Erkenntnisse aus dem Werkstattgespräch "Telekommunikationsüberwachung und Datenabfrage durch staatliche Behörden bei Unternehmen" vom 1. Juli 2014

Am 1. Juli 2014 veranstalteten das Walter Hallstein-Institut für europäisches Verfassungsrecht (WHI) der Humboldt-Universität zu Berlin, das Kompetenznetzwerk für das Recht der zivilen Sicherheit in Europa (KORSE) am Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG) und das "Privacy Project" der stiftung neue verantwortung das dritte Werkstattgespräch in einer Reihe. Diskutiert wurde zum Thema „Telekommunikationsüberwachung und Datenabfrage durch staatliche Behörden bei Unternehmen."

An den Diskussionen beteiligten sich rund 25 Teilnehmerinnen und Teilnehmer, darunter Expertinnen und Experten des (europäischen) Verfassungsrechts und des IT-Rechts aus Wissenschaft, Politik und Wirtschaft. Vertreterinnen und Vertreter deutscher und internationaler Telekommunikationsunternehmen teilten ihre Expertise zum Thema Datenzugriffe bei privaten Unternehmen durch Polizei und Geheimdienste.

Die erste Sitzung des Werkstattgespräches befasste sich mit Telekommunikationsüberwachung, Datenabfrage und der erforderlichen Transparenz darüber in Deutschland. Frau Haya Hadidi, Leiterin des Referats Automatisiertes Auskunftsverfahren und PTSG [1] der Bundesnetzagentur, gab hier einen einleitenden Impuls.

Die zweite Sitzung behandelte die transnationalen Aspekte des Themas. Einleitende Impulse durch Frau Dorothee Belz von Microsoft Europe und Herrn Wolfgang Kopf der Deutschen Telekom AG beleuchteten die Schwierigkeiten unterschiedlicher und teils widersprüchlicher Regelungen verschiedener Staaten zur Kooperation mit Sicherheitsbehörden und des Datenschutzes für international agierende Unternehmen.

Im Folgenden sind einige der Erkenntnisse, offenen Fragen und angesprochenen Problematiken aufgelistet.

Session I: Transparenzberichte und Telekommunikationsüberwachung

- Deutsche Behörden veröffentlichen weder umfassende noch detaillierte Berichte zur Telekommunikationsüberwachung (TKÜ) und Datenabfragen bei privaten Unternehmen. Von staatlicher Seite ist lediglich das Bundesjustizministerium gesetzlich verpflichtet, jähr-

[1] Gesetz zur Sicherstellung von Postdienstleistungen und Telekommunikationsdiensten in besonderen Fällen, http://www.gesetze-im-internet.de/ptsg_2011/BJNR050610011.html (abgerufen 27. Juli 2014)

lich Statistiken zu den Anordnungen nach § 100a und § 100g StPO zu veröffentlichen.[2] Über viele andere, teils stark invasive, Überwachungsmaßnahmen wird nicht gesondert berichtet. Hierunter fallen z.B. Funkzellenabfragen, „Stille SMS“ und der Einsatz von IMSI-Catchern.[3] Die von der Bundesnetzagentur in ihrem Jahresbericht veröffentlichten Statistiken zum „Automatisierten Auskunftsverfahren“ (§112 TKG) sind „freiwillig“.[4]

- Da es an klaren rechtlichen Grundlagen fehlt, haben private Unternehmen keine Rechtssicherheit hinsichtlich der Erforderlichkeit und des Inhalts der Transparenzberichte.[5]
- Von Seiten der Behörden werde teilweise argumentiert, dass hohe Transparenz in Bezug auf staatliche Ermittlungsmaßnahmen (Cyber-)Kriminellen ermögliche, Lücken dieser Methoden auszumachen und anschließend auszunutzen. So gehe der Abschreckungseffekt, den die Unsicherheit über die technischen Möglichkeiten der Behörden für Kriminelle mit sich bringe, verloren. Daher brauche man „Security by Obscurity“. Dagegen wurde vorgebracht, dass „Security by Obscurity“ nicht im Einklang mit der Verfassung und dem demokratischen Rechtsstaat stehe. Überwachung diene keinem Selbstzweck, sondern dem Schutz der Bürger. Unsicherheit bzgl. TKÜ-Maßnahmen schrecke jedoch nicht nur Kriminelle ab. Vielmehr halte sie auch die Bürger ab, von ihren Kommunikationsgrundrechten Gebrauch zu machen. Es sei daher ein gesellschaftlicher Diskurs über die Notwendigkeit und die Reichweite der (praktizierten) Überwachungsmaßnahmen zu führen.
- Das Automatisierte Auskunftsverfahren:
  - Das System zum Automatisierten Auskunftsverfahren besteht zwar seit 1999, wurde dennoch bis dato nicht vollständig umgesetzt. Drei Arten von Daten (vgl. aber §111 Abs. 1 Satz 1-6 TKG) können grundsätzlich abgerufen werden: Rufnummer, Name und Anschrift. Noch nicht abrufbar aufgrund technischer Limitationen sind etwa Geburtsdatum und Gerätenummer (IMEI).
  - Rund 250 Sicherheitsbehörden und Notrufleitstellen sowie 140 Unternehmen sind derzeit an das System zum Automatisierten Auskunftsverfahren angeschlossen. 2013 wurden sieben Millionen Anfragen gestellt, die zu 36 Millionen Auskünften führten. (Dass eine Anfrage zu mehreren Auskünften führen kann, beruhe darauf, dass eine verdächtigte Person u.U. mehrere Anschlüsse bei verschiedenen Anbietern haben kann. So gebe es bspw. in Deutschland mittlerweile über 150 Mio. angemeldete SIM-Karten.)
  - Die Bundesnetzagentur prüft weder den Zweck der Abfrage noch, ob und wie diese von den abfragenden Stellen gespeichert oder gelöscht werden.
  - Die Protokolldaten der Anfragen werden zu Datenschutzzwecken für ein Jahr durch die BNetzA doppelt verschlüsselt abgespeichert. Dabei ist ein Schlüssel bei der

---

[2] https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung_node.html (abgerufen 27. Juli 2014).

[3] http://privacy-project.net/cms/assets/uploads/2014/06/Nr.1_PP-White-Paper-JPKleinhans.pdf (abgerufen 27. Juli 2014).

[4] http://www.bundesnetzagentur.de/DE/Allgemeines/DieBundesnetzagentur/Publikationen/Berichte/berichte-node.html (abgerufen 27. Juli 2014).

[5] https://posteo.de/Gutachten_Transparenzbericht.pdf (abgerufen 27. Juli 2014).

BNetzA, der andere beim Bundesbeauftragten für Datenschutz und die Informationsfreiheit (BfDI) hinterlegt. Zur Prävention von Missbrauch werden die Protokolldaten mittels eines Vier-Augen-Prinzips durch BNetzA und BfDI einige Male im Jahr überprüft. In der Diskussion wurde bezweifelt, dass dies – angesichts von sieben Mio. Abfragen pro Jahr – eine adäquate Kontrolle darstelle.

- Zum Automatisierten Auskunftsverfahren wurde abschließend angemerkt, dass dieses Verfahren letztlich nicht der sensibelste Bereich sei. Die eigentliche Gefahr gehe von der Datenmacht der Unternehmen aus, die durch "Apps" auf dem Smartphone unbemerkt große Mengen an persönlichen Informationen „absaugen".

- Hinsichtlich der TKÜ sei ein „Going Dark Effect" [6] zu beobachten. Kommunikation finde zunehmend über „Telemediendienste" wie Facebook, Twitter, etc. oder in der Cloud statt und/oder werde verschlüsselt. Diese Medien seien durch klassische TKÜ nicht überwachbar. Auch zu der Frage, ob und wie diese Telemediendienste überwacht werden müssten, sei eine gesellschaftliche Debatte notwendig.

- Da Informationen und Kommunikation zu einem großen Teil über IP-Netze [7] übertragen werden ("data" statt "voice") sei insgesamt fraglich, ob die derzeitigen Gesetze zur TKÜ und Datenabfrage noch die technische Realität abbildeten und ob sie für den Bürger noch verständlich und nachvollziehbar seien. Um diese Dienste gleichermaßen zu überwachen wie herkömmliche Telekommunikationsdienste müsse die TKÜV überarbeitet und eine Rechtsgrundlage geschaffen werden. Das zuständige BMWi warte zur Zeit jedoch ab.

- Cyber-Kriminalität bedrohe immer stärker das Internet der Dinge, wozu etwa allgemein "kritische Infrastrukturen" gehören können, aber auch Steuerungssysteme von Energie- und Gesundheitssystemen sowie vernetzte Autos. In diesem Bereich sei ebenfalls keine TKÜ sei möglich. Im gesellschaftlichen Diskurs sei insofern zu klären, wie und durch wen diese Systeme geschützt werden sollten und wem die Verantwortung für eventuelle Schäden zugerechnet werden könnte. Mit Blick auf die USA wurde auf die Bedeutung und Auswirkungen der Network Security Agreements [8] hingewiesen. Diese sollen US Behörden (auch ohne Gesetz) ungehinderten Zugang zu US-amerikanischen Providernetzen ermöglichen.

Session II: Nach den Microsoft- und Google-Urteilen – welches Recht gilt für wen, und wenn ja, wo?

- Es sei zu bedenken, dass die USA und Deutschland – zwei souveräne Staaten – jeweils eigene, voneinander abweichende Entscheidungen zur Ausgestaltung des Spannungsverhältnisses zwischen Sicherheit (durch TKÜ und Datenabfrage) und individueller Freiheit getroffen hätten. Diese Entscheidungen seien grundsätzlich zu respektieren. Nunmehr führe das Internet als globales Netzwerk jedoch dazu, dass die Territorialität der an sich

[6] http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies (abgerufen 27. Juli 2014).
[7] http://www.itwissen.info/definition/lexikon/IP-Netz-IP-network.html (abgerufen 27. Juli 2014).
[8] https://publicintelligence.net/us-nsas/ (abgerufen 27. Juli 2014).

souveränen Staaten im Hinblick auf die (Kommunikations-)Übertragung aufgehoben werde und so die abweichenden Rechtsverständnisse kollidierten.

- Global agierende Unternehmen sehen sich konfligierenden Rechtsvorschriften ausgesetzt. Sie stecken in einem Dilemma, da die Erfüllung der gesetzlichen Vorschriften in einem Staat zum Verstoß gegen Normen eines anderen Staates führen. [9]
- Private Unternehmen sehen sich mangels übergeordneter internationaler Regelungen bzw. Instanzen gezwungen, einen internationalen Rechtskonflikt selbst zu entscheiden. Unternehmen legen folglich eigenständig fest, mit welchen (vermeintlich) guten Sicherheitsbehörden sie kooperieren und mit welchen nicht. Dabei würden sie im Zweifelsfall nach einer pragmatischen kommerziellen Lösung suchen, um in allen Märkten erfolgreich zu sein. Diese Verortung derartiger Entscheidungsmacht bei privaten Unternehmen wurde als sehr diskussionswürdig erachtet.
- Zur Strafverfolgung solle grundsätzlich das Mittel des Rechtshilfeverfahrens (MLAT) genutzt werden. Dieses Verfahren sei jedoch sehr langwierig. Daher versuchten Sicherheitsbehörden direkt beim Diensteanbieter auf die Nutzerdaten zuzugreifen.
- In diesem Zusammenhang wurde auch auf das laufende Verfahren von Microsoft in den USA hingewiesen. In erster Instanz hatte der „magistrate judge“ eines New York District Court entschieden[10], dass Microsoft mit Sitz in den USA auch solche Daten, die auf einem ausländischen Server (hier: Irland) gespeichert seien, an unmittelbar die US Behörden herausgeben müsse. Ein Rechtshilfeverfahren sei zu langwierig und eigne sich daher nicht für die Strafverfolgung.
- Nationales Routing müsse nicht im Widerspruch zu einem freien und offenen Internet stehen, da nur der Verkehr, der ohnehin für den inländischen Verkehr bestimmt ist, auch im jeweiligen Land bleibe. Ausländischer Datenverkehr bleibe möglich.
  Der US-amerikanische Datenverkehr werde seit 15 Jahren innerhalb der USA geroutet.
- Diskutiert wurde, ob nach der Festschreibung des Marktortprinzips im Google-Urteil des EuGH das Safe Harbor Abkommen noch Bestand haben könne.
- Es wurde angemerkt, dass im ersten Entwurf der Europäischen Datenschutzgrundverordnung[11] durch Art. 41 eine Klausel zur Beschränkung der Übermittlung personenbezogener Daten kurzfristig enthalten war. Durch intensives "Lobbying" wurde dieser Artikel zunächst entfernt und später wieder in den Entwurf aufgenommen.

[9] http://www.vergabeblog.de/2014-07-01/spy-erlass-des-bundesinnenministeriums/ (abgerufen 27. Juli 2014).
[10] https://www.eff.org/document/microsofts-objection-magistrates-opinion (abgerufen 27. Juli 2014).
[11] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf (abgerufen 27. Juli 2014).

Teilnehmerinnen und Teilnehmer

Ingolf Pernice
Direktor des Walter Hallstein-Instituts und des Humboldt Instituts für Internet und Gesellschaft
Markus Löning
stiftung neue verantwortung, Direktor des Privacy Projects

Dorothee Belz
Microsoft Europe, Vice President Legal and Corporate Affairs
Haya Hadidi
Bundesnetzagentur, Referatsleiterin Automatisiertes Auskunftsverfahren und PTSG
Wolfgang Kopf
Deutschen Telekom AG, Leiter Politik und Regulierung

Annegret Bendiek
Stiftung Wissenschaft und Politik, stellv. Forschungsgruppenleiterin EU-Außenbeziehungen
Ansgar Baums
Hewlett Packard, Government Relations Germany
Ben Scott
stiftung neue verantwortung, Direktor Europäische Digitale Agenda
Claus Schaale
Cisco Systems, Cloud Computing Business Development
Emma Peters
Humboldt Institut für Internet und Gesellschaft, Doktorandin
Hannfried Leisterer
Humboldt Institut für Internet und Gesellschaft, Doktorand
Hansjörg Geiger
ehem. Präsident des Bundesverfassungsschutzes und des BND, ehem. Staatssekretär im BMJ
Jan-Peter Kleinhans
stiftung neue verantwortung, Projektmanager Privacy Project
Jenny Paschen
Vodafone Deutschland
Julian Staben
Humboldt Institut für Internet und Gesellschaft, Doktorand
Matthias Bergt
von Boetticher Rechtsanwälte
Pascal Schumacher
Noerr Rechtsanwälte
Patrik Löhr
Posteo.de, Geschäftsführer
Simon Rinas
Humboldt Institut für Internet und Gesellschaft, Doktorand
Stefan Heumann
stiftung neue verantwortung, stellv. Direktor Europäische Digitale Agenda
Susanne Dehmel
BITKOM, Bereichsleiterin Datenschutz
Tim Klaws
Telefonica, Senior Government Relations Manager
Tobias Frevert
Noerr Rechtsanwälte, Head of Telecommunications