Die Evolution des Cybersecurity-Rechts: Vom Kernkraftwerk bis zur elektrischen Zahnbürste

Was im Jahr 2015 mit dem ersten IT-Sicherheitsgesetz begann, hat sich mittlerweile zu einem eigenständigen Rechtsgebiet entwickelt, das sowohl aus dem Alltag von Anwälten als auch aus dem von Behörden, Gerichten, Sachverständigen und IT-Dienstleistern nicht mehr hinwegzudenken ist und vielfältige Schnittpunkte zu weiteren juristischen und technischen Themen aufweist. Und wenn man sich um einige Jahre weiter zurückerinnert, wird man feststellen, dass die Cybersicherheit eher ein allgemeines Compliance-Thema denn eine eigenständige Rechtsmaterie war. Manch einer betrachtete die Cybersicherheit auch als Anhang des technischen Datenschutzes. Gerade in den letzten Jahren mussten wir jedoch feststellen, dass Cybersicherheit weit mehr als nur abstrakte technisch-organisatorische Maßnahmen darstellt und in unserer allgegenwärtig vernetzten Gesellschaft nicht nur für das Funktionieren lebenswichtiger Prozesse essenziell ist, sondern vielmehr unsere gesamte Wirtschaftsordnung mit ihren digitalen Geschäftsmodellen auf dieser aufbaut. Umso verständlicher ist es deshalb auch, dass nach der anfänglichen Regulierung von Kritischen Infrastrukturen mittlerweile sogar die vernetzte elektrische Zahnbürste als IoT-Device mit strengen gesetzlichen Vorgaben zur Cybersicherheit belegt wird.

Doch allein mit der Regulierung und der Schaffung immer strengerer gesetzlicher Vorgaben ist es nicht getan, denn sowohl in den adressierten Unternehmen als auch bei den beaufsichtigenden Behörden müssen angemessene Implementierungs- und Kontrollstrukturen vorhanden sein. Doch genau damit tut man sich gegenwärtig noch schwer, denn IT-Fachkräfte am Markt sind rar. Ein weiteres Problem betrifft die nationale und europäische Cybersicherheitsarchitektur, der innerhalb der nächsten Jahre vermutlich bahnbrechende Veränderungen bevorstehen, um der neuen Regelungssystematik gerecht zu werden. Last but not least stellt sich immer wieder die Frage, wie entsprechende Rechtsvorschriften auszulegen sind, denn insbesondere das Cybersicherheitsrecht wimmelt nur so von unbestimmten Rechtsbegriffen und Generalklauseln, sodass bestenfalls juristischer und technischer Sachverstand in einer Person vereinigt sind. Genau damit aber tun sich altbewährte und standardisierte juristische Ausbildungsmodelle immer schwerer.

Es bleibt also bei der Erkenntnis, dass Cybersicherheit zwar immer wichtiger wird und dies von Politik und Gesetzgebung auch erkannt wurde, wir gegenwärtig aber noch mit zahlreichen Umsetzungsdefiziten und Widersprüchen im Regulierungsgefüge zu kämpfen haben. Das lässt darauf schließen, dass wir zumindest zurzeit eine Regulierungsgrenze erreicht haben, wenngleich gesetzlich zunehmend die „Vollregulierung" sämtlicher IT-Sachverhalte angestrebt wird. Aber auch das Recht der Cybersicherheit selbst entwickelt sich laufend weiter: Manch einer stellt gar fest, dass Cybersicherheit in Zukunft nicht die abstrakte technische Sicherheit von vernetzten IT-Systemen bleibt, sondern als essenzieller Bestandteil in das Produktsicherheitsrecht überführt wird, womit auch das BSI zunehmend die Rolle einer digitalen Marktzulassungs- und Marktüberwachungsbehörde einnehmen dürfte.

Diesen Bogen in der Evolution des Cybersecurity-Rechts spannt auch das vorliegende Schwerpunktheft, das sich unter anderem mit den Fragen der nationalen Cybersicherheitsarchitektur im Bund-Länder-Verhältnis, der komplexen Systematik der Produkt-Cybersicherheitsregulierung, dem Cyber Resilience Act sowie den forschungsrelevanten Fragestellungen in der IoT-Verbrauchersicherheit befasst.

Dennis-Kenji Kipker