In this context, it is desirable that separate security requirements for the transmission procedure be standardized in order to protect sensitive data. Furthermore, the right to detect security gaps in publicly accessible systems only exists for the purpose of pointing out possible security gaps to the operator and to inform them about their existence, whereby port scans, sinkholes, and honeypots ought to be used in particular. Nevertheless, penetration tests and red-team activities are not explicitly excluded, although these can endanger the critical infrastructure and thus do not necessarily increase security, but may even pose a threat themselves. It would be

conceivable to minimize this risk of failure occurring within the operator's system due to these hacking activities if the BSI had to notify the targeted company.

To come to a conclusion: At first glance, the current draft of the IT-SiG 2.0 contains some sensible regulatory approaches, but, overall, it appears to cast more of a shadow than light on some of the existing issues. This is primarily a result of combining various fundamentally good concepts that do not seem to have been entirely thought through. The considerable criticism regarding the first draft from 2019 has apparently not been, to a large extent, considered by the legislator. Against this background, an evaluation of the already existing laws concerning cybersecurity in Germany is more desirable than ever. The goal of creating a uniform European solution for IT security should also be aimed at much more strongly than before, in lieu of promoting national solo efforts, such as the new IT security label. Existing EU instruments, e.g., the 5G Toolbox, as well as European and international technical norms and standards, offer many points of contact for the German legislator.