Nationale Krisenbewältigung in der Cybersicherheit

Die verfassungsrechtliche Schutzpflicht des deutschen Staates, ihre Ausgestaltung und Grenzen

Prof. Dr. Dennis-Kenji Kipker, Bremen

A. Grundrechtliche Gewährleistungen der Cybersicherheit

- **Allgemeines Persönlichkeitsrecht (APR) gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG:** Kernbereichsschutz/Schutz der Intimsphäre auch im digitalen Bereich
  - **Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG:** Befugnis des Einzelnen, selbst über die Verwendung seiner persönlichen Daten zu bestimmen, soweit keine Ausnahmen greifen
  - **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht bzw. Computer-Grundrecht) gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG:** Computer als „ausgelagertes Gedächtnis“, Schutz vor Kompromittierung der Vertraulichkeit komplexer IT-Systeme
- **Fernmeldegeheimnis (Telekommunikationsgeheimnis) gem. Art. 10 GG:** Schutz der unkörperlichen Übermittlung von Nachrichten vor unbefugter Kenntnisnahme

B. Grundrechtsfunktionen in der Cybersicherheit

- Unterscheidung zwischen Abwehr- und Schutzfunktion
- Handlungsmaßstab für gesetzgeberisches und behördliches Handeln bei Grundrechtseingriffen
- **Abwehrfunktion:** Schutz des Bürgers **VOR** dem Staat, historisch gewachsene Grundrechtsfunktion (Übermaßverbot)
- **Schutzfunktion:** Schutz des Bürgers **DURCH** den Staat, kann auch Handlungspflichten des Staates auslösen, den Bürger vor rechtswidrigem/unzulässigem Einfluss Dritter zu schützen (sog. Leistungs- und Gewährleistungsrechte, Untermaßverbot zu beachten!) → jedoch: weit gefasster staatlicher Entscheidungsspielraum!
- Häufig kommunizierter **„Widerstreit" von Freiheit und Sicherheit** findet sich hier wieder und erfordert Verhältnismäßigkeitsprüfung für jedwedes staatliche Handeln (Interessenabwägung verschiedener Grundrechtspositionen)!

C. Staatliche Schutzpflichten in der Cybersicherheit: Beispiele

- Umsetzung und Kontrolle von Datensicherheitsstandards ggü. „Big Tech“
- Schutz von Bürger:innen vor Ausforschung durch „fremde Mächte“
- Gewährleistung der Versorgungssicherheit und Funktionsfähigkeit lebenswichtiger IT bzw. von Diensten, die hierauf angewiesen sind (z.B. KRITIS, korreliert an dieser Stelle mit Schutzpflichten aus weiteren Grundrechten, z.B. Leben und körperliche Unversehrtheit)

Dennis-Kenji Kipker / Friederike Voskamp

PRISM und staatliche Schutzpflichten – ein politisches Märchen?

Die Datenströme machen an den nationalstaatlichen Grenzen nicht halt. Besonders deutlich wurde die globale Vernetzung des Datenverkehrs an dem zur Jahresmitte 2013 vom amerikanischen Whistleblower Edward Snowden bekannt gemachten NSA-Skandal, in dessen Rahmen auch die personenbezogenen Daten deutscher Bürger zu Zwecken der öffentlichen Sicherheit von amerikanischen Regierungsbehörden ausgewertet wurden. Folglich bedeutet für die Zukunft die Interessenabwägung zwischen informationeller Freiheit und staatlicher Sicherheit nicht nur, sich auf die Kontrollrechte und Abwehrmöglichkeiten gegenüber nationalen, deutschen Behörden zu beschränken. Darüber hinaus stellt sich die Frage, ob die informationellen Grundrechte in Deutschland über ihre Abwehrfunktion hinaus Geltung beanspruchen können, indem der einzelne Betroffene auch eine Schutzfunktion des deutschen Staates in Bezug auf seine Privatsphäre gegenüber fremden Staaten einfordern kann, die in seine informationelle Freiheit zu Zwecken der Aufrechterhaltung der öffentlichen Sicherheit eingreifen.

D. Rechtsrahmen und Verwaltungshandeln in der Cybersicherheit: die Rolle des Bundes

- **Umfassendes staatliches Betätigungsfeld für Cybergefahren, die über den Kontext einzelner Länder hinausgehen:** Abgrenzung von nachrichtendienstlichem Tätigwerden, Gefahrenabwehr und Strafverfolgung
  - **Sonderrolle:** Tätigwerden der Bundeswehr im CIR („aktive Cyberabwehr/„Hackback“)
- Aufgabenzuweisungen resultieren in komplexem behördlichen Zuständigkeitsgefüge inkl. bereichsspezifischer Gesetzgebung, die Cybersecurity auch nur mittelbar adressieren kann: https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur
- Cybersicherheit als **Querschnittsthema**, das viele Einrichtungen in Teilbereichen tangiert
- Unterscheidung zwischen strategischer und operativer Ebene:
  - **Strategische Ebene:** Bundeskanzleramt und Bundesministerien in ihren Geschäftsbereichen; Nationaler Cyber-Sicherheitsrat (NCSR)
  - **Operative Ebene:** Spezifische Geschäftsbereichsbehörden – v.a. BSI, BfV, BKA, BND, MAD, BPol, BBK; Kooperations- und Koordinierungseinrichtungen – Nationales Cyber-Abwehrzentrum (NCAZ)

E. Rechtsrahmen und Verwaltungshandeln in der Cybersicherheit: die Rolle der Länder

- **Kompetenzgefüge zwischen Bund und Ländern:** IT-Sicherheit als Bestandteil der öffentlichen Sicherheit und als Voraussetzung für das Funktionieren staatlicher Organisationen

- **Föderale Aufteilung gesetzgeberischer Kompetenz begründet vor allem auch Verantwortung der Länder** → Länder müssen für eigene Sicherheit und Sicherheit der Zivilgesellschaft selbst aufkommen und können entsprechende Landesgesetze erlassen

- **Gesetzliche Anforderungen der Länder:** Cybersicherheit vorwiegend verstanden als Absicherung von IT-Systemen der Länder, Beispiel Bayern:

  - Gesetz über die elektronische Verwaltung in Bayern (BayEGovG)

  - Gesetz zur Errichtung des Landesamts für Sicherheit in der Informationstechnik

- **Landesbeauftragte für Informationssicherheit häufig in den Innenministerien verortet:** deutlicher Bezug zur Gefahrenabwehr als Länderaufgabe, verbesserter und beschleunigter Informationsaustausch **(„Time is Security!“)**

- Verwaltungs-CERT-Verbund (VCV) als institutionalisierte, teilnehmergeschlossene Kooperationsgemeinschaft

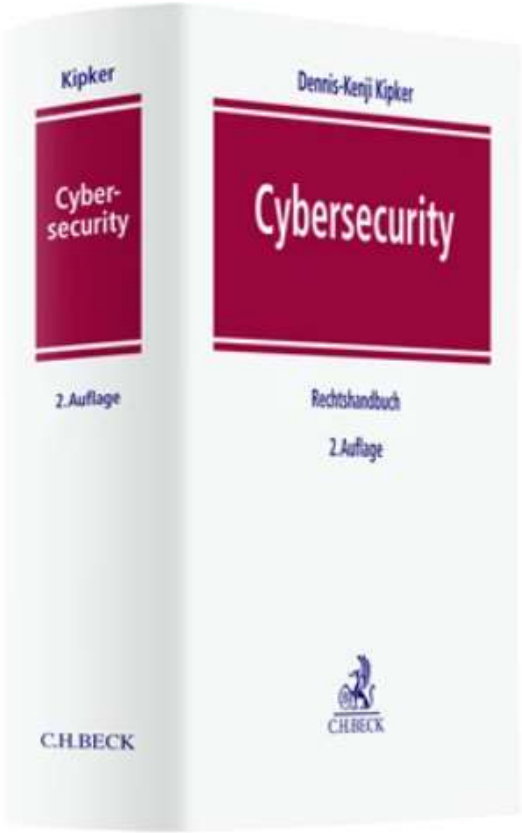
- **Verwaltungspraxis:** Gefälle in der Cybersicherheit zwischen bevölkerungsreichen Flächen- und Stadtstaaten feststellbar

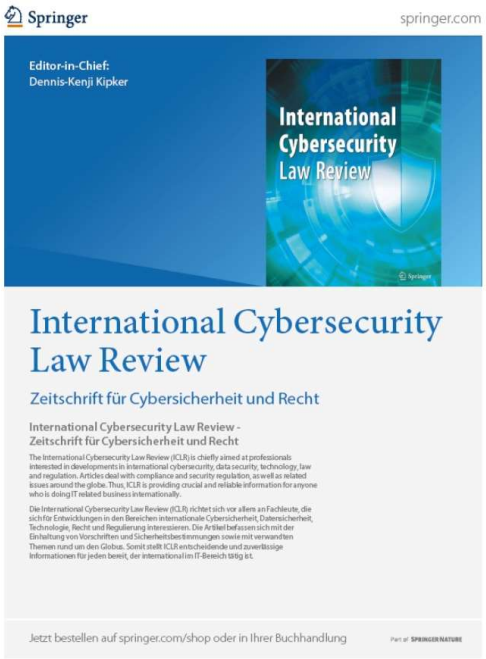
- **Kommunale Cybersicherheit** bislang nicht/unzureichend in die Landesregelungen zur IT-Sicherheit einbezogen

F. Fazit und Ausblick

- Cybersicherheit wird durch verschiedene **verfassungsrechtliche Gewährleistungen** adressiert und ist abhängig vom Anknüpfungspunkt des jeweils konkret zu schützenden Rechts/Rechtsguts → **Interessenabwägung notwendig!**
- **Grundrechtsfunktionen** ermöglichen weit gefasste Einschätzungsprärogative des Staates mit Blick auf Schutzpflichten zur Cybersicherheit
- **Föderalistisches Gefüge** zur Cybersicherheit ist in Deutschland hochkomplex und keinesfalls in sich geschlossen/widerspruchsfrei
- Zunehmende **Kompetenzverlagerung in den Bund** einerseits notwendig aufgrund länderübergreifender Bedrohungslage („Cyberwar"), andererseits auch Schutz von Verwaltung und **Daseinsvorsorgeträgern vor Ort** zwingend notwendig (insb. Sub-KRITIS)
- Status quo der **kommunalen Cybersicherheit** verbesserungsbedürftig – sowohl regulatorisch, finanziell als auch technisch-organisatorisch – insb. in der Informationsanbindung im Hinblick auf kommunale Verwaltungsnetze und aktuelle Cyberbedrohungen

Weiterführende Literatur





Vielen Dank für die Aufmerksamkeit!

Prof. Dr. Dennis-Kenji Kipker

contact@denniskenjikipker.de