DSI Industrial & Policy Recommendations (IPR) Series

Recommendations for the systematization of IT security law

PD Dr. Oliver Raabe, Martin Schallbruch, Anne Steinbrück

Issue 2, 2018

SecUnity is a project funded by the Federal Ministry of Education and Research to strengthen IT security research in Germany and Europe. Its core objectives are interdisciplinary networking and the identification of IT security research topics. For this purpose, the Center for Applied Law (ZAR) of the Karlsruhe Institute of Technology and the Digital Society Institute (DSI) of ESMT Berlin jointly conducted the second secUnity workshop "Law" in February 2018. The main topics were the systematization of IT security law and the design of the intersections of IT security and data protection law, risk assessment, and the state of the art as possibly relevant research topics. Jürgen Müller (BfDI), Dr. Markus Dürig (BMI) and attorney Karsten U. Bartels (HK2 Rechtsanwälte) contributed presentations and impulses. The workshop was attended by scientists, representatives of IT security and data protection supervisory authorities, ministries, and legal practitioners from the fields of consulting and business.

1. Status and development perspectives of IT security law

Status of IT security law

The federal government understands IT security law broadly in the sense of "guaranteeing freedom and security for citizens and companies in Germany" in the digital age. IT security law in the narrower sense is understood as the requirements for the IT security of systems, services and products and those who manufacture, distribute, and use them (working definition of the workshop). Based on regulations in the Act to Strengthen the Security of Federal Information Technology of 1991 (BSIG), data security regulations in data protection law and civil liability regulations, a wide-ranging field of law has developed in recent years in the field of IT security law. Some 63 federal laws and regulations allot tasks to the Federal Office for Information Security (BSI) with regard to specific IT security requirements.

In addition to general IT security law regulations, sector-specific IT security law – for example in the area of telecommunications or banking – is becoming increasingly prevalent. In addition, primary IT security regulations aim to address the classic protection goals of system confidentiality, integrity, and availability are to be found, as are secondary regulations in which the IT security goals are tools for certain technical objectives, such as the protection of personal data, tax secrecy, and the integrity of electronic transactions.

Relationship to data protection law

There are close points of reference and intersections between IT security law and data protection law (see DSI IPR 2/2017) as well as partly diverging interests. A central commonality is protection against the risks of information technology uses. However, the risk concept in data protection law, which primarily focuses on the risks for those affected, differs from the risk concept in IT security law, which must also take into account the risks for society.

Strong common interests exist in the coherent design of technical protection measures and a comprehensible "state of the art" in data and IT security measures, some of which relate to the same systems with similar objectives.

Development perspectives of IT security law

A further development of European IT security law is currently taking place with the ongoing consultation of the Commission proposals on "Cyber Security Regulation." Further proposals have been announced.

According to the Federal Ministry of the Interior (BMI), there are currently various reasons why it is necessary to further develop IT security law. On the one hand, the involvement of other sectors of the economy in IT security law is required. The scope of involvement of the public administration must also be reviewed. Secondly, especially with regard to internet-of-things devices, the introduction of binding standards and norms for software and devices must be examined. Thirdly, the increase in the penalties for cyber crimes is under discussion. Fourthly, the creation of a legal framework for state network operations to avert serious cyber attacks is also on the political agenda.

Political projects from the coalition agreement

The new federal government's coalition agreement of February 2018 addresses IT security law in a variety of ways. The further development of the IT Security Act for an IT Security Act 2.0 is envisaged. Manufacturers and providers of technology should also be more committed to the obligation - even outside of critical infrastructures - to tighten product liability and product safety regulations and to develop security standards for Internet-enabled products. The tasks of the BSI are to be concretized and expanded, the role of the BSI strengthened, and the cooperation between federal and state governments in cyber defense structurally reorganized. The legal capacity of the security authorities to prevent and combat cyber crime is also to be strengthened.

It is to be expected that in the 19th parliamentary term of the German Bundestag there will be extensive legislative projects relating to IT security, both in the sectoral and in the overarching IT security law.

2. Questions on the systematization of IT security law

System classification and statutory framework convergence

Classification of systems

IT security regulations of different legal sources use different terms for the information technology systems concerned. An inconsistent system of classification of systems has emerged, on the one hand due to the convergence of technologies, and on the other hand due to the coexistence of European and national legislation. Facilities providing critical services as defined by the BSIG, digital services under the TMG (“telemedia services”), digital services under the NIS Directive, telecommunications services, broadcasting services, and trust services have significant interfaces and overlaps. The virtualization of systems also dissolves the conventional separation of "systems" and "services." The legal delimitation difficulties will become even more pronounced with the hybrid protection regime of telecommunications secrecy and data protection in the upcoming ePrivacy Regulation. In addition, there is the special issue of information technology systems that are used for the processing of personal data, arising at the intersections of data protection law and IT security law.

The general IT security law does not offer any assistance for the classification of information technology systems, for system responsibility (operator vs. User in cases of virtualization), for the nesting of systems, nor for the interaction of systems.

Statutory framework

With the extensions and amendments of 2009, 2015, and 2017, the BSIG now forms a kind of normative core

of a general IT security law. These are IT security regulations that define IT security requirements that are separate from the individual application areas of IT systems. The BSIG not only describes the duties and powers of the authority, but also safety requirements and other legal obligations for operators and providers in various areas. Another rather general IT security law regulation can be found in § 13 Paragraph 7 TMG. At the European level, general regulations on IT security are more likely to be found in data protection law (Art. 32 GDPR) and the eIDAS Regulation. The forthcoming adoption of the Cybersecurity Act will add further general regulations.

In addition to the general IT security law – both at European and federal levels and increasingly at the state level – there are sector-specific IT security law regulations relating to specific fields of application. Examples are § 291b SGB V, § 22 MsbG, and § 2 FahrPersV. The corresponding provisions in the sector-specific law typically specify requirements for the IT security of specialist applications and introduce a system for establishing conformity in advance (through certification, etc.) or subsequently (through supervisory authorities, provisions for fines, etc.).

The definitions of protective purpose, protection requirements, conformity assessment, etc. used differ considerably from sector to sector. The integration of the BSI, which is usually planned, is also worked out very differently.

Protection goals, risk definition, and risk assessment

The concept of risk is of paramount importance for determining protection needs and appropriate safeguards, both in IT security and in data protection law. The concept of risk differs fundamentally from the system introduced for state risk provision obligations, which marks a relevant statutory intervention threshold. Rather, the risk of an infringement of legally protected goods is to be set here as an assessment criterion within the framework of cost-benefit considerations. Therefore a reference to the law of hazard prevention must be precluded in the determination of a suitable method for risk assessment. To this extent, measures must typically be selected in line with the risk, so that the risk can always be determined relative to the protection objective of the respective legal regulation.

Protection goals in IT security and data protection

IT security regularly aligns with the functional protection goals of availability, integrity, confidentiality, and authenticity of information technology systems. Data protection, on the other hand, is oriented towards the individual protection of basic rights of individuals and will be extended even more vaguely beyond the right to informational self-determination by referring to "rights and freedoms of natural persons" in the GDPR. This very different perspective of the protection goals alone characterizes the risk analysis and risk assessment derived from it.

But this also eliminates a simple adoption of best practices, such as the BSI's basic protection for determining the severity and probability of occurrence of risks for the data protection problem. Risks arising from security breaches in information technology systems cannot be determined uniformly. However, an independent data protection methodology for risk assessment is also lacking for the time being, especially as regards the establishment of guidelines, recommendations and best practices according to type. 70 para. 1 lit h) of the GDPR by the European Data Protection Committee cannot be expected in a timely manner.

Risk management

Finally, for the provider or operator of information technology services or systems subject to standards, an assessment of the risks is necessary in order to be able to select the technical-organizational measures appropriate to the risk within the context of the assessment of risk-management measures. Basically, risk assessments can be made quantitatively, semi-quantitatively, or qualitatively. Since a purely descriptive qualitative risk assessment already lacks a result which can form a uniform basis of assessment in the balance with the investment costs, this methodology is ruled out. In the methodologies that can be mapped on the basis of metrics, the problem arises that the evaluation is always aimed at future infringements of legally protected goods. In the context of data protection law, this regularly encounters implementation difficulties, since at the time of the assessment there is hardly any empirical evidence on the likelihood of occurrence and serious consequences of violations. Possible risk assessment procedures on the basis of frequentist probabilities therefore still require a variety of methodological clarifications.

The existing tools developed from a practical point of view, such as the semi-quantitative methods of basic IT protection or the standard data protection model (SDM) derived from this, can basically provide indications for risk management. But in addition to the different protection goals, the question arises, whether

the rough granular estimation envisaged there can sufficiently take into account the intensities of interference in the right to informational self-determination.

Especially with regard to the basic methodological advantages of quantitative risk assessments on a cost basis, it is surprising that the implementation of the requirements of the IT security and data protection law so far lacks a methodically and legally sound technical tool support. An appropriate self-learning and possibly certified system would first have to reflect the methodological and legal bases to be researched for risk management in data protection and IT security. At the same time, a technical system, in contrast to the existing paper-based procedures, can serve as a storehouse for the historical occurrence of specific infringements of legally protected goods and form the currently still lacking empirical basis for evaluations. This would be particularly useful in light of the duty to imply risk-based decision-making program based on Art. 25 (1) GDPR for almost all ICT providers , which may lead to a significant reduction in the burden on the implementation of "Privacy by Design" and enable legally compliant operation.

State of the art

The technical reference point for the legal requirements of IT security law for protective measures is the "state of the art" in almost all IT security law regulations. The obligation of a provider or operator to "consider" or "comply" with a legally indeterminable state of the art refers out of the law to the technical sphere. There must be an objectifiable determination of the state of the art.

Content and determination of state of the art

The term "state of the art," which is commonly used in Germany, is based on a graduated system of increasing demands on the technology. The "state of the art" is above the "recognized rules of technology" and below the "state of the art in science and technology." EU law also uses the state of the art as a point of reference in IT security, without a comparable stage model being available under common law.

Even if the legislator does not further determine the state of the art legally, the respective individual regulation in IT security law or its systematic position provides further indications, such as the enabling of industry-specific minimum standards in the IT security law. Although it has no binding effect but is important for legal practice, there are also official recommendations on the state of the art or elaborations by industry associations which, in view of their broad agreement, suggest a presumption of an appropriate description. Developments on the state of the art exist both subject-related and interdisciplinary, partly with overlapping contents.

A uniform and generally accepted method for determining the state of the art, especially with regard to the dynamic character of this requirement, does not exist.

"State of the art" consideration

While the state of the art is a technically objectifiable requirement, the "consideration" of the state of the art required by law (e.g., by the provider of digital services in § 8c Para. 2 of the BSIG) has a subjective component. The provider must actively deal with the objective state of the art in the area of the relevant protective measures, determine the relevant measures, evaluate their technical relevance for the implementation of the legal requirements in the respective area, and finally make a reasoned decision as to which measures correspond to the statutory mandate in the specific case.

The decision on the consideration of the state of the art is a personal obligation of the provider, which exists dynamically, with the further development of the respective technical application, the change of the risk profile, as well as the further development of the objective state of the art of protective measures to examine and adapt, if necessary.

Benchmark

The rapid development of IT security law has led to inconsistencies and contradictions in these areas. Due to the lack of systematization of IT security law and the lack of consistency with the future European legal framework on data protection, the number of inconsistencies and contradictions will increase with each new legislation at European and national levels. For the operators of information technology systems and providers of digital services subject to the law, reliable and

verifiable compliance with IT security regulations is becoming increasingly difficult. In addition, both the system landscape and business models are subject to strong dynamics, as are the two main reference points of IT security law: the methods of risk assessment and the state of the art.

The lack of systematization also has disadvantages for the state and the economy as a whole. Information technology users have significant bureaucratic burdens when it comes to identifying, implementing, and verifying IT security requirements for their IT systems using a variety of methods.

Politicians, on the other hand, find it difficult to understand what level of security exists at what point in the use of digital technology.

The providers of IT security technology are therefore not able to establish scalable standard technologies and measures on the market that implement recognized IT security requirements and, at the same time, adequately resolve unavoidable conflicts regarding data protection measures required by data protection law. There is also the risk of further fragmentation of IT security technologies if sector-specific national security technology is promoted or demanded by law (e.g., SmartMeter, beA, connector in the healthcare system) and, as a result, these sector-specific requirements could also be considered from a European perspective as non-tariff barriers to trade.

3. Recommendations

Research needs

IT security legislation will continue to develop rapidly over the next few years. It is clear that a systematization of the legal area is required. To this end, research projects should be initiated as quickly as possible that create the basis for systematization, help legal users to penetrate the subject matter and, above all, develop a model for an amendment of IT security law for the purpose of systematizing the disordered legal area.

The central task of research must be the systematic development of general IT security law, the determination of its relationship to sector-specific regulations, and the harmonized solution of conflicts with European technical data protection law.

System classification and statutory framework

In order to overcome the various overlapping and contradictory references to information technology systems in IT security law, it is necessary to develop a model of the classification of information technology systems that is largely independent of the subject and market. All types of systems and digital services should be considered, irrespective of the current legal context.

A technical-practical feasibility must be kept in mind as well as a legal assignment of responsibility to actors such as operators, providers, and users. The model must take into account the nesting of IT systems (and responsibility) as well as the interaction of systems.

The model of information technology systems in IT security law should be anchored in a general part of IT security law in such a way that sector and application-specific IT security regulations can refer to it. Such a general part could also incorporate principles of accountability (e.g., due diligence) and general conformity assessment procedures. Which subjects should be included in a general part would be the subject of a research project.

Risk assessment appropriate to the legally protected goods

The aim of research in the field of risk assessment must be to develop a method that is equally suitable in terms of data protection law and IT security law for the presentation and measurement of risks due to security breaches of information technology systems. In the field of tension of practicability and certainty for the legal users up to the protective granularity of the methods, there must be a common foundation, which necessarily makes different assessments possible with regard to the different IT security and data protection rights. Following from the professional and market-independent classification of information technology systems, the option of typical data protection classes of damage ("rights and freedoms of natural persons") should be investigated at the same time. These dynamic classifications and basic protection measures could form the basis for the actual cost-based risk assessment/ choice of measures within the framework of "Privacy by Design,"

as well as data security and data protection impact assessments, and lead to a layered reduction in complexity within the framework of the existing testing and procedural system of the GDPR.

The method(s) to be developed should be accompanied by prototype tool support and ideally tested in various areas of application.

A generalizable method of risk recording and evaluation could be anchored as an instrument in the general part of the IT security law in order to allow the sector-specific IT security law a coherent reference to the necessary risk assessment.

State of the art

The various approaches and methods for determining the state of the art must be supported scientifically. The main focus must be on how to ensure the objectivity and dynamism of technical findings and what effects this will have on the market for IT security services.

The central research question is whether a meta-method of determining the state of the art would be possible. It could become part of a general part of IT security law. Furthermore, there is a need for research with regard to the requirements for the subjective performance of the drafted standards to adequately consider the state of the art.

Recommendations to business and politics

Political recommendations

German and European legislation will not achieve a systematization of IT security law in the short and medium term. However, they should already address the goal of systematization and the proposal of a strict separation of general and domain-specific IT security law. In Germany, general regulations should only be included in a BSIG renamed "General IT Security Act" (AITSG). These could include, for example, the IT security regulations of the Telemedia Act (TMG).

Parallel to a research project to develop a general IT security law, the various actors involved in sector-specific IT security regulation should be familiarized with the basic ideas and concepts of separating general and sector-specific law, for example in the form of organizing a regular "IT security law dialog," with which the coherence of regulations can already be improved in the transitional period.

Recommendations to industry

In view of the inconsistencies and contradictions in IT security and data protection law, companies are recommended to precisely document the impact of legal requirements on their own systems, the procedure for risk assessment, and the method for determining the application-specific state of the art. Existing official recommendations and industry standards must be comprehensibly included in the audit.

It is recommended that associations of the user industry, in particular also cross-industry associations such as BDI and VOICE, develop their own competence for systematizing IT security law so that problems and practical requirements can be incorporated into research work and legislation.

The DSI Industrial & Policy Recommendations (IPR) Series is published by the Digital Society Institute of ESMT Berlin, http://dsi.esmt.org.

DSI Industrial & Policy Recommendations (IPR) Series

Empfehlungen zur Systematisierung des IT-Sicherheitsrechts

PD Dr. Oliver Raabe, Martin Schallbruch, Anne Steinbrück

Ausgabe 2, 2018

SecUnity ist ein vom Bundesministerium für Bildung und Forschung gefördertes Projekt zur Stärkung der IT-Sicherheitsforschung in Deutschland und Europa, dessen Kernziele die interdisziplinäre Vernetzung und die Identifizierung von IT-Sicherheits-Forschungsthemen sind. Hierzu wurde gemeinsam vom Zentrum für Angewandte Rechtswissenschaft (ZAR) des KIT Karlsruhe und vom Digital Society Institute (DSI) der ESMT Berlin im Februar 2018 der zweite secUnity-Workshop „Recht“ durchgeführt. Als inhaltliche Schwerpunkte waren die Systematisierung des IT-Sicherheitsrechts und die Ausgestaltung der Schnittbereiche von IT-Sicherheits- und Datenschutzrecht, die Risikoeinschätzung und der Stand der Technik als möglicherweise relevante Forschungsthemen ausgewählt worden. Vorträge und Impulse steuerten MinDirig Jürgen Müller (BfDI), MinR Dr. Markus Dürig (BMI) und RA Karsten U. Bartels (HK2 Rechtsanwälte) bei. Insgesamt haben an dem Workshop Wissenschaftlerin-nen und Wissenschaftler, Vertreterinnen und Vertreter von IT-Sicherheits- und Datenschutzaufsichten, Ministerien sowie Rechtsanwender aus Beratung und Wirtschaft teilgenommen.

1. Stand und Entwicklungsperspektiven des IT-Sicherheitsrechts

Stand des IT-Sicherheitsrechts

Die Bundesregierung versteht das IT-Sicherheitsrecht weit im Sinne der „Gewährleistung von Freiheit und Sicherheit für Bürgerinnen und Bürger sowie Unternehmen in Deutschland“ im Digitalzeitalter. IT-Sicherheitsrecht im engeren Sinne wird hingegen verstanden als die Anforderungen an die IT-Sicherheit von Systemen, Diensten und Produkten und diejenigen, die sie herstellen, vertreiben und benutzen (Arbeitsdefinition des Workshops). Ausgehend von Regelungen im BSI-Gesetz von 1991, Datensicherheitsvorschriften im Datenschutzrecht und zivilrechtlichen Haftungsregelungen hat sich in den letzten Jahren ein weit verzweigtes Rechtsgebiet des IT-Sicherheitsrechts entwickelt. Allein 63 Gesetze und Verordnungen des Bundes enthalten eine Aufgabenzuweisung an das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Hinblick auf spezifische IT-Sicherheitsanforderungen.

Neben den “allgemeinen” IT-sicherheitsrechtlichen Regelungen tritt zunehmend ein “bereichsspezifisches IT-Sicherheitsrecht”, etwa im Bereich Telekommunikation oder Banken, auf. Zudem sind „primäre” IT-Sicherheits-Regelungen, deren Ziele die klassischen Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit der Systeme adressieren, ebenso zu finden wie „sekundäre” Regelungen, bei denen die IT-Sicherheits-Ziele Hilfsmittel für bestimmte fachliche Ziele sind, etwa den Schutz persönlicher Daten, das Steuergeheimnis oder die Unverfälschbarkeit elektronischer Transaktionen.

Verhältnis zum Datenschutzrecht

Zwischen dem IT-Sicherheitsrecht und dem Datenschutzrecht gibt es enge Bezugspunkte und Schnittmengen (vgl. DSI IPR 2/2017) und teilweise divergierende Interessenlagen. Zentrale Gemeinsamkeit ist der Schutz gegen die Risiken informationstechnischer Nutzungen. Allerdings unterscheidet sich der Risikobegriff des Da-

tenschutzrechts, der primär auf die Risiken für die Betroffenen abhebt, von dem Risikobegriff des IT-Sicherheitsrechts, der auch die Risiken für die Gesellschaft in den Blick nehmen muss.

Starke gemeinsame Interessen bestehen bei der kohärenten Ausgestaltung technischer Schutzmaßnahmen und eines nachvollziehbaren „Stands der Technik" bei den Daten- bzw. IT-Sicherheitsmaßnahmen, die teilweise mit ähnlicher Zielrichtung die gleichen Systeme betreffen.

Entwicklungsperspektiven des IT-Sicherheitsrechts

Eine Weiterentwicklung des europäischen IT-Sicherheitsrechts erfolgt derzeit mit der laufenden Beratung der Kommissionsvorschläge „Cyber Security Regulation". Weitere Vorschläge sind angekündigt.

Nach Einschätzung des BMI ergibt sich derzeit aus verschiedenen Gründen die Notwendigkeit zur fachlichen Weiterentwicklung des IT-Sicherheitsrechts. Zum einen sei die Einbeziehung weiterer Bereiche der Wirtschaft in das IT-Sicherheitsrecht erforderlich. Auch die Reichweite der Einbeziehung der öffentlichen Verwaltung müsse überprüft werden. Zum zweiten müsse – gerade im Hinblick auf Internet-of-things-Devices – eine Einführung von verbindlichen Standards und Normen für Programme und Geräte geprüft werden. Zum dritten sei die Erhöhung der Strafrahmen für Cyberstraftaten in der Diskussion. Schließlich sei, viertens, auch die Schaffung rechtlicher Rahmenbedingungen für staatliche Netzwerkoperationen zur Abwehr schwerwiegender Cyberangriffe auf der politischen Agenda.

Politische Vorhaben aus dem Koalitionsvertrag

Der Koalitionsvertrag der neuen Bundesregierung vom Februar 2018 adressiert das IT-Sicherheitsrecht in vielfältiger Weise. Vorgesehen ist die Weiterentwicklung des IT-Sicherheitsgesetzes zu einem IT-Sicherheitsgesetz 2.0. Hersteller und Anbieter von Technologie sollen – auch außerhalb kritischer Infrastrukturen – stärker in die Pflicht genommen werden, Regelungen der Produkthaftung und Produktsicherheit verschärft werden, Sicherheitsstandards für internetfähige Produkte entwickelt werden. Die Aufgaben des BSI sollen konkretisiert und erweitert, die Rolle des BSI gestärkt, die Bund-Länder-Zusammenarbeit bei der Cyberabwehr strukturell neu geordnet werden. Die Fähigkeiten der Sicherheitsbehörden zur Prävention und Bekämpfung von Cyberkriminalität sollen auch rechtlich gestärkt werden.

Es ist zu erwarten, dass es in der 19. Wahlperiode des Deutschen Bundestages zu umfangreichen gesetzgeberischen Vorhaben mit Bezug zur IT-Sicherheit kommt, sowohl im sektoralen als auch im übergreifenden IT-Sicherheitsrecht.

2. Fragestellungen zur Systematisierung des IT-Sicherheitsrechts

Klassifikation von Systemen und Konvergenz der gesetzlichen Systematik

Klassifikation von Systemen

IT-sicherheitsrechtliche Regelungen verschiedener Rechtsquellen verwenden unterschiedliche Begriffe für die betroffenen informationstechnischen Systeme. Einerseits durch die Konvergenz von Technologien, andererseits durch ein Nebeneinander europäischer und nationaler Gesetzgebung hat sich ein inkonsistentes System der Klassifikation von Systemen ergeben. Anlagen zur Erbringungen kritischer Dienstleistungen im Sinne des BSIG, Telemediendienste nach dem TMG, digitale Dienste nach der NIS-Richtlinie, Telekommunikationsdienste, Rundfunkdienste und Vertrauensdienste weisen erhebliche Schnittstellen und Überschneidungen auf. Mit der Virtualisierung von Systemen löst sich zudem die herkömmliche Trennung von „Systemen" und „Diensten" auf. Die rechtlichen Abgrenzungsschwierigkeiten werden sich mit dem hybriden Schutzregime aus einfachrechtlichem Fernmeldegeheimnis und Datenschutz in der kommenden ePrivacy-Verordnung noch

vertiefen. Hinzu kommt die Besonderheit informationstechnischer Systeme, die für die Verarbeitung personenbezogener Daten verwendet werden, bei denen sich quer zu den IT-sicherheitsrechtlichen Definitionen aus dem Datenschutzrecht weitere Anforderungen ergeben.

Das allgemeine IT-Sicherheitsrecht bietet keine Hilfestellung zur Klassifikation von informationstechnischen Systemen, zur Systemverantwortung (Betreiber vs. Nutzer in Fällen der Virtualisierung), zur Schachtelung von Systemen und zur Interaktion von Systemen.

Gesetzliche Systematik

Mit den Erweiterungen und Änderungen von 2009, 2015 und 2017 bildet das BSI-Gesetz mittlerweile eine Art normativen Kern eines allgemeinen IT-Sicherheitsrechts. Darunter werden IT-sicherheitsrechtliche Regelungen verstanden, die von einzelnen Anwendungsbereichen informationstechnischer Systeme losgelöste Anforderungen an die IT-Sicherheit definieren. Das BSIG beschreibt nicht nur Aufgaben und Befugnisse der Behörde, sondern auch Sicherheitsanforderungen und sonstige Rechtspflichten für Betreiber und Anbieter in verschiedenen Bereichen. Eine ebenfalls eher allgemeine IT-sicherheitsrechtliche Regelung findet sich in § 13 Abs. 7 TMG. Auf europäischer Ebene sind eher allgemeine Regelungen zur IT-Sicherheit im Datenschutzrecht (Art. 32 DSGVO) und der eIDAS-Verordnung zu finden. Mit der bevorstehenden Verabschiedung des Cybersecurity Act kommen weitere allgemeine Regelungen hinzu.

Neben dem allgemeinen IT-Sicherheitsrecht bestehen sowohl auf europäischer wie auch auf Bundesebene, zunehmend auch auf Landesebene, bereichsspezifische, auf konkrete Anwendungsfelder bezogene IT-sicherheitsrechtliche Regelungen. Beispiele sind § 291b SGB V, § 22 MsbG oder § 2 FahrPersV. Die entsprechenden Regelungen im Fachrecht legen typischerweise Anforderungen an die IT-Sicherheit fachspezifischer Anwendungen fest und führen ein System der Feststellung von Konformität ein, vorab (durch Zertifizierung o.ä.) oder nachträglich (durch Kontrollbefugnisse, Bußgeldvorschriften o.ä.).

Die dabei verwendeten Definitionen von Schutzbedarf, Schutzanforderungen, Konformitätsfeststellung etc. unterscheiden sich von Fachgesetz zu Fachgesetz erheblich. Auch die in der Regel vorgesehene Einbindung des BSI erfolgt sehr unterschiedlich.

Schutzziele, Risikodefinition und Risikobewertung

Der Begriff des Risikos ist von überragender Bedeutung für die Bestimmung des Schutzbedarfes und der angemessenen Schutzmaßnahmen, sowohl im IT-Sicherheits- wie auch im Datenschutzrecht. Dabei unterscheidet sich der Risikobegriff grundlegend von der eingeführten Systematik bei staatlichen Risikovorsorgepflichten, welche eine relevante gesetzliche Eingriffsschwelle markiert. Vielmehr ist hier das Risiko einer Schutzgutverletzung als Bewertungsmaßstab im Rahmen von Kosten-Nutzen-Erwägungen einzustellen. Daher ist eine Rückbeziehung auf die Maßstäbe im Gefahrenabwehrrecht nunmehr ausgeschlossen. Maßnahmen müssen insofern typischerweise risikoangemessen ausgewählt werden, so dass sich das Risiko immer relativ zum Schutzziel der jeweiligen rechtlichen Vorschrift bestimmen lässt.

Schutzziele in der IT-Sicherheit und im Datenschutz

Die IT-Sicherheit richtet sich regelmäßig an den funktionalen Schutzzielen Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität informationstechnischer Systeme aus. Hingegen orientiert sich der Datenschutz an dem individuellen Grundrechtsschutz einzelner und wird mit dem Verweis der Datenschutzgrundverordnung auf „Rechte und Freiheiten natürlicher Personen“ zukünftig über das Recht auf informationelle Selbstbestimmung hinaus noch unbestimmter erweitert. Allein schon dieser unterschiedliche Blickwinkel der Schutzziele prägt die davon abgeleitete Risikoanalyse und Risikobewertung.

Damit scheidet aber auch eine einfache Übernahme von bewährten Verfahren, wie dem BSI-Grundschutz zur Bestimmung von Schwere und Eintrittswahrscheinlichkeit von Risiken für den datenschutzrechtlichen Problemkreis aus. Risiken, die sich aus Sicherheitsverletzungen informationstechnischer Systeme ergeben, können damit nicht einheitlich bestimmt werden. Aber auch eine eigenständige datenschutzrechtliche Methodik zur Risikobeurteilung fehlt einstweilen, zumal die Aufstellung von Leitlinien, Empfehlungen und bewährten Verfahren nach Art. 70 Abs. 1 lit h) DS-GVO durch den europäischen Datenschutzausschuss naturgemäß nicht zeitnah zu erwarten sein kann.

Risikobewältigung

Für den normunterworfenen Anbieter bzw. Betreiber informationstechnischer Dienste bzw. Systeme ist schließlich eine Bewertung der Risiken erforderlich, um im Rahmen der Beurteilung von Maßnahmen zur Risikobewältigung die risikoangemessenen, technisch-organisatorischen Maßnahmen auswählen zu können. Grundsätzlich können Risikobewertungen quantitativ, semi-

quantitativ oder qualitativ vorgenommen werden. Da es bei einer rein beschreibenden qualitativen Risikobewertung schon an einem Ergebnis mangelt, welches eine einheitliche Bewertungsbasis in der Abwägung mit den Investitionskosten bilden kann, scheidet diese Methodik hier aus. Bei den auf Basis von Metriken abbildbaren Methodiken ergibt sich das Problem, dass die Bewertung immer auf zukünftige Schutzgutverletzungen gerichtet ist. Dies stößt im datenschutzrechtlichen Kontext regelmäßig auf Umsetzungsschwierigkeiten, da zum Beurteilungszeitpunkt kaum Empirie zur Eintrittswahrscheinlichkeit und Folgenschwere von Verletzungen vorliegen kann. Möglichen Risikobewertungsverfahren auf Basis von frequentistischen Wahrscheinlichkeiten steht insofern noch vielfältiger methodischer Klärungsbedarf entgegen.

Die vorhandenen, insbesondere aus dem Blickwinkel der Praktikabilität entwickelten Hilfsmittel, wie die semi-quantitativen Methoden des IT-Grundschutzes oder des hieraus für den Datenschutz abgeleiteten Standard-Datenschutzmodells (SDM), können grundsätzlich Anhaltspunkte zur Risikobewältigung leisten. Aber neben den unterschiedlichen Schutzzielen stellt sich die Frage, ob die dort vorgesehene grobgranulare Schätzung, den Eingriffsintensitäten in das Recht auf informationelle Selbstbestimmung hinreichend Rechnung tragen kann.

Gerade im Hinblick auf die grundsätzlichen methodischen Vorteile quantitativer Risikobewertungen auf Kostenbasis ist überraschend, dass es für die Umsetzung der Vorgaben des IT-Sicherheits- und Datenschutzrechts bislang an einer methodisch und rechtlich fundierten technischen Werkzeugunterstützung mangelt. Ein entsprechendes selbstlernendes und ggf. zertifiziertes System müsste zunächst die zu erforschenden methodischen und rechtlichen Grundlagen zum Risikomanagement im Datenschutz und in der IT-Sicherheit reflektieren. Gleichzeitig kann ein technisches System, im Gegensatz zu den bestehenden in Papier formalisierten Verfahren, als Speicher für das historische Vorkommen von spezifischen Schutzgutverletzungen dienen und selbstlernend die derzeitig noch fehlende empirische Basis für Bewertungen bilden. Dies würde gerade im Hinblick auf die Umsetzung eines für fast alle IKT-Anbieter obligatorischen, risikobasierten Entscheidungsprogramms nach Art. 25 Abs.1 DS-GVO zukünftig zur Realisierung von „Privacy by Design“ eine deutliche Entlastung und die Ermöglichung eines rechtssicheren Betriebes zur Folge haben können.

Stand der Technik

Technischer Bezugspunkt der rechtlichen Anforderungen des IT-Sicherheitsrechts an die Schutzmaßnahmen ist in nahezu allen IT-sicherheitsrechtlichen Regelungen der „Stand der Technik“. Die Verpflichtung eines Anbieters oder Betreibers zur „Berücksichtigung“ oder „Einhaltung“ eines rechtlich nicht weiter bestimmbaren Standes der Technik verweist aus dem Recht hinaus in die technische Sphäre. Dort muss eine objektivierbare Bestimmung des Standes der Technik erfolgen.

Inhalt und Bestimmung des Standes der Technik

Die in Deutschland gebräuchliche Begrifflichkeit des Standes der Technik orientiert sich an einem abgestuften System steigender Anforderungen an die Technologie. Der „Stand der Technik“ liegt dabei vom Niveau her oberhalb der „anerkannten Regeln der Technik“ und unterhalb des „Standes von Wissenschaft und Technik“. Auch das EU-Recht verwendet in der IT-Sicherheit den Stand der Technik als Bezugspunkt, ohne dass gemeinschaftsrechtlich ein vergleichbares Stufenmodell existiert.

Auch wenn der Gesetzgeber den Stand der Technik rechtlich nicht weiter bestimmt, so gibt doch die jeweilige Einzelregelung im IT-Sicherheitsrecht oder ihre systematische Stellung weitergehende Anhaltspunkte, etwa die Ermöglichung branchenspezifischer Mindeststandards im IT-Sicherheitsgesetz. Zwar ohne Bindungswirkung, jedoch mit Bedeutung für die Rechtspraxis existieren zudem behördliche Empfehlungen zum Stand der Technik oder Ausarbeitungen von Branchenverbänden, die im Hinblick auf ihre breite Abstimmung die Vermutung einer zutreffenden Beschreibung nahelegen. Ausarbeitungen zum Stand der Technik existieren sowohl fachbezogen als auch fachübergreifend, teilweise mit überschneidenden Inhalten.

Eine einheitliche und allgemein akzeptierte Methode zur Bestimmung des Standes der Technik, insbesondere auch im Hinblick auf den dynamischen Charakter dieser Anforderung existiert nicht.

Berücksichtigung des Standes der Technik

Während der Stand der Technik eine technisch objektivierbare Anforderung ist, hat die vom Gesetzgeber verlangte „Berücksichtigung“ des Standes der Technik

(z.B. vom Anbieter digitaler Dienste in § 8c Abs. 2 BSIG) eine subjektive Komponente. Der Anbieter muss sich mit dem objektiven Stand der Technik im Bereich der jeweils relevanten Schutzmaßnahmen aktiv auseinandersetzen, die relevanten Maßnahmen ermitteln, ihre fachliche Relevanz für die Umsetzung der gesetzlichen Anforderungen im jeweiligen Bereich bewerten und schließlich eine begründete Entscheidung treffen, welche Maßnahmen dem gesetzlichen Auftrag im konkreten Fall entsprechen.

Die Entscheidung über die Berücksichtigung des Standes der Technik ist eine persönliche Verpflichtung des Anbieters, die dynamisch besteht, mit der Weiterentwicklung der jeweiligen fachlichen Anwendung, der Veränderung des Risikoprofils sowie der Fortentwicklung des objektiven Standes der Technik von Schutzmaßnahmen zu überprüfen und ggf. anzupassen ist.

Bewertung

Die schnelle Weiterentwicklung des IT-Sicherheitsrechts hat auf den genannten Gebieten zu Inkonsistenzen und Widersprüchen geführt. Aufgrund der fehlenden Systematisierung des IT-Sicherheitsrechts und der fehlenden Konsistenz mit dem zukünftigen europäischen Rechtsrahmen zum Datenschutz wird mit jeder neuen Gesetzgebung auf europäischer und nationaler Ebene die Zahl der Inkonsistenzen und Widersprüche zunehmen. Für die rechtsunterworfenen Betreiber informationstechnischer Systeme und Anbieter digitaler Dienste wird die belastbare und nachweisbare Einhaltung der IT-sicherheitsrechtlichen Vorgaben immer schwieriger. Hinzu kommt, dass sowohl Systemlandschaft und Geschäftsmodelle einer starken Dynamik unterworfen sind als auch die beiden wesentlichen Bezugspunkte des IT-Sicherheitsrechts, die Methoden der Risikobewertung und der Stand der Technik.

Die mangelnde Systematisierung hat überdies auch Nachteile für Staat und Wirtschaft insgesamt. Die Anwender von Informationstechnik haben erhebliche Bürokratielasten zu tragen, wenn IT-Sicherheitsanforderungen für ihre IT-Systeme mit verschiedenen Methoden ermittelt, umgesetzt und geprüft werden müssen.

Die Politik kann wiederum nur schwer nachvollziehbar darstellen, welches Sicherheitsniveau an welcher Stelle der Anwendung digitaler Technologie besteht.

Die Anbieter von IT-Sicherheitstechnik können deshalb schließlich keine skalierbaren Standard-Technologien und Maßnahmen auf dem Markt etablieren, die anerkanntermaßen IT-sicherheitsrechtliche Anforderungen umsetzen und auch gleichzeitig zwangsläufige Konfliktlagen zu datenschutzrechtlich geforderten Schutzmaßnahmen angemessen auflösen. Es besteht zudem die Gefahr einer weiteren Zersplitterung von IT-Sicherheitstechnologien, wenn bereichsspezifische nationale Sicherheitstechnik gesetzlich gefördert oder gefordert wird (z.B. SmartMeter, beA, Konnektor im Gesundheitswesen) und sich in der Folge erweisen könnte, dass sich diese bereichsspezifischen Vorgaben aus europäischer Perspektive überdies als nichttarifäre Handelshemmnisse darstellen.

3. Empfehlungen

Forschungsbedarf

Die IT-sicherheitsrechtliche Gesetzgebung wird sich in den nächsten Jahren unverändert schnell weiterentwickeln. Es zeichnet sich deutlich ab, dass eine Systematisierung des Rechtsgebiets erforderlich ist. Hierfür sollten möglichst zügig Forschungsprojekte initiiert werden, die die Grundlage einer Systematisierung schaffen, den Rechtsanwendern bei der Durchdringung der Materie helfen und vor allem dem Gesetzgeber ein Modell für eine Novellierung des IT-Sicherheitsrechts zwecks Systematisierung des ungeordneten Rechtsgebiets entwickeln.

Zentraler Auftrag an die Forschung muss die systematische Entwicklung des allgemeinen IT-Sicherheitsrechts, die Bestimmung seines Verhältnisses zu den bereichsspezifischen Regelungen und die harmonisierte Lösung von Kollisionslagen mit dem europäischen technischen Datenschutzrecht sein.

Klassifikation von Systemen und gesetzliche Systematik

Zur Überwindung der verschiedenen überschneidenden und widersprüchlichen Bezugnahmen auf informationstechnische Systeme im IT-Sicherheitsrecht, muss ein weitgehend fach- und marktunabhängiges Modell der Klassifizierung informationstechnischer Systeme entwickelt werden. Jede Art von Systemen und digitalen Diensten ist hierbei, unabhängig von der derzeitigen rechtlichen Anknüpfung, zu berücksichtigen.

Dabei muss eine technisch-praktische Umsetzbarkeit ebenso im Blick behalten werden, wie eine rechtliche Zuordenbarkeit von Verantwortung an Akteure wie Betreiber, Anbieter, Nutzer. Das Modell muss die Schachtelung von IT-Systemen (und Verantwortung) ebenso berücksichtigen, wie die Interaktion von Systemen.

Das Modell informationstechnischer Systeme im IT-Sicherheitsrecht sollte in einem allgemeinen Teil des IT-Sicherheitsrechts dergestalt verankert werden, dass bereichs- und anwendungsspezifische IT-Sicherheitsregelungen darauf Bezug nehmen können. In einem solchen allgemeinen Teil könnten auch Grundsätze der Verantwortungsverteilung (z.B. Sorgfaltspflichten) und allgemeine Verfahren der Konformitätsbewertung verankert werden. Welche Materien in einem allgemeinen Teil aufgenommen werden sollten, wäre Inhalt eines Forschungsvorhabens.

Schutzgutangemessene Risikobewertung

Ziel der Forschung im Bereich der Risikobewertung muss die Entwicklung einer datenschutzrechtlich und IT-sicherheitsrechtlich gleichermaßen tauglichen Methode zur Darstellung und Messung von Risiken durch Sicherheitsverletzungen informationstechnischer Systeme sein. Im Spannungsfeld von Praktikabilität und Bestimmtheit für die Rechtsanwender bis zur schutzgutangemessenen Granularität der Methoden, muss ein gemeinsames Fundament bestehen, welches hinsichtlich der unterschiedlichen IT-sicherheits- und datenschutzrechtlichen Schutzgüter notwendigerweise unterschiedliche Bewertung möglich macht. Anknüpfend an die fach- und marktunabhängige Klassifikation von informationstechnischen Systemen, sollte gleichzeitig die Option von typischen datenschutzrechtlichen Schadklassen („Rechte und Freiheiten natürlicher Personen“) untersucht werden. Diese dynamischen Klassifikationen und Grundschutzmaßnahmen könnten die Basis für die eigentliche kostenbasierte Risikobewertung/Maßnahmenwahl im Rahmen des „Privacy by Design“, Datensicherheit und Datenschutzfolgenabschätzungen bilden und zu einer abschichtenden Komplexitätsreduktion im Rahmen der bestehenden Prüf- und Verfahrenssystematik der DS-GVO führen.

Die zu entwickelnde Methode(n) sollte durch eine zunächst prototypische Toolunterstützung begleitet werden und im Idealfall pilothaft in verschiedenen Einsatzbereichen erprobt werden.

Eine verallgemeinerbare Methode der Risikoerfassung und -bewertung könnte als Instrument im allgemeinen Teil des IT-Sicherheitsrechts verankert werden, um dem fachspezifischen IT-Sicherheitsrecht eine kohärente Bezugnahme auf die nötige Risikoermittlung zu erlauben.

Stand der Technik

Die verschiedenen Ansätze und Methoden zur Ermittlung des Standes der Technik sind wissenschaftlich zu begleiten. Dabei ist vor allem herauszuarbeiten, wie die Objektivierbarkeit der technischen Feststellung und ihre Dynamisierung gewährleistet werden und welche Auswirkungen dies auf den Markt der IT-Sicherheitsangebote hat.

Zentrale Forschungsfrage ist es, ob eine Metamethode der Feststellung des Standes der Technik möglich wäre. Sie könnte Bestandteil eines allgemeinen Teils des IT-Sicherheitsrechts werden. Weiterhin besteht Forschungsbedarf hinsichtlich der Anforderungen an die subjektive Leistung der Normentworfenen, den Stand der Technik adäquat zu berücksichtigen.

Empfehlungen an Wirtschaft und Politik

Empfehlungen an die Politik

Die deutsche und europäische Gesetzgebung wird kurz- und mittelfristig keine Systematisierung des IT-Sicherheitsrechts erreichen. Sie sollte jedoch das Ziel einer Systematisierung und den Vorschlag einer strikten Trennung zwischen allgemeinem und bereichsspezifischem IT-Sicherheitsrecht schon jetzt aufgreifen. Allgemeine Regelungen sollten in Deutschland allein in ein in „Allgemeines IT-Sicherheitsgesetz“ (AITSG) umbenanntes BSIG aufgenommen werden. Dazu könnten beispielsweise die IT-sicherheitsrechtlichen Regelungen des TMG gehören.

Parallel zu einem Forschungsvorhaben zur Entwicklung eines allgemeinen IT-Sicherheitsrechts sollten die unterschiedlichen Akteure fachspezifischer IT-Sicherheitsregulierung mit den Grundgedanken und Grundkonzepten der Trennung allgemeinen und bereichsspezifischen Rechts vertraut gemacht werden, etwa in Form der Organisation eines regelmäßigen „Dialogs IT-Sicherheitsrecht“, mit dem die Kohärenz der Regelungen schon in der Übergangszeit verbessert werden kann.

Empfehlungen an die Wirtschaft

Angesichts der Inkonsistenzen und Widersprüche im IT-Sicherheits- und Datenschutzrecht wird den Unternehmen empfohlen, die Betroffenheit eigener Systeme von gesetzlichen Anforderungen, die Verfahrensweise zur Risikobewertung und die Methode der Bestimmung des anwendungsspezifischen Standes der Technik genau zu dokumentieren. Vorhandene behördliche Empfehlungen und Branchenstandards, sind jedenfalls nachvollziehbar in die Prüfung einzubeziehen.

Den Verbänden der Anwenderwirtschaft, insbesondere auch branchenübergreifenden Verbänden wie BDI und VOICE wird empfohlen, eigene Kompetenz zur Systematisierung des IT-Sicherheitsrechts aufzubauen, um Probleme und Anforderungen aus der Praxis in die Forschungsarbeiten und die Gesetzgebung einbringen zu können.

Die DSI Industrial & Policy Recommendations (IPR) Series wird herausgegeben vom Digital Society Institute der ESMT Berlin, http://dsi.esmt.org.