TAGUNG

Die Rolle der Europäischen Union – zwischen dem Ausbau von Kontrolle und dem Schutz von Daten

Jana Hunnius, Frédéric Krumbein und Benjamin Schmidt[*]

Reacting to Surveillance by Security Agencies in the Age of Big Data – What is the Role of the European Union?

Hochschule für Wirtschaft und Recht Berlin und Arbeitskreis Europäische Integration e.V.

Mit finanzieller Unterstützung der Europäischen Union und der Groupe Européen de Recherches sur les Normativités (GERN)

13./14. Mai 2016, Berlin

Begrüßung

Prof. Dr. Andreas ZABY, President, Hochschule für Wirtschaft und Recht Berlin
Prof. Dr. Sabrina SCHÖNROCK, Dean, Department of Police and Security Management, Hochschule für Wirtschaft und Recht Berlin
Prof. Dr. Clemens ARZT, Director, Forschungsinstitut für Öffentliche und Private Sicherheit, Berlin
Prof. Dr. Hartmut ADEN, Hochschule für Wirtschaft und Recht Berlin

Surveillance technology and its impact upon everyday life

Chair: Prof. Dr. Clemens ARZT, Director, Forschungsinstitut für Öffentliche und Private Sicherheit, Berlin

The impact of surveillance on private life: the example of electronic surveillance in the criminal justice system
Dr. Dr. Peter ULLRICH, Technische Universität Berlin

Der Einfluss von Surveillance-Technologien auf das Alltagsleben

Peter Ullrich sprach über ‚surveillance' und ‚counter-surveillance' und stellte beide Phänomene anhand empirischer Befunde aus der Protestforschung in Deutschland und Österreich vor. Vorherrschend in der Diskussion um ‚surveillance' sei lange die Idee des „Panopticons" (Michel Foucault) gewesen, bei der die Asymmetrie zwischen Beobachter und Beobachteten zentral sei. Aus einer neueren Perspektive, dem Ansatz der „surveillant assemblage" (Kevin D. Haggerty/Richard V. Ericson), gehe man davon aus, dass sich gerade die Struktur von Überwachung verändert hat, diese nun die Gesellschaft „durchzieht" und das Beobachten des jeweils anderen auf Gegenseitigkeit beruht.

Diese Veränderungen zeichnete Ullrich anhand von Videoaufnahmen bei Protestaktionen nach. Er zeigte zunächst, dass der vermeintlich neutrale Vorgang des Aufnehmens sozial gerahmt ist und Entscheidungen über den Moment der Aufnahme, den (gewählten) Ausschnitt, die Verwendung als gerichtliches Beweismittel, beispielsweise durch Behörden, und die Möglichkeit zur Sicherung einer bestimmten Sichtweise oder Deutung der (Protest-)Situation bietet. Zugleich erstellten Demonstranten eigenes Videomaterial, um das Geschehen aus ihrer Perspektive festzuhalten. Dieses Vorgehen, in dem beide Seiten Daten produzieren, gleiche einem „sozialen Tanz" (Gary T. Marx), bei dem es um die Kontrolle

* Jana Hunnius, Universität Potsdam.
Dr. Frédéric Krumbein, Geschäftsführer des Arbeitskreises Europäische Integration e.V., Berlin.
Benjamin Schmidt, Hochschule für Wirtschaft und Recht Berlin.

DOI: 10.5771/0720-5120-2016-4-354

des jeweils anderen geht. Ullrich mahnte, diese Dynamiken im Diskurs um die Entwicklung von Bürgerrechten und Datenschutz im Blick zu behalten.

Anja Mihr sprach über Menschenrechte im virtuellen Raum und stellte die gemeinsame Verantwortung der Staatengemeinschaft heraus, diese in diesen Kontext zu integrieren. Sie veranschaulichte in ihrem Vortrag, dass der virtuelle Raum nicht nur ein grenzenloser, sondern mit dem Aufschluss des Südens ein noch immer stetig wachsender Raum sei, dem jedoch bisher eine gemeinsame rechtliche Rahmung sowie eine globale oder transnationale Gerichtsbarkeit fehlten.

Eine Möglichkeit, Haftung von Akteuren im virtuellen Raum sowie Transparenz zu gewährleisten, stelle der Ansatz der „cyber justice" dar. Ziel dieses Konzepts sei, unter Berücksichtigung der Menschenrechte eine gleichberechtigte Nutzung des virtuellen Raums zu gewährleisten und dabei dessen gemeinsame Regulierung über Institutionen wie Gerichte, Regierung, Polizei oder Parlament zu erreichen. Diese Institutionen sollten einerseits virtuelle Aktivitäten fördern, gleichzeitig jedoch Schutz für alle Nutzer bieten, gleich welcher nationalen Zugehörigkeit. Der Schutz der Nutzer in Form der Sicherstellung von Menschenrechten und damit auch eine Haftbarmachung bei Verletzung könnten, so Mihr, nur als gemeinsame, internationale Aufgabe begriffen werden.

Christopher Dunn zeichnete in seinem Vortrag die Entwicklungen von „mass surveillance" aus Perspektive der amerikanischen Bürgerrechte nach. Während es seit dem 11. September 2001 eine verstärkte öffentliche Befürwortung von Überwachungsaktivitäten gegeben habe, seien die Snowden-Enthüllungen im Jahr 2013 ein Wendepunkt gewesen und hätten eine Debatte über exzessive Überwachungspraktiken angestoßen. Dies habe, so Dunn, in der Folge zu Veränderungen

Privacy and Human Rights in the Cyberspace
Prof. Dr. Anja MIHR, Programme Director, Center on Governance through Human Rights, Berlin

Mass surveillance – perceived from a US civil liberties perspective
Prof. Christopher DUNN, New York Civil Liberties Union, New York

Limiting or promoting surveillance & mass surveillance versus targeted surveillance: how EU institutions shape and react to surveillance
Chair: Prof. Dr. Hartmut ADEN, Hochschule für Wirtschaft und Recht Berlin

Norm transfer for surveillance: from transatlantic Passenger Name Records to PNR in the EU
Prof. Dr. Christian KAUNERT, Director, European Institute for Security and Justice (EISJ), University of Dundee; and Dr. Sarah LÉONARD, Senior Lecturer, University of Dundee

Mass surveillance by intelligence services – inevitable in times of terrorist threat?
Chair: Prof. Dr. Hans-Gerd JASCHKE, Hochschule für Wirtschaft und Recht Berlin

Intelligence cooperation in the EU: Is there a trend towards regime formation?
Dr. Anna DAUN, Hochschule für Wirtschaft und Recht Berlin

No rules are good rules? Data Protection, Information Sharing & Intelligence Cooperation in Europe
Dr. Ben WAGNER and Kilian VIETH, Centre for Internet and Human Rights, Viadrina University, Frankfurt/Oder

Can mass surveillance by intelligence services be integrated into a rule-of-law framework?
Dr. Konstantin von NOTZ, Member of the German Federal Parliament, Chair of the Inquiry Committee on NSA surveillance, Berlin

How to react to new forms of surveillance in Europe?
Chair: Dr. Frédéric KRUMBEIN, Arbeitskreis Europäische Integration, Berlin

The implementation of Prüm: Are we ready for a central European DNA database?
Inès GALLALA, Free University of Brussels

Do citizens accept surveillance? Divergent or convergent trends in Europe?
Mathias BUG, University of Marburg

in der Überwachungspraxis und bei Gesetzen geführt, dennoch sei der datenschutzrechtliche Rahmen in den USA noch immer nicht ausreichend. Es fehle an einer grundlegenden Transparenz. Als besonders problematisch stellte er heraus, dass die Dokumentation der Überwachungspraktiken nicht zugänglich ist und deshalb nicht aktiv dagegen vorgegangen werden könne.

Verdachtsunabhängige Vorratsdatenspeicherung von Passagierdaten

Christian Kaunert und *Sarah Léonard* sprachen über die Sammlung und Verwendung von Fluggastdaten in der Europäischen Union und deren Austausch mit den USA. Passagierdaten beinhalteten alle Angaben, die ein Passagier bei Buchung, Check-in und Boarding preisgibt. Die erfassten Personen seien der Polizei in der Regel nicht bekannt, da sie zum allergrößten Teil weder Verdächtige noch Straftäter seien.

Es gebe grundsätzlich zwei Möglichkeiten für den Staat, auf diese Daten zuzugreifen: die „Pull-Methode", das heißt, die staatlichen Behörden würden Zugang zu den Daten bei den Fluglinien erhalten, oder die „Push-Methode", das heißt, die Fluglinien transferierten die Daten an die Behörden.

Kaunert und Léonard erklärten anhand des Agenda-Setting-Modells, wie der Zugriff auf Passagierdaten in der Europäischen Union eingeführt wurde. Beim Agenda-Setting gebe es drei relativ unabhängige Ströme: Probleme, politische Alternativen und die Politik. Diese Ströme existierten die meiste Zeit parallel und an einigen Stellen würden sie aber konvergieren. Bei einer Konvergenz entstehe politische Veränderung, wie zum Beispiel ein neues Gesetz. Die Vortragenden definierten zudem Normen als geschriebene oder ungeschriebene Regeln, die Verhalten beschränken, konstituieren oder ermöglichen, indem sie einen Standard für angemessenes Verhalten setzten. Im verwendeten Modell des Agenda-Setting gebe es einen vierten Strom, den „Normstrom".

Anhand des Zusammenspiels dieser vier Ströme erläuterten Kaunert und Léonard, wie die Speicherung und der Austausch von Passagierdaten in verschiedenen Schritten erst auf Druck der USA und schließlich aufgrund eigener Erfahrungen mit Terroranschlägen in der Europäischen Union umgesetzt wurden.

The European Union and public-private partnerships for securing and surveilling cyberspace
Dr. Raphael BOSSONG, Viadrina University Frankfurt/Oder

Technological autonomy – a European answer to surveillance

Chair: Dr. Daniel VENTRE, Centre de recherches Sociologiques sur le Droit et les Institutions Pénales, Guyancourt

Mutual legal assistance, data localization and the long arm of law enforcement agencies
Jan-Peter KLEINHANS, Stiftung Neue Verantwortung, Berlin

Cryptography – an effective strategy to limit surveillance?
Prof. Dr. Rüdiger WEIS, Beuth Hochschule für Technik, Berlin

Comment: The impact of surveillance from the perspective of critical criminology
Prof. Dr. Dr. Fritz SACK, University of Hamburg

Roundtable

The EU's ambivalent role for surveillance: conference results and outlook
Prof. Dr. Hartmut ADEN, Hochschule für Wirtschaft und Recht Berlin

Statements: Limiting or promoting surveillance? What role can and should the EU play in the future? What should be the role of (critical) surveillance studies?
Dr. Raphael BOSSONG, Viadrina University Frankfurt/Oder
Dr. Anna DAUN, Hochschule für Wirtschaft und Recht Berlin
Prof. Dr. Christian KAUNERT, Director, European Institute for Security and Justice (EISJ), University of Dundee

Die USA führten im November 2001 den „US Aviation and Transportation Security Act“ ein, der den USA Zugang zu allen Passagierdaten von Fluglinien ermöglicht habe, die in den USA operieren. Aber dieses Gesetz habe eine Verletzung von EU-Datenschutzbestimmungen dargestellt, sodass eine Sonderregelung für EU-Fluglinien gefunden werden musste. Im Mai 2006 sei diese aber vom Europäischen Gerichtshof gekippt und in den Jahren 2007 und 2011 seien ein zweites und drittes Abkommen vereinbart worden.

Die Europäische Union habe schließlich selbst ein System für die Speicherung von Passagierdaten eingeführt: Im April 2016 sei vom Europäischen Parlament eine entsprechende Richtlinie verabschiedet worden. Die Terroranschläge in Brüssel im März 2016 hätten die Verabschiedung dieser Richtlinie erleichtert, obwohl klar sei, dass sie nicht zur Verhinderung der Attacken beigetragen hätte. Ihre Verabschiedung symbolisiere jedoch Handlungsfähigkeit. Die verschiedenen Regelungen demonstrierten, wie sowohl Terroranschläge als auch Normen zu unterschiedlichen Zeitpunkten im Entscheidungsprozess eine Rolle gespielt haben.

(Informelle) Massenüberwachung durch Nachrichtendienste

Anna Daun sprach über nachrichtendienstliche Zusammenarbeit innerhalb der Europäischen Union und mit den USA und ging der Frage nach, ob sich ein gemeinsames Regime bildet. Regime hätten das Ziel, Kooperation zwischen Staaten in Teilbereichen der Politik zum gegenseitigen Nutzen zu fördern. Der Fokus des Vortrags lag auf den Prinzipien, Normen und Regeln, die Regimebildung ausmachen. Ein erstes Prinzip sei Reziprozität. Ein zweites Prinzip stellten Normen dar, wie der Verzicht auf Spionage (einschließlich Industriespionage) unter Freunden. Diese Norm werde aber nicht wirklich eingehalten. Weiterhin gebe es standardisierte Abläufe der Kooperation, wie regelmäßige Besuche von Regierungs- und Behördenvertretern bei anderen Nachrichtendiensten.

Die Tiefe der Kooperation reiche vom Austausch von Informationen bis hin zu gemeinsamen Operationen. Beispielsweise habe es deutsch-amerikanische Zusammenarbeit bei der Verhaftung der sogenannten Sauerland-Gruppe gegeben, einer Gruppe von Terroristen, die US-amerikanische Einrichtungen in Deutschland attackieren wollte. Hier lieferten die US-amerikanischen Sicherheitsdienste Informationen an deutsche Behörden und letztere führten den Zugriff aus. Das Regime der nachrichtendienstlichen Kooperation sei sowohl effektiv als auch widerstandsfähig, das heißt, es bringe Ergebnisse und bleibe trotz externer Herausforderungen bestehen.

Ben Wagner und *Kilian Vieth* konzentrierten sich in ihrem Vortrag auf den Austausch von Informationen und Daten zwischen Nachrichtendiensten innerhalb der Europäischen Union sowie die diesem zugrunde liegenden Regeln. Viele Nachrichtendienste kooperierten (horizontal) direkt miteinander und nicht über die EU-Ebene. Ein Grund dafür sei, dass die Europäische Union zum Teil strengere Regeln beim Datenschutz habe als ihre Mitgliedstaaten. Nachrichtendienste suchten gezielt nach Lücken in der Gesetzgebung und nutzten die Möglichkeiten der Kooperation, die am wenigsten Datenschutz und Kontrolle beinhalten. Ein Beispiel für ein informelles Arrangement von Nachrichtendiensten stelle das Five-Eye-Abkommen von Australien, Großbritannien, Kanada, Neuseeland und den USA dar, über dessen Regeln wenig bekannt sei. Es sei ein Beispiel für ein altes Netzwerk, die anglophone Welt.

Diese Netzwerke reflektierten die Macht des Informellen und seien häufig als eine flexible Antwort auf zum Entstehungszeitpunt drängende Probleme entstanden. Weil in der Wahrnehmung der Akteure innerhalb des nationalen Rechtsstaates keine Möglichkeit bestehe, diese Probleme zu lösen, griffen die Nachrichtendienste auf informelle Absprachen zurück.

Auch die „EU Internet Referral Unit“ (IRU) bei Europol sei ein weiteres Beispiel für eine

informelle Zusammenarbeit. Es gehe um die Überwachung, Identifikation und Analyse von illegalen, extremistischen oder terroristischen Inhalten im Internet (in erster Linie nachrichtendienstliche Aufgaben) sowie um polizeiliche Funktionen, wie die Abschaltung von Internetseiten. Hier habe Europol zuerst Aufgaben übernommen und erst später sei die rechtliche Grundlage dafür geschaffen worden. Für die Forschung bestehe die Herausforderung schließlich darin, die informelle Zusammenarbeit der Nachrichtendienste zu verstehen und zu erfassen, wie diese formale Strukturen beeinflusse.

Konstantin von Notz berichtete über die Kooperation deutscher Nachrichtendienste mit US-amerikanischen. Er sagte, dass die Zusammenarbeit der National Security Agency (NSA) mit dem Bundesnachrichtendienst illegal gewesen ist. Diese Zusammenarbeit betreffend seien wichtige Überwachungsorgane des Bundestags, wie das Parlamentarische Kontrollgremium zur Überwachung der Nachrichtendienste und die G10-Kommission zur Genehmigung von Maßnahmen zur Überwachung von Kommunikation durch die deutschen Nachrichtendienste, von der Bundesregierung belogen worden und hätten keine ausreichenden Informationen für ihre Arbeit erhalten.

Bündnis 90/Die Grünen setzten sich für eine europäische und internationale Regulierung der Sammlung und des Austausches von Daten ein. Deutschland müsse aber seiner Verantwortung gerecht werden und die nationalen Kontrollgremien stärken. Beschränkungen der Massenüberwachung müssten eingeführt werden, wie der Europäische Gerichtshof und das Bundesverfassungsgericht in aktuellen Urteilen zur EU-Datenschutzrichtlinie und zum Bundeskriminalamtsgesetz entschieden hätten.

Über den Umgang mit neuen Formen der Kontrolle und Überwachung in Europa

Inès Gallala referierte über die Nutzung einer gemeinsamen DNA-Datenbank durch europäische Staaten, wie sie der Vertrag von Prüm vorsieht und von Polizei und Strafverfolgungsbehörden genutzt werden soll. Hierbei handele es sich um ein dezentrales Modell begrenzt auf den Schengen-Raum, wobei die Mitgliedstaaten den Zugriff der jeweiligen Partner auf die eigene Datenbank ermöglichen. Neben DNA-Daten betrifft dies insbesondere Fingerabdrücke und Daten zu Kraftfahrzeugen und deren Haltern.

Mit Europol wurde, entgegen der Strategie der dezentralen Vernetzung beziehungsweise Zugriffsberechtigungen bei Datenbanken, eine Institution geschaffen, die zentralisiert ist und Kompetenzen bündelt. Mit Blick auf die von Gallala dargestellten Implementationsprobleme beim Vertrag von Prüm, insbesondere bei den DNA-Datenbanken, stellte sie die Frage, wie handlungs- und kosteneffizient eine solche Lösung ist. Das dezentrale Modell sei in jedem Fall die am schnellsten umzusetzende Lösung.

Mathias Bug erörterte in seinem Vortrag die Akzeptanz von Kontrolle und Überwachung innerhalb der EU-Staaten. Die gesellschaftliche Akzeptanz von Überwachung folge den drei Kategorien von Legitimation (Renate Mayntz): der rechtlichen, der demokratischen und der sozialen. Um die Frage nach der sozialen Akzeptanz zu beantworten, zog Bug verschiedene Studien heran, die sich dem Thema auf unterschiedlichen Wegen näherten. Neben dem Mediendiskurs (indirekte Messung) waren vor allem verschiedene Befragungen (direkte Messung) Teil seiner Untersuchung. Da es sich um unterschiedliche Studien (beispielsweise das Eurobarometer) oder Befragungswellen handelte, würden sich zahlreiche Schwierigkeiten ergeben, da Trends aufgrund von Formulierungsunterschieden beziehungsweise Schwerpunktsetzungen nur schwer feststellbar seien.

Auch wenn die Frage der Akzeptanz in der Bevölkerung nicht eindeutig zu beantworten sei, so ließen sich zumindest einige Aussagen treffen. Obwohl nicht allen Unionsbürgern

die Datensammlung verschiedener Behörden bewusst sei und deren Wahrnehmung in den unterschiedlichen Ländern durch die Skandale (Snowden, WikiLeaks) geprägt sei, stimme die Mehrheit der Bevölkerung der Europäischen Union den Überwachungsmaßnahmen zu. Dass zunehmend persönliche Daten online abgefragt werden, während eine große Mehrheit immer noch das Gefühl habe, Kontrolle über die eigenen Daten zu besitzen, bezeichnete Bug als „digitales Dilemma". Das Vertrauen, insbesondere in die Polizei, die bei Sicherheitsfragen als wichtiger Partner angesehen wird, sei besonders hoch. Als Konsequenz der zunehmenden Überwachung habe das Wissen um Restriktionen in Zusammenhang mit den Grundrechten zugenommen. Es vollziehe sich, so Bug, eine Kosten-Nutzen-Abwägung in Bezug auf die Akzeptanz von Überwachung.

Raphael Bossong thematisierte im Rahmen seines Beitrags den immer stärkeren Einfluss von privaten Akteuren auf dem „Überwachungsmarkt". Beim Thema Cybersecurity spielten insbesondere in den USA privatwirtschaftliche Akteure bei der Erledigung einst staatlicher Aufgaben bereits heute eine sehr große Rolle. Beispielhaft zeigten dies der Fall Snowden und die Kooperation von Central Intelligence Agency (CIA) sowie NSA mit IT-Unternehmen, die Lösungen im Rahmen von Big Data anbieten. Zwar seien diese Public-Private-Partnerships (PPP) zumeist ökonomisch sehr effizient, aber auch mit enormen Risiken verbunden, was der Fall Snowden einmal mehr verdeutliche. Auffällig im Bereich Cybersecurity sei, so Bossong, dass eine Zusammenarbeit nicht mehr wirklich stattfinde, sondern eine vollkommene Privatisierung von Aufgaben eingesetzt habe, während sich staatliches Handeln vornehmlich auf die Regulierung konzentriere. Mit Blick auf die Kooperation von Unternehmen wie Microsoft und Kaspersky mit Sicherheitsbehörden wie der US-amerikanischen Bundespolizei FBI[1] oder die Kooperation bei der Entfernung von Inhalten aus sozialen Netzwerken existiere diese Zusammenarbeit aber noch immer.

Technologische Eigenständigkeit – eine europäische Antwort auf internationale Abhängigkeiten?

Jan-Peter Kleinhans widmete sich in seinem Beitrag dem Zugriff auf Daten, die nicht auf Servern innerhalb der eigenen Landesgrenzen liegen. Beispielhaft verwies er auf Konzerne wie Google oder Facebook, die zum Teil für die Strafverfolgung notwendige Daten speicherten. Während bis dato, so die Beschreibung Kleinhans', mehr als ein Jahr vergehen würde, bis eine Kette von deutschen und anschließend ausländischen, vornehmlich US-amerikanischen, Behörden darüber entscheidet, in welcher Form ein Zugriff auf Daten möglich ist, sind im Falle von Meta-Daten US-amerikanische Firmen (beispielsweise Cloud-Anbieter) frei, Daten zur Verfügung zu stellen.

Rüdiger Weis stellte in seinem Beitrag die Frage, ob Kryptografie und Open Source sinnvolle und effektive Strategien zum Schutz vor Überwachung seien. Zunächst konstatierte er, dass verschiedene Regierungen gewollt oder ungewollt dabei versagt hätten, die Daten ihrer Bürger zu schützen. Kryptografie, also die Verschlüsselung von Informationen vor allem im Internet, so Weis, sei ein effektives Mittel zum Schutz vor ausländischen Geheimdiensten, da der Entschlüsselungsaufwand sehr hoch sei. Dies gelte auch für zahlreiche Hacker, die im selben Maße wie staatliche Institutionen in der Lage seien, Informationen zu sammeln.

Dadurch dass kommerzielle Anbieter in ihren Software-Produkten oftmals Hintertüren programmierten, die die Anfälligkeit von Systemen erhöhen, böten, so Weis, Open-Source-Lösungen, bei denen sämtliche Codes öffentlich sind und durch die User verbessert werden könnten, besseren Schutz.

1 Federal Bureau of Investigation.

Fritz Sack nutzte seinen Vortrag, um die Diskussion über den Umgang mit neuen und älteren Formen der Überwachung in den Kontext der kritischen Kriminologie einzuordnen. Er verwies auf deren Anfänge, in der die aktuellen Formen der Kontrolle und Überwachung noch nicht vorhanden waren. Ansätze der kritischen Kriminologie würden allerdings zahlreiche Möglichkeiten bieten, eine Auseinandersetzung mit aktuellen Themen zu suchen. Mit dem Blick auf das Schwinden von Privatheit würde die präventive Wirkung des Nichtwissens ausgehebelt. Die Strafverfolgungsbehörden würden somit zum Hauptprofiteur der von der Europäischen Union initiierten Überwachung. Big Data und ‚predictive policing' würden zu einer Vorverlagerung der Ermittlungen führen. Whistleblowing über Form und Ausmaß der gemachten Datensammlung, so Sack abschließend, wäre die einzig funktionale Möglichkeit, um die Gefahren der Massenüberwachung aufzuzeigen.