# Freiheit und Sicherheit im digitalen Raum: Akteure und Steuerungsmechanismen in vergleichender Perspektive

## Gemeinsames Panel des Forums Junge Staats-, Verwaltungs- und Policyforschung (FoJuS) und der Nachwuchsgruppe Vergleichende Politikwissenschaft im Rahmen des DVPW-Kongresses 2015

*Chair: Dr. Stefan Thierse, Universität Duisburg-Essen*

*Discussants: Prof. Dr. Christoph Bieber, Universität Duisburg-Essen / Dr. des. Toralf Stark, Universität Duisburg-Essen*

Das Verhältnis von Freiheit und Sicherheit steht im digitalen Zeitalter vor neuen Herausforderungen. Der digitale Raum verheißt ein Mehr an Freiheit. Ein vielfältigeres Informations- und Kommunikationsangebot ermöglicht es mehr Menschen als je zuvor, von ihrem individuellen Recht auf freie Meinungsäußerung Gebrauch zu machen. Dieses Mehr an Freiheit geht allerdings auch mit einem gesteigerten Bedürfnis nach Sicherheit einher.

Im digitalen Raum verschwimmen nicht nur die Grenzen zwischen öffentlicher und privater Sphäre, auch die Anonymität schafft eine neue Dimension von Gefährdungslagen, die sowohl das politische System als auch die Gerichtsbarkeit vor komplexe Herausforderungen stellt. Der Diebstahl persönlicher Daten, Wirtschafts- und Industriespionage oder die Instrumentalisierung gesellschaftlicher, politischer oder religiöser Konflikte durch Gewaltaufrufe und Hetze sind nur einige Beispiele für die Notwendigkeit einer Neuvermessung des Sicherheitsbegriffs im digitalen Raum. Wie schwierig es ist, ein angemessenes Verhältnis von Freiheit und Sicherheit im digitalen Zeitalter zu definieren, zeigt sich exemplarisch an der Forderung seitens der Politik, die Gewährleistung von Sicherheit mit der Einschränkung von Freiheitsrechten zu begründen. Die Vorratsdatenspeicherung oder die Totalüberwachung von Kommunikationsprozessen werden als ein mögliches Mittel diskutiert, um die Sicherheit der Bürger zu schützen.

Der Beitrag der Politikwissenschaft auf diesem Feld nimmt sich nach wie vor eher bescheiden aus. Diesen Umstand nimmt das gemeinsam von der Nachwuchsgruppe Vergleichende Politikwissenschaft und dem Forum Junge Staats-, Policy- und Verwaltungsforschung (FoJuS) ausgerichtete Panel zum Anlass, um u.a. folgende Forschungsfragen zu adressieren:

- Warum gestaltet es sich gerade in demokratischen Gesellschaften so schwierig, die ‚richtige' Balance zwischen Freiheitsrechten und Sicherheitsbedürfnissen zu finden?
- Mit welchen Formen der Bedrohung im digitalen Raum sehen sich staatliche und private Akteure konfrontiert?
- Welche Strategien für eine Sicherheitspolitik im digitalen Raum existieren insbesondere aus vergleichender Perspektive?
- Welche öffentlichen Sicherheitsstrukturen existieren ländervergleichend auf dem Feld der Sicherheit im digitalen Raum?
- Welche Akteure und Steuerungsmechanismen kennzeichnen das Feld der Sicherheit im digitalen Raum im Allgemeinen (ländervergleichend) als auch im Besonderen (länder-spezifisch)?
- Inwiefern sind die etablierten methodischen und theoretischen Ansätze der Politik- und Verwaltungswissenschaft dem Problemgegenstand angemessen? Welche alternativen Ansätze bieten sich an?

**Cybersicherheitsstrategien an deutschen Hochschulen. Eine Analyse anhand des Securitization-Ansatzes**

*Lena Ulbricht (WZB Berlin)*

Welche Folgen hat der Bedeutungszuwachs von Cybersicherheit im öffentlichen Diskurs und in politischen Strategien für den Umgang mit IT-Sicherheit an Hochschulen? Auf der einen Seite werden vielfältige Bedrohungsszenarien für die IT-Sicherheit an Hochschulen identifiziert (Datenklau, Sabotage, Missbrauch der Infrastruktur) und Forderungen nach einer Verbesserung der IT-Sicherheit geäußert. Auf der anderen Seite gelten Hochschulen, anders als staatliche Behörden und privatwirtschaftliche Unternehmen als zwar zunehmend strategische, aber dennoch nur bedingt steuerbare Akteure. Zudem stehen Sicherheitsstrategien an Hochschulen in einem Spannungsverhältnis zum Prinzip der Freiheit von Forschung und Lehre.

Der Vortrag untersucht die Entwicklung von IT-Sicherheitsstrategien an deutschen Hochschulen anhand des Securitization-Ansatzes: Sicherheitsstrategien gründen sich hier weniger auf messbare Risiken, sondern werden vielmehr als Gegenstand eines konflikthaften, kollektiven Verständigungsprozesses verstanden. Anhand von Dokumenten (etwa IT-Sicherheitskonzepten) und Experteninterviews mit Sicherheitsverantwortlichen an Hochschulen soll rekonstruiert werden, welche Akteure innerhalb und außerhalb der Hochschulen Konflikte bezüglich einer Versicherheitlichung der Hochschulen austragen und welche Strategien sie dabei verfolgen.

## Staatliche Regulierung von Hatespeech im Internet

*Dr. Christoph Busch (Ministerium für Inneres und Kommunales Nordrhein-Westfalen, Abteilung Verfassungsschutz)*

Das Internet stellt staatliche Regulierungsversuche vor neuartige Herausforderungen – dies betrifft auch die Versuche, die Verbreitung von Hatespeech im Internet zu verhindern. So stehen sämtliche Regulierungsmaßnahmen vor dem normativen Problem, den Schutz der Menschenwürde zu garantieren, ohne die Meinungsfreiheit unverhältnismäßig einzuschränken. Zudem scheint die Effektivität von nationalstaatlichem Handeln bei diesem Regulierungsobjekt fraglich zu sein. Vor diesem Hintergrund wird in dem Vortrag der Frage nachgegangen, wie der Staat versucht, Hatespeech im Internet zu unterbinden und inwieweit er dabei die Kriterien der Legitimität und Effektivität staatlichen Handelns erfüllt.

In dem Beitrag wird die Vielzahl von einzelnen Regulierungsmaßnahmen in drei Regulierungstypen zusammengefasst und deren jeweilige Legitimität und Effektivität erörtert. 1. Der nationalstaatlich intervenierende Staat, der unter anderem mit Filtern und Sperren von Internetinhalten neuartige Regulierungsinstrumente entwickelt. 2. Der international kooperierende Staat, der durch die Zusammenarbeit mit anderen Staaten reguliert. 3. Der zivilgesellschaftlich aktivierende Staat, der auf indirekte Steuerung setzt, indem er die Zivilgesellschaft zur Selbstregulierung befähigt und unterstützt. Abschließend wird vergleichend diskutiert, welcher Regulierungstypus, beziehungsweise welcher Mix von Regulierungsmaßnahmen sowohl ein hohes Maß an Legitimität als auch an Effektivität verspricht.

## Datenschutzbehörden im internationalen Vergleich

*Philip Schütz (Fraunhofer Institut für System- und Innovationsforschung ISI/Institut für Politikwissenschaft der Universität Göttingen)*

Das Spannungsverhältnis von Freiheit und Sicherheit im digitalen Raum spiegelt sich momentan verstärkt im Themenkomplex Datenschutz und der Frage, wie der Umgang mit personenbezogenen Daten reguliert werden soll, wider. Aktuell werden hier vor allem das in Verhandlungen stehende Datenschutzreformpaket auf EU-Ebene sowie die Notwendigkeit einer besseren Kontrolle von Geheimdiensten (angestoßen durch die Snowden-Enthüllungen) diskutiert. Bis auf wenige Ausnahmen hat die Politikwissenschaft das Thema Datenschutz trotz seiner großen Relevanz bisher jedoch stiefmütterlich vernachlässigt. Aus diesem Grund soll dieser Beitrag, der erste Ergebnisse einer sich momentan im Verschriftlichungsprozess befindlichen Dissertation beinhaltet, helfen, diese auffallend große Forschungslücke zu verkleinern. Die Dissertation widmet sich in Form einer intra-europäischen Vergleichsstudie dem zentralen Regulierungsakteur im Themenfeld Datenschutz: den Datenschutzbehörden. Es soll die Frage geklärt werden, inwieweit sich institutionelle Beschaffenheit und

Regulierungspraktiken von Datenschutzbehörden in EU-Mitgliedsländern voneinander unterscheiden und worin hierfür die Gründe liegen.

Basierend auf Theorien zum *regulatory state* und dem daraus hervorgegangenen Konzept der *Independent Regulatory Authorities (IRAs)* wurden zentrale Merkmale von Datenschutzbehörden wie deren Unabhängigkeit, finanzielle und personelle Ausstattung sowie Regulierungsinstrumente zum einen *de jure* (also in Form einer Gesetzes- und Dokumentenanalyse) und zum anderen *de facto* (in Form von leitfadengestützten Experteninterviews) analysiert. Die Länderfallstudien beinhalten Großbritannien, Schweden, Polen und Deutschland (Bundesebene sowie eine Auswahl von Bundesländern). Zur Erklärung für die Unterschiede in institutioneller Beschaffenheit und Regulierungspraktiken wird u.a. auf Schulen der vergleichenden Staatstätigkeitsforschung zurückgegriffen. Insbesondere sollen hier politisch-institutionalistische Theorien sowie Effekte der Internationalisierung als Erklärungsansätze herangezogen und untersucht werden. Dabei ist bereits abzusehen, dass neben historisch bedingten Pfadabhängigkeiten in der rechtlichen Ausgestaltung von Datenschutzbehörden und dem Einfluss von internationalen Regimen vor allem der individuelle Führungsstil des Datenschutzbeauftragten in Verbindung mit ländertypischen Regulierungstraditionen und -ansätzen wichtige Determinanten für die Art und Weise, wie eine Datenschutzbehörde aufgestellt ist und wie Regulierung stattfindet, darstellen.

## Freiheit oder Sicherheit: Analysen zur Akzeptanz digitaler Überwachungspolitiken im deutsch-britischen Vergleich

*Matthias Bug (Deutsches Institut für Wirtschaftsforschung) / Dr. Sebastian Bukow (Heinrich-Heine-Universität Düsseldorf)*

Die Digitalisierung des Alltags betrifft in besonderer Weise das Politikfeld ‚Innere Sicherheit'. Die Verknüpfung des individuellen und gesellschaftlichen Handelns mit dem virtuellen Raum verändert die alltägliche Kommunikation, Mobilität und Informationsfülle. In der Folge sieht sich der sicherheitsgewährleistende Nationalstaat gezwungen, auch im digitalen Raum seiner sicherheitspolitischen Verpflichtung durch eine ‚digitale' Sicherheitspolitik nachzukommen. Dabei werden unterschiedliche Maßnahmen diskutiert (bspw. Vorratsdatenspeicherung, Fluggastdatenspeicherung, Europäischer Datenaustausch). Im internationalen Vergleich zeigen sich deutliche Unterschiede in der Akzeptanz dieser Maßnahmen. Im Beitrag fokussieren wir daher auf die Adressatenseite staatlicher Sicherheitsmaßnahmen und fragen nach deren Akzeptanz in der Bevölkerung. Wir fragen danach, welche Faktoren auf individueller Ebene zur Akzeptanz oder Ablehnung spezifischer Überwachungs-/Sicherheitsmaßnahmen führen. Dazu wird zunächst ein allgemeines Modell der Akzeptanz (digitaler) Sicherheitsmaßnahmen entwickelt, das anschließend empirisch für Deutschland und Großbritannien überprüft wird, also für zwei Länder, deren Sicherheitspolitiken und -kulturen sich stark unterscheiden. Im Ergebnis zeigt sich, dass

nicht nur der institutionell-gesellschaftliche Rahmen, sondern auch konkrete individuelle Erfahrungen und Präferenzen für die Akzeptanz oder Ablehnung von digitalen Sicherheitsmaßnahmen entscheidend sind. Der Beitrag liefert somit einen theoretisch und empirisch fundierten Einblick in die Adressatenseite digitaler Sicherheitspolitik und weist darüber hinaus Bezüge zur Legitimation(-snotwendigkeit) staatlichen Handelns in diesem Politikfeld auf.