MMR

Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT

In Kooperation mit: Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. · davit im DAV – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein · eco – Verband der Internetwirtschaft e.V. · game – Verband der deutschen Games-Branche e.V. · Legal Tech Verband Deutschland e.V. · VAUNET – Verband Privater Medien

5/2026

EDITORIAL

Das neue Exzellenzzentrum IT-Sicherheitsrecht

Lesedauer: 8 Minuten

Die Cybersicherheitslandschaft befindet sich in einem tiefgreifenden Wandel. Die fortschreitende Digitalisierung in Staat, Wirtschaft und Gesellschaft geht nicht nur mit erheblichen Effizienzgewinnen und Innovationspotenzialen einher, sondern zugleich mit einer stetig wachsenden Gefährdung durch hochentwickelte Cyberbedrohungen. Cyberangriffe wie Ransomware-, Phishing- und Lieferkettenangriffe haben in den vergangenen Jahren sowohl an Häufigkeit als auch an Professionalität deutlich zugenommen und prägen das aktuelle Risikobild maßgeblich. Vor diesem Hintergrund wird deutlich, dass klassische, vorwiegend reaktive Sicherheitskonzepte den heutigen Anforderungen nicht mehr gerecht werden. Unternehmen, Behörden und sonstige Einrichtungen sehen sich einer Bedrohungslage gegenüber, die sowohl in ihrer Komplexität als auch in ihrer Dynamik kontinuierlich zunimmt. Parallel hierzu hat die Digitalisierung sämtlicher Lebens- und Wirtschaftsbereiche die strukturelle Abhängigkeit moderner Gesellschaften von informationstechnischen Systemen erheblich verstärkt.

Lisa Grochala

Derya Catakli

Charlotte Berg

Entwicklung des Cybersicherheitsrechts

Diese Entwicklung bleibt nicht ohne Auswirkungen auf die rechtliche Einordnung und Mitigation von Cybersicherheitsrisiken. Das Cybersicherheitsrecht hat sich in den vergangenen Jahren von einer fragmentarischen Gesetzeslage zu einem zentralen Instrument staatlicher und unternehmerischer Risikovorsorge entwickelt. Es dient längst nicht mehr ausschließlich der reaktiven Abwehr, sondern setzt zunehmend im Vorfeld an, indem es Anforderungen an Prävention, Resilienz und Risikomanagement definiert und die Durchsetzung ermöglicht. Auf europäischer Ebene ist dabei eine deutliche regulatorische Verdichtung zu beobachten. Zahlreiche Rechtsakte mit unmittelbarem oder mittelbarem Bezug zur Cybersicherheit sind in den letzten Jahren in Kraft getreten oder befinden sich in fortgeschrittenen Gesetzgebungsverfahren. Gemeinsames Ziel ist es, ein einheitlich hohes Cybersicherheitsniveau innerhalb der Europäischen Union zu etablieren und zugleich die Fragmentierung nationaler Regelungen zu überwinden und dieser vorzubeugen, indem die Rechtsakte vollharmonisierend wirken.

Einen zentralen Bezugspunkt dieser Entwicklung bildet die NIS-2-RL. Sie steht exemplarisch für einen grundlegenden Paradigmenwechsel im europäischen Cybersicherheitsrecht: Weg von einer punktuellen Regulierung einzelner Sektoren hin zu einem umfassenden, risikobasierten Ansatz, der eine deutlich größere Zahl von Unternehmen und Einrichtungen einbezieht. Gleichzeitig verschärft die NIS-2-RL die Anforderungen an das Risikomanagement und normiert die Verantwortlichkeit von Geschäftsleitungen. Sie verfolgt damit einen ganzheitlichen Ansatz, der Cybersicherheit

fest in unternehmerische und organisatorische Strukturen einbindet.

Flankiert wird diese Entwicklung durch weitere europäische Rechtsakte, die jeweils spezifische Aspekte der Cybersicherheit adressieren und in ihrer Gesamtheit zu einem immer dichteren Regulierungsgefüge beitragen. Hervorzuheben ist insbesondere der CRA, der erstmals verbindliche Cybersicherheitsanforderungen für Produkte mit digitalen Elementen normiert und damit ein Mindestmaß an Cybersicherheit für diese einführt. Der CSA etabliert die Agentur der Europäischen Union für Cybersicherheit (ENISA) und legt zudem einen Rahmen europäischer Schemata für Cybersicherheitszertifizierung fest. Auch die KI-VO setzt in diesem Kontext relevante Maßstäbe, indem sie cybersicherheitsbezogene Anforderungen an die Entwicklung und den Einsatz künstlicher Intelligenz formuliert und ebenfalls einem risikobasierten Ansatz folgt. Insgesamt zeigt sich eine klare Tendenz hin zu einer umfassenden, sektorübergreifenden und zugleich differenzierten Regulierung digitaler Systeme und Prozesse.

Herausforderungen für Gesetzgeber und Regelungsadressaten

Die o.g. Entwicklungen stellen auch den nationalen Gesetzgeber vor erhebliche Herausforderungen. Europäische Vorgaben sind nicht nur fristgerecht umzusetzen, sondern müssen zugleich in bestehende nationale Regelungsstrukturen integriert und mit diesen in Einklang gebracht werden. Dies betrifft insbesondere das IT-Sicherheitsrecht sowie die Ausgestaltung und Weiterentwicklung behördlicher Zuständigkeiten und Befugnisse. Zugleich rücken Fragen der effektiven Rechtsdurchsetzung, der Ausgestaltung von Aufsichtsmechanismen sowie der Verhängung wirksamer, verhältnismäßiger und abschreckender Sanktionen stärker in den Fokus. Aus Sicht der Regelungsadressaten ergeben sich ebenfalls zahlreiche Herausforderungen: Durch die Überlappung verschiedener Anforderungen aus parallel anwendbaren Rechtsvorschriften kann es für einzelne Szenarien zu multiplen Pflichten kommen. Der Gesetzgeber reagiert auf diese Problematiken zwar durch Vereinfachungen („Digital Omnibus"), die jedoch erst zukünftig in Kraft treten. In der Zwischenzeit müssen die Regelungsadressaten die geltenden Rechtsvorschriften einhalten.

Rolle des BSI

In diesem dynamischen regulatorischen Umfeld kommt dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine zentrale Rolle zu. Das BSI ist die zentrale Bundesbehörde für Fragen der Informationstechnik und der IT-Sicherheit und nimmt eine koordinierende sowie fachlich normprägende Rolle innerhalb der nationalen Cybersicherheitsarchitektur ein. Ziel des BSI ist es, den sicheren Einsatz von Informations- und Kommunikationstechnik in der Gesellschaft zu ermöglichen und voranzutreiben. Im Zuge der Umsetzung der NIS-2-RL wird das BSI seine Funktion als zentrale Meldestelle für Cybersicherheitsvorfälle weiter ausbauen und zugleich verstärkt Aufgaben im Bereich der Aufsicht über die betroffenen Einrichtungen wahrnehmen. Dies spiegelt sich auch bei der Durchführung des CRA wider: Hier wird das BSI nicht nur als Marktüberwachung und notifizierende Behörde agieren, sondern aktiv die betroffenen Wirtschaftsakteure durch die Durchführung von Sensibilisierungs- und Schulungsmaßnahmen sowie durch die Einrichtung und den Betrieb eines Reallabors für Cyberresilienz unterstützen. Dieses neue Aufgabenfeld weißt deutlich auf eine veränderte Rolle der Aufsichtsbehörden hin: Statt wie bisher hauptsächlich eine sanktionsgeprägte Funktion wahrzunehmen, sollen diese zunehmend als unterstützender Partner mit dem gemeinsamen Ziel einer verbesserten Cyberresilienz wahrgenommen werden. Darüber hinaus versteht sich das BSI zunehmend als Impulsgeber und Plattform für den fachlichen Austausch sowie für die Weiterentwicklung des Cybersicherheitsrechts.

Exzellenzzentrum IT-Sicherheitsrecht

Mit dem im Jahr 2024 gegründeten Exzellenzzentrum IT-Sicherheitsrecht hat das BSI eine zentrale Anlaufstelle geschaffen, die diesen Anforderungen Rechnung trägt und das IT-Sicherheitsrecht im nationalen rechtswissenschaftlichen Diskurs auf die Agenda hebt. Das Exzellenzzentrum IT-Sicherheitsrecht verfolgt das Ziel, im Austausch mit Stakeholdern aus Verwaltung, Wissenschaft und juristischer Fachwelt die Weiterentwicklung nationaler Kompetenzen im Bereich des Cybersicherheitsrechts zu fördern. Dies umfasst zum einen das Halten und Besuchen von Vorträgen rund um das Cybersicherheitsrecht auf Fachkonferenzen und -tagungen. So hat das Exzellenzzentrum IT-Sicherheitsrecht bereits im vergangenen Jahr einige Vorträge mit cybersicherheitsrechtlichem Bezug gehalten wie zB zum sicheren Einsatz von KI oder zu den aktuellen Entwicklungen des Cybersicherheitsrechts. Zum anderen steht die Veröffentlichung von juristischen sowie interdisziplinären Beiträgen und Artikeln in Fachzeitschriften auf der Agenda, um auch stärker in den wissenschaftlichen Diskurs einzusteigen. Hier soll insbesondere auch der Blick auf die behördliche Praxis gelegt werden. Perspektivisch ist die Entwicklung weiterer Formate zum gezielten Austausch geplant.

Der Austausch soll dazu beitragen, aktuelle Entwicklungen frühzeitig aufzugreifen, praktische Herausforderungen zu identifizieren und Impulse für die Fortentwicklung des Rechts zu setzen. Zugleich unterstreicht die zunehmende Dichte europäischer Regelungen den Handlungsbedarf bei der cybersicheren Ausgestaltung digitaler Prozesse. Der Aufbau dieses Netzwerks soll daher nicht nur den bestehenden Austausch sichern, sondern auch neue Formate ermöglichen und Synergiepotenziale gezielt erschließen.

Das Exzellenzzentrum IT-Sicherheitsrecht bietet hierbei eine einzigartige Perspektive: Durch die Ansiedelung am BSI deckt es nicht nur eine juristische Perspektive ab, sondern kann, durch den engen Kontakt zu den Fachabteilungen, auch praktische Auswirkungen eines veränderten Cybersicherheitsrechts auf die IT-Sicherheitslandschaft in Deutschland in den Diskurs einbringen. Die Expertise des Hauses umfasst hierbei eine große Bandbreite, von Fragen des nationalen Sicherheitsrechts über IT-sicherheitsrechtliche Aspekte in Bezug auf kritische Infrastrukturen bis hin zu cybersicherheitsrechtlichen Anforderungen an Produkte mit digitalen Elementen. Dieses gebündelte Fachwissen ist in seiner Ausprägung deutschlandweit einzigartig. Bisher bringt das BSI diese Expertise auch und vor allem iRd Beratung der Bundesregierung bei Gesetzgebungsverfahren, wie zB dem NIS2UmsuCG oder aktuell dem CRA ein. Um dieses Expertenwissen einer breiten Öffentlichkeit zugutekommen zu lassen, versteht sich das Exzellenzzentrum für IT-Sicherheitsrecht als Schnittstelle zu den verschiedenen Stakeholdern.

Signifikanz eines kontinuierlichen Austauschs

Angesichts der dargestellten Dynamik und Komplexität wird deutlich, dass die Fortentwicklung des Cybersicherheitsrechts nicht isoliert erfolgen kann. Sie lebt vom kontinuierlichen Austausch zwischen Gesetzgebung, Verwaltung, Wirtschaft und Wissenschaft sowie von der Zusammenführung unterschiedlicher Perspektiven und Erfahrungen.

Das Exzellenzzentrum IT-Sicherheitsrecht versteht sich daher als Dialograum, in dem aktuelle Fragestellungen gemeinsam aufgegriffen, diskutiert und weitergedacht werden können. Kontaktaufnahmen, Vortragsanfragen und fachliche Gespräche sind ausdrücklich willkommen. Ziel ist es, eine Plattform zu schaffen, auf der Wissen geteilt, Perspektiven gebündelt und praxisnahe Lösungen entwickelt werden. Denn ein belastbares, praxisgerechtes Cybersicherheitsrecht/IT-Sicherheitsrecht entsteht nur dort, wo unterschiedliche Erfahrungen zusammenfließen und Entwicklungen aktiv begleitet werden.

Bonn, im Mai 2026

Lisa Grochala, Derya Catakli, Charlotte Berg
sind Referentinnen im Referat K 25 – IT-Sicherheit und Recht beim BSI in Bonn.