

lich (zumindest teilweise), viele andere tun das nicht. Die Waffen sind vergleichsweise billig und leicht zu bauen; das führt zu einer Rüstungsspirale. Durch internationale Verträge wird heute auf biologische und chemische Waffen verzichtet; dieser Versuch sollte auch auf andere Bereiche übertragen gemacht werden.

- Das Problem am autonomen Waffensystem ist, nicht dass es für Informatiker:innen wichtig, sich klar zu machen, was sie in ihrer Arbeit tun. Die Informatik darf als Disziplin nicht missbraucht werden.
- Es ist eine neue Qualität autonomer Systeme, dass sie sich verselbständigen und autonom weiterentwickeln können;

erschieden in der Fiff-Kommunikation,  
herausgegeben von Fiff e.V. - ISSN 0938-3476  
www.fiff.de

evtl. können sie im Gegensatz zu normalen Waffen auch nicht mehr deaktiviert werden. Zumindest die Energie kann ihnen jedoch entzogen werden; es ist skeptisch zu beurteilen, ob solche Systeme wirklich im menschlichen Sinne intel-

llectuell sind. Die Entscheidungen irgendwann nicht mehr klar ist, ob der Mensch die Kontrolle hat oder die Maschine.

- Programmierer sind verantwortlich für die von ihnen produzierten Systeme. Doch auch diejenigen tragen eine Verantwortung für die Folgen, die unbegründete Theorien von der Möglichkeit einer Maschinenethik in die Welt setzen.



## Fiff-Konferenz 2016

# Die neue Globalisierung – wenn das Inland zum Ausland wird

## Zusammenfassung des Vortrags von Klaus Landefeld

Was hat die Klage gegen den BND wegen Überwachung am Internetknoten DE-CIX mit der BND-Reform nach dem Beschluss zur Ausland-Ausland-Fermeldeaufklärung zu tun? Sehr, sehr viel – darum ging es im Beitrag von Klaus Landefeld.

Klaus Landefeld leitete seinen Vortrag mit einem Zitat des Bundesverfassungsgerichts ein, in dem es deutlich machte, dass Überwachung nicht in Einklang zu bringen ist mit der verfassungsrechtlichen Identität der Bundesrepublik Deutschland:

*„Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss.“ (BVerfG, 2010)*

Ähnlich sieht es der Europäische Gerichtshof (EuGH); er betont:

*„Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert werden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren.“ (EuGH, 2014)*

Anders sieht es Bundesinnenminister Thomas de Maizière:

*„Es ist nicht Aufgabe des Gerichts, ständig dem Gesetzgeber in Sachen Sicherheit in den Arm zu fallen.“ (Bundesinnenminister Thomas de Maizière, 2016)*

Landefeld unterschied zwischen zwei Kategorien der Fernmeldeüberwachung: Gezielte behördliche Maßnahmen, die unmittelbar auf einzelne Personen zielen, und ungezielte Maßnahmen, die die übergreifende strategische Überwachung zum Ziel haben. Zur ersten Kategorie zählt er anbietergestützte Maßnah-

men nach § 110ff. TKG – Quellen-TKÜ, Vorratsdatenspeicherung, Funkzellenabfrage, Bestandsdatenauskunft und Online-Durchsuchung; Maßnahmen im Rahmen des G10-Gesetzes im Inland. Zu den strategischen Maßnahmen zählen die Maßnahmen nach G10-Gesetz mit Auslandsbezug (§ 5 G10-Gesetz): z.B. Ausland-Ausland-Fermeldeüberwachung und Überwachung durch den Verfassungsschutz, um „Cyberbedrohungen“ im Inland zu erkennen.



Klaus Landefeld

Seit den Enthüllungen durch Edward Snowden wurden die Überwachungsbefugnisse durch mehrere Gesetzesinitiativen systematisch ausgeweitet:

- Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 20.11.2015

- Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10.12.2015
- Gesetz zur Ausland-Ausland-Fernmeldeaufklärung vom 21.10.2016

Aus Sicht der Sicherheitsbehörden ist diese Ausweitung der Überwachung erforderlich, um den aktuellen Gefahren zu begegnen: Es gibt heute nur unzureichende Maßnahmen gegen globalen Terrorismus und *Cyber Threats*; die Diskrepanz zwischen Sicherheitsbehörden und Geheimdiensten, die ersteren nicht erlaubt, strategische Überwachungsmaßnahmen durchzuführen, muss überwunden werden. Als ein zunehmendes Problem sei die Tendenz zum „going dark“ anzusehen, d. h. die Geräte- und Dienstverschlüsselung durch Internet-Nutzer. Zuletzt sei auch eine systematische Verkehrsdatenerfassung notwendig, um Beziehungen zwischen Gefährdern darzustellen.

## Überwachung global und in Deutschland

Massenerhebung und Filterung haben sich zu einem globalen Trend entwickelt. Sicherheitsbehörden wollen systematischen Zugang („bulk access“) zu Daten erhalten, um diese systematisch auswerten zu können. Dies umfasst sowohl Verkehrsdaten, den Inhalt der Kommunikation und auch private Datensammlungen aus Social Networks und Daten zu persönlichen Interessen, z. B. aus Suchmaschinen. Überwachung und Datenspeicherung erfolgen anlasslos, dabei werden unterschiedliche Formen von Spionagesoftware eingesetzt (Trojaner, Malware, Spyware). In Deutschland dagegen ist die Überwachung nach G10-Gesetz bisher nur in relativ engem Rahmen zulässig. Überwacht werden dürfen nur Leitungen mit Auslandsbezug; dabei gilt eine Begrenzung auf 20 % der Leitungskapazität. Zielgebiet und Suchbegriffe müssen im Antrag genannt werden; die Genehmigung muss alle drei Monate überprüft werden.

Das Aufgabenprofil des BND sieht Folgendes vor:

*Die grundsätzliche Aufgabe des Bundesnachrichtendienstes ist es, seine Abnehmer zur richtigen Zeit bedarfsgerecht mit belastbaren Informationen umfassend zu versorgen. Als Dienstleister für Bundesregierung, Ressorts und auch Bundeswehr umfasst dies Informationen zu*

- *wichtigen politischen, wirtschaftlichen aber auch technischen Entwicklungen,*
- *militärischen Fragestellungen und*
- *abstrakten oder konkreten Bedrohungen für die Sicherheit der Bundesrepublik Deutschland und ihrer Bürger.*

Derzeitige prioritäre thematische Aufklärungsziele des BND sind Proliferation, internationaler Terrorismus, Zerfall von Staaten und Auseinandersetzungen um Ressourcen. Aktuelle regionale Aufklärungsziele mit höchster Priorität sind der nahe und mittlere Osten, Nordafrika, West- und Zentralasien.

Der BND darf nur im Ausland tätig werden. Dieser Rechtsrahmen wird dabei vom BND aber sehr frei interpretiert: Satellitenüber-

wachung wird generell als „Ausland“ angesehen (Prinzip des „freien Himmels“). Dabei argumentiert der BND, die Erfassung erfolge ausschließlich am Satellit, nur die Speicherung und Auswertung erfolge im Inland (in Bad Aibling). Filter zur Sicherstellung des Grundrechtsschutzes seien notwendig (wegen Art. 10 GG); alle weiteren Daten könne der BND frei verwenden.

Diese Interpretation führt dazu, dass auch der Netzknoten DE-CIX in Frankfurt am Main als „virtuelles Ausland“ aufgefasst wird: DE-CIX sei ein „internationaler Netzknoten“, an dem Carrier aus vielen Ländern aufeinanderträfen. Damit sei Auslandsbezug für alle Leitungen gegeben. Die Ausleitung erfolge auf Basis einer G10-Anordnung. Dabei sei wiederum ein G10-Filter erforderlich, weitere Daten seien frei verwendbar.

DE-CIX äußerte bereits 2009 Bedenken:

- das G10-Gesetz sei nicht ohne weiteres auf paketorientierte Kommunikation anwendbar, da es keinen Leitungsbezug gäbe,
- es ist unklar, ob die Leitungskapazität oder der Verkehr für die Ermittlung der 20 % maßgeblich sind,
- der Transport erfolge von Router zu Router innerhalb Frankfurts, ein Auslandsbezug sei daraus nicht erkennbar,
- die Abgrenzung der Carrier in national/international sei schwierig,
- die Zwischenspeicherung aller Verkehre sei notwendig,
- die trennscharfe Filterung zur Sicherstellung von Art. 10 sei nicht möglich.

Das Kanzleramt sicherte dagegen zu, dass alles innerhalb des zulässigen Rechtsrahmens stattfinden würde.

Anders ist die Sichtweise des NSA-Untersuchungsausschusses:

- im Gegensatz zur Rechtsauffassung des BND gilt der Grundrechtsschutz auch für Ausländer,
- das Konzept des „freien Himmels“ ist nicht haltbar,
- das Programm DAFIS, das die Filterung inländischer Personen zur Sicherstellung von Art. 10 GG leisten soll, ist äußerst rudimentär, weniger effektiv als zunächst erwartet,
- nicht als G10-Verkehre markierte Daten werden mit anderen Geheimdiensten getauscht,
- wie sich herausstellt, empfindet auch die G10-Kommission das „Vorgehen als unredlich“, da G10-Anordnungen dafür verwendet werden, Daten zu erlangen, für die es keine Gesetzesgrundlage gibt.

Dies hat DE-CIX dazu bewogen, gegen die Überwachungsmaßnahmen zu klagen. Basis dafür ist ein Gutachten des früheren Verfassungsrichters H. J. Papier, in dem er zu folgenden Ergebnissen kommt:

- Art. 10 ist Menschenrecht, kein „Deutschenrecht“, und gilt für alle Menschen, unabhängig von der Nationalität,
- die Regeln der Verfassung gelten bereits immer dann, wenn ein deutscher Dienst tätig ist,
- der Grundrechtsschutz bei der Tätigkeit eines deutschen Dienstes im Inland steht außer Frage,
- im Ergebnis sind die Anordnungen insgesamt unzulässig.

Damit werden sämtliche Bedenken des DE-CIX aus 2009 bestätigt; die gerichtliche Klärung der Zulässigkeit zwingend erforderlich. Deswegen wird Klage vor dem Bundesverwaltungsgericht Leipzig geführt.

Das neue BND-Gesetz zur Ausland-Ausland-Fernmeldeaufklärung legalisiert dagegen die bestehenden Praktiken:

- Verfassungsrechtliche Fragen aus G10 werden durch das neue Gesetz nicht berührt,
- Kommunikation wird nach Kommunikation von Deutschen, EU-Bürgern und anderen Ausländern unterschieden,
- Datenweitergabe an Partnerdienste ist nach dem neuen Gesetz möglich,
- es wird eine neue Kontrollinstanz geschaffen – diese soll mehr Vorgänge bearbeiten, aber mit weniger inhaltlicher Tiefe.

Staatssekretär Klaus-Dieter Fritsche aus dem Bundeskanzleramt erklärte dazu:

*„Mit der Frage von Rechtssicherheit für die Angestellten des BND gegenüber der Rechtsstaatlichkeit für Bürger konfrontiert muss ich sagen, dass mich primär die Rechtssicherheit interessiert.“*

Selbst wenn man zugutehält, dass sich Fritsche in der Rolle des Arbeitgebers hinter seine Mitarbeiter stellt, ist diese Aussage für einen Staatssekretär sehr fragwürdig.

Inhaltlich regelt das Gesetz die Erhebungsgrundlage neu:

- Wegfall des Leitungsbezugs
- Wegfall der Kapazitätsschranken
- Einschränkung des Auslandsbezugs
- Verlängerung der Anordnungsdauer von 3 auf 9 Monate
- Erhebung im Inland ausdrücklich zulässig
- Umfang der Erhebung unterliegt keiner Kontrolle

Im Ergebnis ist die Erhebung nach dem neuen Gesetz ausschließlich durch die finanziellen Ressourcen des Dienstes beschränkt.

## Filterung

Der Grundrechtsschutz wird beim neuen Gesetz alleine durch das Filtersystem DAFIS sichergestellt. Bewertung, Filterung etc. erfolgen dabei vollständig im Kontrollbereich des BND. Das Filtersystem unterliegt keiner Kontrolle durch ein unabhängiges Gremium, wie z.B. das G10-Gremium oder das parlamentarische Kontrollgremium.

Darüber hinaus kann das Filtersystem für bis zu 6 Monate abgeschaltet werden, um die Verkehre zur „Eignungsprüfung“ zu analysieren, diese Anordnung unterliegt keiner externen Kontrolle.

Das Filtersystem DAFIS ist mehrstufig aufgebaut:

- IP-Filter zur Filterung nach Geo-Location
- Typfilter zur Filterung nach Dateitypen (http, smtp, video, chat etc.)
- Metadatenfilter zur Vorfilterung von Inhalten (z. B. E-Mail-Header, SIP)
- Inhaltsfilter (RTP, E-Mail, Kurznachricht etc.)

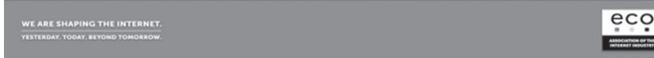
Einem Gutachten von eco zufolge beträgt die Qualität des Systems DAFIS geschätzt 98,5–99 % korrekter Filterung. Kommerzielle Filter leisten bis maximal 99,5 %. Analysen der Stufe 3 und 4 sind aus Sicht des DE-CIX bereits ein Grundrechtseingriff mit Notifizierungspflicht.

### Filter im Mengengerüst (Iudex non calculat)

- Verkehrsaufkommen DE-CIX
- 5,5 Tbps Peak -> 10,0 Mio Peak Flows/sec
- 3,4 Tbps Average -> 6,0 Mio Average Flows/sec
- ca. 500 Mrd. Verbindungen/Tag

Filterqualität 99,9% -> 0,5 Mrd. Verbindungen/Tag  
 Filterqualität 99,5% -> 2,5 Mrd. Verbindungen/Tag  
 Filterqualität 99,0% -> 5,0 Mrd. Verbindungen/Tag

Bei Kommunikationsanteil 20% und Beispielhaft 1% Erfassung  
 1 Mio. Verbindungen/Tag falsch analysiert – alleine am DE-CIX



Betrachtet man die Zahlen, so muss man am Knoten DE-CIX von einem Verkehrsaufkommen von 5,5 Tbps (10,0 Mio. Peak Flows/sec) in der Spitze und 3,4 Tbps im Schnitt (6,0 Mio. Average Flows/sec) ausgehen. Es gibt ca. 500.000.000.000 Verbindungen pro Tag.

## Klaus Landefeld

**Klaus Landefeld** ist Vorstand für Infrastruktur und Netze beim eco e. V., dem größten Verband der Internetwirtschaft in Europa. Er ist Beirat der DE-CIX Management GmbH, Betreiberin des weltgrößten Internetknotens. Darüber hinaus ist er selbständiger Unternehmer und Gründungsmitglied der DENIC eG, AMS-IX, MINX und weiteren IP-Exchanges weltweit. Er war geladener Sachverständiger im NSA-Untersuchungsausschuss des Bundestages.

- Bei einer Filterqualität von 99,9 % ergeben sich 0,5 Mrd. falsch zugeordnete Verbindungen/Tag.
- Bei einer Filterqualität von 99,5 % ergeben sich 2,5 Mrd. falsch zugeordnete Verbindungen/Tag.
- Bei einer Filterqualität von 99,0 % ergeben sich 5,0 Mrd. falsch zugeordnete Verbindungen/Tag.

D.h. bei einem Kommunikationsanteil von 20 % und beispielhaft 1 % Erfassung werden 1 Mio. Verbindungen/Tag falsch analysiert – alleine am DE-CIX –, d.h. es gibt pro Tag 1 Mio. Grundrechtsverstöße.

Bei einem Grundrechtseingriff muss der Betroffene informiert werden. Diese Information kann ausgesetzt werden; die Entscheidung darüber trifft die G10-Kommission. Eine Aussetzung ist alle drei Monate zu überprüfen – wie eine Einzelfallprüfung bei potenziell mehr als 100.000.000 Fällen erfolgen soll, bleibt offen. Der endgültige Verzicht auf Information ist nach fünf Jahren möglich; in diesem Zeitraum dürfen die Daten nicht gelöscht werden.

## Einordnung des Gesetzes

Der Gesetzgeber sieht das Gesetz positiv: Es werde kein Grundrecht eingeschränkt – mindestens wird im Gesetzentwurf kein eingeschränktes Grundrecht angegeben, was erforderlich wäre – und die Grenze für die Überwachung sei hinreichend bestimmt (durch das Budget des Bundesnachrichtendienstes). Nach Auffassung der Koalition ist es ein „sehr gutes Gesetz mit internationalem Beispielcharakter“.

Sachverständige haben eine andere Auffassung: der Wissenschaftliche Dienst des Deutschen Bundestags beurteilt das Gesetz sehr kritisch; auch unabhängige Sachverständige sehen es durchweg überaus kritisch. Beim Bundesverfassungsgericht sind erste Klagen anhängig, z.B. durch Amnesty International; weitere sind in Vorbereitung. DE-CIX wird bei Empfang der ersten Anordnung umgehend Klage beim BVerwG in Leipzig einreichen.



FIF-Konferenz 2016

## Un.Sichtbare Datenpraktiken?

### Big Data in Wirtschaft, Wissenschaft & Politik

#### Zusammenfassung des Vortrags von Judith Simon

*Die Proliferation von Big-Data-Praktiken ist ein relativ neues und komplexes Thema. Insbesondere die Intransparenz der verwendeten – häufig zudem proprietären – Systeme bereitet dabei Schwierigkeiten. Dabei muss man zwischen funktionaler Intransparenz („kein Zugriff“) und epistemischer Intransparenz („Schnelligkeit“, „Komplexität der Prozesse“, usw.) unterscheiden, um sinnvolle Desiderate für die Governance von Big Data ableiten zu können. Ein wesentlicher Teil solcher Governance-Bemühungen ist neben den rechtlichen Regelungen natürlich auch die transparenzförderliche Gestaltung der IT-Systeme (Stichwort: value-sensitive Design).*

#### Warum und in welcher Weise müssen wir uns mit Big Data beschäftigen?

Die meisten werden das folgende Beispiel kennen: 2012 ging durch die Medien die Geschichte eines US-amerikanischen Vaters, der sich bei der Supermarktkette Target beschwerte, weil er Werbematerial zu schwangerschaftsbezogenen Produkten zugesendet bekommen hatte. Schließlich stellte sich jedoch heraus, dass seine 16-jährige Tochter tatsächlich schwanger war und es ihm bis dahin verschwiegen hatte. Target wusste also mehr als der eigene Vater. Bei aller anfänglichen Empörung oder Überraschung über diesen Fall müssen wir jedoch kritisch fragen: Liegt hier überhaupt ein Problem vor? Wenn ja, wo, und wie kann man es konzeptuell fassen?

Der naheliegendste Ansatz sind die Punkte *Verletzung der Privatsphäre* und *illegitime Datensammlung* – durch die rechtlich legitime Praxis der *Informed-consent-Verfahren* (Einwilligung nach vorheriger Aufklärung) stimmen wir allerdings der Nutzung unserer Daten zu, sodass im Grunde rechtlich hier gar kein Problem vorliegt, denn auch die Tochter hat dem Sammeln und Auswerten ihrer Daten zugestimmt. Die Verletzung der Privatsphäre ist hier jedoch nicht auf Grund des Datensammelns pas-



Judith Simon

siert, sondern erst durch die Inferenzen, die auf Basis der Daten, d.h. der Verarbeitung der Daten und der Prognosen, gemacht wurden. Big-Data-Praktiken müssen also zunächst als epistemische, d.h. wissenschaftliche Praktiken betrachtet werden, die