Das IT-Sicherheitsgesetz als Teil der jüngeren Entwicklung

I. Einleitung

Sicherheit steht zurzeit hoch im Kurs. Die Gesetzgebung im Sicherheitsbereich ist so dynamisch, dass nur noch die Spezialisten mitkommen. Die Polizeigesetze der Länder sind im ständigen Fluss und kaum wiederzuerkennen. Das Nachrichtendienstrecht ist in einer Weise durchnormiert, dass es kaum noch den Namen „geheim“ verdient. Die parlamentarische Kontrolle findet im Grundgesetz eine verfassungsrechtliche Grundlage (Artikel 45d GG) und das Bundesverfassungsgericht kreiert Gesetzgebungsaufträge in einem zeitlichen Takt, dass man leicht den Überblick verliert. Die Sicherheitsbehörden erhalten mehr und mehr Ressourcen. Wer als Wissenschaftler Sicherheitsrecht betreibt, erfreut sich in den letzten Jahren einer erhöhten Nachfrage, Selbst Drittmittel fließen im Sicherheitsrecht. Selbstverständlich ist diese Entwicklung nicht. Der aufklärerische Geist der Wissenschaft gepaart mit einer staatskritischen Sicht als Spätfolge der 68er-Jahre führte in den 90er-Jahren dazu, dass jeder der Sicherheit etwas Positives abgewinnen konnte, entweder Polizist oder Systemstabilisierer sein musste.

Das hat sich grundsätzlich gewandelt.

Drei Gründe sind dafür maßgebend:

- Zunächst ist von der Sache her eine ausschließlich skeptische Sicht auf die Sicherheit falsch und falsche Gedanken halten sich nicht ewig. So soll sich mittlerweile auch rumgesprochen haben, dass Männer nicht klüger sind als Frauen und die Erde keine Scheibe ist.

- Zweitens hat vor allem der islamistische Terrorismus das Bedürfnis nach Sicherheit deutlicher werden lassen;
- Drittens hat die Europäische Union die Sicherheit als Thema entdeckt und wenn Europa etwas zum Thema macht, fliegen bekanntlich „nationalrechtliche Fetzen“.

Der Begriff Sicherheit ist dabei vielschichtig und wird unterschiedlich verwendet. Er setzt sich zumindest aus drei Komponenten zusammen: (a) aus einem geschützten Rechtsgut, (b) einem bestimmten Beeinträchtigungsgrad, und (c) einer bestimmten Form von Beeinträchtigung. Je nachdem wie das Rechtsgut definiert wird, kann der Kreis des Sicherheitsrechts unterschiedlich weit verstanden werden. Der im Titel dieses Beitrags verwendete Begriff der Sicherheitsarchitektur meint das Geflecht von Behörden, Aufgaben und Befugnissen, das vom Grundgesetz sowie Bundes- und Landesrecht zur Gewährleistung der Sicherheit innerhalb der staatlichen Gemeinschaft geschaffen wird.

II. Das IT-Sicherheitsgesetz als Sicherheitsgesetz

Das IT-Sicherheitsgesetz ist ein Sicherheitsgesetz. Dies ist deswegen deutlich, weil es den Namen im Titel trägt. Der Titel des IT-Sicherheitsgesetzes ist dabei auch deshalb bemerkenswert, weil es ein Artikelgesetz ist, das sich darauf beschränkt, bestehende Gesetze zu ändern und dennoch einen eigenen Namen erhalten hat. Der Gesetzgeber wollte mit dem Namen erkennbar eine sicherheitsrechtliche Aufgabe aufnehmen und zwar die Gewährleistung bestimmter Aspekte der Sicherheit der IT-Netze und in bestimmter Weise lösen.

1. Die Ziele

Der Entwurf verfolgt vor allem drei Ziele:

- Stärkung der IT-Sicherheit des Bundes;

- Stärkung der IT-Sicherheit für alle Nutzer des Internets,
- Stärkung der IT-Sicherheit von kritischen Infrastrukturen.

2. Die Mittel

Diese Ziele verfolgt der Entwurf vor allem mit folgenden Mitteln:

- eine Inpflichtnahme der Betreiber so genannter Kritischer Infrastruktur,
- Relevante Vorfälle der Beeinträchtigung der IT Sicherheit müssen gemeldet werden.
- Anbieter öffentlich zugänglicher Telekommunikationsdienste, und -netze müssen Nutzerinnen und Nutzer benachrichtigen, wenn erkannt wird, dass von deren Datenverarbeitungssystemen Störungen ausgehen.
- Das BSI erhält eine Aufgaben-, Kompetenz- und Ressourcenerweiterung
- Das BKA. BfV und BND erhalten mehr Personal.

Gemessen an der oben genannten Definition der Sicherheit will das IT-Sicherheitsgesetz bestimmte Teile des IT-Netzes in der Regel vor intendierten Funktionsstörungen schützen.

III. IT-Sicherheitsgesetz als Teil der aktuellen Entwicklung der Sicherheitsarchitektur

1. Die Entwicklung als Reaktion auf tatsächliche Veränderungen

Die Entwicklung der Sicherheitsarchitektur besitzt durchaus Struktur. Die Entwicklung der deutschen Sicherheitsarchitektur ist im Augenblick massiv von Erfahrungen getrieben. Die Fortentwicklung vollzieht sich nicht blind, sondern Schritt bei Schritt. Der Gesetzgeber reagiert auf

äußere Einflüsse (Terroranschlägen, Skandalen, unbewältigten Situationen) und beobachtet dabei zugleich die Wirkung seiner Änderungen.

2. Die Entwicklungslinie

Die Entwicklungslinien sind dabei verhältnismäßig klar. Sie sind oft beschreiben worden. Folgende Aspekte prägen die Entwicklung des Sicherheitsrechts:

- eine starke Verrechtlichung des Informationsvorgangs;
- eine Stärkung der parlamtenarischen Kontrolle mitsamt einer Stärkung des Evaluationsgedankens;
- der Gedanke der Zentralisierung: der Bund bemüht sich seit Jahrzehnten in kleinen Schritten um den Ausbau seiner Kompetenzen im Sicherheitsbereich, parallel dazu läuft eine Unionalisierung dieses Gebietes;
- eine Präzisierung der geschützten Rechtsgüter;
- Privatisierungstendenzen;
- Befugniserweiterungen zugunsten der Behörden, insbesondere zur Terrorbekämpfung;
- Entwicklung zu einem Präventivstaat mit erheblicher Grenzverwischung der bisher getrennten Sicherheitsbereiche:.

3. Die Beurteilung des IT-Sicherheitsgesetz vor dieser Entwicklung

Misst man das IT-Sicherheitsgesetz an dieser Entwicklung, fügt es sich im Ergebnis in dieses Raster ein.

Offensichtlich ist, dass es sich um ein Beispiel zunehmender Verrechtlichung handelt.

Auch der Charakter der Sicherheitsrechtsentwicklung als kontrollierte anlassbezogen Fortentwicklung ist erfüllt. So sieht etwa Artikel 10 eine Evaluierung bis zum 17.07.2019 vor.

Ebenfalls eindeutig ist, dass durch das IT-Sicherheitsgesetz Behörden des Bundes eine stärkere Rolle erhalten im Vergleich zum Zustand vor Erlass des Gesetzes. Der Umstand, dass im Fall der Netzsicherheit, landesrechtliche Regelungen kaum sinnvoll wären, ändert an diesem Befund nichts sondern allenfalls an seiner Bewertung. Auch die europäische Annäherung wird gestärkt. Das BSiG ist bewusst im Vorgriff zu der Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL) ergangen

Interessant ist die Frage der Präzisierung des Schutzgutes. Die Netzsicherheit in der vom IT-Sicherheitsgesetz formulierten Form war bisher kein in vergleichbarer Weise geschütztes Rechtsgut. Die Neudefinition der IT-Sicherheit in den betroffenen Teilbereichen bildet eine naheliegende Folgerung auf die technische Entwicklung und realisiert die Aufgabe des Gesetzgebers, schützenswerte Gemeinschaftsgüter, die aus der Zeit heraus entwickelt werden, bei Bedarf neu aufzunehmen. Angriffe und Störungen der IT-Infrastruktur von Behörden, zentralen Unternehmen oder Teilen des Gesamtnetzes sind Gesamtgesellschaftliche relevante Störungen, die mit Störungen anderer Infrastruktureinrichtungen vergleichbar sind. Der Schutz der Infrastruktur ist seit jeher ein Bestandteil der Sicherheitsarchitektur.

Die Besonderheiten für die Sicherheit der Infrastruktur beruhen darauf, dass die allgemeinen Regeln des Sicherheitsrechts gerade beim Wirklichkeitsausschnitt „Infrastruktur“ in besonderer Form greifen. Die Einbettung in das allgemeine Sicherheitsrecht sieht man beim IT-

Sicherheitsgesetz daran, dass der Gesetzgeber davon ausgeht, dass das Ziel der Gewährleistung der IT-Sicherheit beim Bundesamt für Verfassungsschutz einen erhöhten Personalbedarf auslöst, obwohl die Kompetenzen des Bundesamt sich nicht verändert haben. Nach der Einschätzung der Gesetzgebers erfassen schon die bisherigen Aufgaben des Bundesamtes für Verfassungsschutz die Beobachtung der relevanter Beeinträchtigungen des IT-Netzes.

Das IT-Sicherheitsgesetz ist in besonderer Weise dadurch geprägt, dass der Gesetzgeber privaten Akteuren die Einhaltung von Sicherheitsaufgaben und Sicherheitsstandards auferlegt. Es handelt sich dabei nicht um die Fortschreibung der vielgepriesenen Partnerschaft von Staat und Privaten bei der Sicherheitserfüllung, sondern um das klassische Instrument der In-Dienstnahme Privater zu öffentlichen Aufgaben, hier zur Erfüllung einer Sicherheitsgewährleistung. Die privaten Unternehmen haben keine Wahl. Wollen sie die von ihnen gewählten Wirtschaftszweige weiter ausüben, müssen sie die staatlichen Vorgaben beachten. Insofern ist die Struktur ähnlich wie bisher bei der Wahrnehmung von technisch gefährlichen Anlagen.

Kooperationselemente greifen allerdings auf einer zweiten Ebene, unterhalb des Obs der Pflicht und zwar bei dem Ausmaß der Pflicht. Die genaue Ausdifferenzierung der einzuhaltenden Standards werden nicht einseitig vom Staat auferlegt, vielmehr werden hier die Betroffenen einbezogen und ihnen die Möglichkeit der Mitwirkung eingeräumt. Dies ist erstens eine in der neuen Rechtsentwicklung nicht untypische Erscheinung. So kennt etwa der europäische Datenschutz die Möglichkeit für Wirtschaftsbranchen, durch sog. Verhaltensregeln die eigenen datenschutzrechtlichen Pflichten innerhalb des Rahmens, den die Europäische Datenschutzgrundverordnung gibt, näher zu konkretisieren unter Einbeziehung der Aufsichtsbehörden oder des

Europäischen Datenschutzausschusses. Darüberhinaus ist die Kooperation von Wirtschaft und Staat bei der Ausdifferenzierung von technischen Standards und deren staatlicher Sanktionierung von der Sache her sinnvoll, nachvollziehbar und nicht unüblich.

4. Das BSI als Sicherheitsbehörde besonderer Art

Das BSI ist die Instanz, mit der der Staat seine Steuerungsfunktion im Bereich der Netzsicherheit übernimmt Die Frage ist, was für eine Art von Behörde das BSI durch diese Rolle wird. Da es um ein Sicherheitsgesetz geht, wird das BSI den Begriff als Sicherheitsbehörde wohl kaum verweigern können.

Die Gestaltung der Steuerung weicht dabei aber ein wenig ab von der sonstigen Steuerung im Sicherheitsbereich. Das Schwergewicht liegt nicht in klassischen Überwachungsbefugnissen. Das BSI soll nicht primär hoheitlichen überwachen, sondern beraten und entscheiden.

Das BSI erhält innerhalb der Sicherheitsbehörden einen singulären Charakter. Es hat etwas von einer unabhängigen Prüfstelle, ähnlich wie die Stiftung Warentest (§ 7a BSIG und § 7 Abs. 1 Nr. 1 BSIG), – andererseits auch etwas von einer unabhängigen Beratungsstelle für die Betreiber kritischer Infrastruktur (ähnlich wie die Datenschutzbeauftragten) (§ 3 Abs. 3 BSIG) und schließlich auch etwas von einer Warnstelle für die Öffentlichkeit und etwas von einer Nachrichtendienststelle, die Lagebilder erstellt und – bezogen auf die Lagebilder – Berichtspflichten bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen übernimmt.

Die Aufgaben des BSI sind bereichsspezifisch zugeschnitten, und nicht vollständig aufeinander abgestimmt – teilweise greifen sie Aufgaben und Befugnisse nur für Besonderheiten der IT-Sicherheit, z. B. im Bereich kritischer Infrastruktur, auf, teilweise für die IT-Sicherheit insgesamt und

teilweise nur für das Netz des Bundes. Die Meldepflicht und die Nachweispflicht angemessener IT-Sicherheit durch die Betreiber Kritischer Infrastruktur gelten gegenüber dem BSI, die Durchsetzung dieser Pflicht obliegt wiederum weitgehend den jeweiligen Aufsichtsbehörden; Das Erstellen des Lagebildes bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen ist zwischen BSI, BNetzA, BfV und BND zerstückelt.

Schluss

Es ist nachvollziehbar, dass der Staat, die Sicherheit bestimmter Teilbereiche von IT-Infrastrukturen zu einen staatlich regulierten Bereich erklärt und die Wirtschaftsunternehmen in erheblichem Maße in die Pflicht nimmt. Die Globalisierung, die Digitalisierung und die Vernetzung legen es nahe, dass der Staat die Sicherheit der IT-Infrastruktur mehr als bisher zu einer staatlichen Aufgabe macht und staatlich gewährleistet. Dafür ist das IT-Sicherheitsgesetz ein grundsätzlich geeigneter Schritt. Zugleich ist das Gesetz eingebettet in die allgemeine Entwicklung der deutschen Sicherheitsarchitektur. Er erweitert die Kompetenzen des Bundes, entwickelt das Sicherheitsrecht weiter, setzt auf eine halb freiwillige Kooperation mit der Wirtschaft und schreibt die sicherheitsrechtlich geschützten Rechtsgüter zeitgemäß fort und schafft für das BSi eine einzigartigen Behördenzuschnitt.