Stefan Hügel

Weltweite Ausspähung der Bevölkerung: Rechtliche Bewertung und Handlungsoptionen

Zum dritten Mal wurde am 20. und 21. Juni 2014 in Rastatt das Gustav-Heinemann-Forum ausgerichtet, in dem sich die Humanistische Union den Defiziten unserer Verfassungsordnung widmet – seien sie national, europäisch oder international bedingt. In diesem Jahr befasste sich das Gustav-Heinemann-Forum mit einer besonders gravierenden Verletzung der freiheitlichen Verfassungsordnung: der von US-amerikanischen, europäischen und deutschen Geheimdiensten und weiteren Behörden seit dem zweiten Weltkrieg betriebenen Ausspähung und Überwachung der Bevölkerung.

In einer der drei Sessions war das FIfF umfassend vertreten: *Instrumente und Konsequenzen: Was ist heute technisch möglich? Worin besteht die Bedrohung? Ist die Technik heute noch demokratisch beherrschbar?* Die Praxis der Überwachung wird nicht nur von den (rechts-)politischen Vorgaben, sondern auch von der Entwicklung der Kommunikationstechnik geprägt. Mit den heutigen Möglichkeiten digitaler, vernetzter Kommunikation sind auch neue Möglichkeiten der Überwachung entstanden. Verstärkt wird dieser Trend dadurch, dass Menschen das Internet und seine Dienste jeden Tag nutzen – vielen ist es inzwischen zu einer Form von Lebenswelt geworden.

Damit stellt sich die Frage nach dem Grundrechtsschutz im Internet. In dem Panel sollten die technischen Möglichkeiten der Überwachung im Rahmen der technischen Entwicklung und ihre Auswirkungen auf die verfassungsmäßigen Rechte ausgelotet werden. Es ging dabei um Veränderungen wie vernetzte Datenbanken mit den Möglichkeiten der Verknüpfung, Datenanalysetechniken, die unter dem Stichwort *Big Data* diskutiert werden, Sensoren, die im „Internet der Dinge" allgegenwärtig sind, die heute praktisch unbegrenzte Speicherkapazität und die Automatisierung von Abläufen und damit weitere Datenbanken, -speicher und Zugriffsmöglichkeiten.

Beispiele dafür sind Datenspeicher für Sozial- und Gesundheitsdaten, wie z. B. bei der elektronischen Gesundheitskarte oder der Erhebung von Sozialdaten, Smart Meter zur exakten Ermittlung des Energieverbrauchs, Datenspeicher für die Strafverfolgung wie bei der Vorratsdatenspeicherung oder Datenzugriffe wie bei der Bestandsdatenauskunft, Nachrichtendienstliche Datenauswertung, wie z. B. bei PRISM, Tempora, XKeyScore oder wirtschaftlich genutzte Daten, z. B. in sozialen Netzwerken oder bei Internet-Suchmaschinen.

Die Diskussion führten *Stefan Hügel* als Moderator, *Sylvia Johnigk*, die die technischen Möglichkeiten der Überwachung und die Konsequenzen daraus betrachtete und *Dietrich Meyer-Ebrecht*, der die Möglichkeiten – und vor allem die Hindernisse – untersuchte, Technik demokratisch zu gestalten und zu kontrollieren. Die Diskussion sollte sich an folgenden Leitfragen orientieren:

- Welchen Umfang und welche Überwachungstiefe erlauben die heutigen technischen Möglichkeiten der Kommunikationsüberwachung?

- Inwieweit werden Menschenrechte durch die Technik gefährdet? Welchen Einfluss hat die technische Entwicklung der Überwachungsmöglichkeiten auf die Freiheitsrechte der Betroffenen? Welche Folgen für Demokratie und Freiheit ergeben sich daraus? Welche politische Bedeutung hat der Schutz der Privatsphäre?

- Welche Anforderungen an die Technikgestaltung ergeben sich aus den grundrechtlich verbürgten Freiheitsgarantien? Insbesondere: Wie weit muss die Auswahl und der Einsatz legitimer Überwachungstechniken für die Öffentlichkeit transparent gemacht werden? Wie kann eine menschenrechtskonforme Nutzung der Technik überprüft und sichergestellt werden?

Sylvia Johnigk fragte in ihrem Referat nach dem Überwachungspotenzial der heutigen Kommunikationstechnik. Genutzt wird von Geheimdiensten und Militär die Verpflichtung von Anbietern zur *lawful Interception* und die weitergehende Kollaborationsbereitschaft von Unternehmen – damit haben sie weitgehenden Zugriff auf die Informations- und Kommunikationstechnik und können Online-Dienste zur flächendeckenden Überwachung nutzen. Geschwächt werden sie, wenn Nutzer-

innen und Nutzer sicher kommunizieren und dazu beispielsweise Kryptoprodukte nutzen.

Für geheimdienstliche Operationen stehen eine Reihe von Methoden und Werkzeugen zur Verfügung:

- die Kompromittierung von Geräten und Infrastruktur, z. B. indem Rechner online mit Schadsoftware verseucht oder Botnetze zur Überwachung aufgebaut werden,
- der Einbau zusätzlicher „Features" in Produkten, z. B. indem bestellte Geräte auf dem Postweg abgefangen und mit Überwachungstechnik ausgestattet werden,
- Desinformation und Propaganda, indem Informationen verfälscht und Aktivisten und Kritiker diskreditiert werden.

Sylvia Johnigk kritisierte in diesem Zusammenhang die Bundesregierung und weitere Exekutivorgane. Durch mangelnde Aufklärung, Kooperation mit der NSA und Befürwortung massenhafter und flächendeckender Ausspähung leisteten sie Beihilfe zu geheimdienstlichen Aktionen, die gegen internationale Menschenrechte und die deutsche Verfassung verstießen. Dies führe zu einer Reihe von Bedrohungen für Zivilgesellschaft und Demokratie: Kommunikation ist nicht mehr vertraulich und unbeobachtet, Geräte sind nicht mehr vertrauenswürdig und Internetdienste können nicht mehr unbeobachtet genutzt werden. Die informationelle Selbstbestimmung ist verletzt, keine freie demokratische Willensbildung mehr möglich.

Weitere Details sind in dem ausführlichen Beitrag von Sylvia Johnigk ab Seite 58 nachzulesen.

Dietrich Meyer-Ebrecht stellte in seinem Referat fest, dass sowohl der Staat als auch die Bürgerinnen und Bürger bei der Abwehr der Ausspähung gefordert sind. Notwendig ist der politische Wille der Verantwortlichen, den Schutz vor Ausspähung und Überwachung durchzusetzen. Dazu ist gesellschaftlicher Druck notwendig, um die Politik zu den notwendigen Entscheidungen zu bringen.

Drei Faktoren sind dafür maßgeblich:

1. Die Innen- und außenpolitische Dimension: Die Ausspähung ist ein wesentliches Element des Cyberwarfare – will die Regierung dem Schutzauftrag gegenüber ihren Bürgerinnen und Bürgern nachkommen, müsste sie die Befugnisse der Nachrichtendienste einschränken und bereit sein, die transatlantischen Beziehungen hintanzustellen – angesichts internationaler Abkommen ein schwieriges Unterfangen.
2. Die gesellschaftliche Dimension: Auch die Gesellschaft wird lieb gewonnene Verhaltensmuster und wirtschaftliche Interessen aufgeben müssen. Der Gesetzgeber kann uns nicht schützen, wenn wir legislative Schutzmaßnahmen durch leichtfertigen Umgang mit unseren Daten unterlaufen, weil wir auf Komfort oder wirtschaftlichen Gewinn nicht verzichten wollen.
3. Die psychologische Dimension: Die Überwachung ist *counterintuitive* – wir können es uns nicht vorstellen, dass aus der Masse an Daten ausgerechnet „unsere" herausgefischt werden. Dabei ist das Gegenteil der Fall – je größer die analysierten Datenmengen, desto größer die Wahrscheinlichkeit, dass vorgegebene Muster in den Daten – auch unseren – gefunden werden.

Sylvia Johnigk, Stefan Hügel und Dietrich Meyer-Ebrecht
Foto: Sven Lüders

Fazit ist, dass wir uns der Gefahren aus der Datenverarbeitung bewusst werden und daraus die Voraussetzungen schaffen, politischen Druck aufzubauen. Dies ist ein langwieriger Prozess – der erste Schritt ist, zum Selbstschutz zu greifen, z. B. durch Nutzung sicherer Kommunikationsmethoden und Verschlüsselung. Wir müssen uns bewusst machen, dass wir uns damit ein Stück Freiheit zurückerobern.

Der vollständige Beitrag von Dietrich Meyer-Ebrecht ist ab Seite 60 nachzulesen.

Weitere Sessions konzentrierten sich auf verfassungsrechtliche Fragen der Ausspähung: *Ausspähung in Lichte des Grundgesetzes – kann die nationale Verfassung Freiheit und Menschenrechte noch effektiv schützen?* und die Handlungsmöglichkeiten: *Was sind unsere Handlungsoptionen, um Demokratie und Freiheit effektiv zu schützen?* Die Zeitschrift **vor***gänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik* wird in ihrer Ausgabe 206/207 ausführlich darüber berichten.

Im Rahmen des Verbandstags der Humanistischen Union wurde am gleichen Abend der Fritz-Bauer-Preis an Edward Snowden verliehen. Mit dem Fritz-Bauer-Preis würdigt die Humanistische Union herausragende Verdienste um die Humanisierung, Liberalisierung und Demokratisierung der Rechtsordnung. Der Preis ist benannt nach dem früheren Hessischen Generalstaatsanwalt *Fritz Bauer*, der als Wegbereiter einer juristischen Aufarbeitung des NS-Unrechts und Reformer des Strafrechts wie des Strafvollzuges gilt.

> *„Edward Snowden steht für eine außergewöhnliche Zivilcourage bei der Aufdeckung grund- und menschenrechtswidriger Überwachungspraktiken. Gemeinsam mit anderen Engagierten enthüllte er, in welchem Ausmaß die geheimdienstliche Überwachungspraxis heute rechtliche Schranken, die Grenzen des Vorstellbaren sowie des moralisch Vertretbaren überschreitet",*

begründete der Bundesvorsitzende der Humanistischen Union, *Werner Koep-Kerstin*, die Vergabe des Preises.

Snowden, der aus bekannten Gründen den Preis nicht persönlich entgegen nehmen konnte, dankte für die Verleihung mit einer Grußbotschaft aus Moskau, in der er unter anderem ausführte:

> *„What we have, as a public, accomplished in one year is to reveal to the world the reality of new restrictions on our rights, on our freedom to speak and associate, even to think and to be. But more critically, we revealed that it is not we the people who changed, but our policies, and that this occured in secret, without neither public consent nor debate. This clandestine movement of government away from the participatory state toward one that is closed and technocratic, I think, cannot survive the light thrust upon it. We say, ‚Always a citizen, never a subject.'"*

Die vollständige Botschaft und weitere Informationen zur Verleihung des Fritz-Bauer-Preises sind auf den Internet-Seiten der Humanistischen Union zu finden.[1]

Anmerkung

1 *http://www.humanistische-union.de/nc/aktuelles/aktuelles_detail/back/aktuelles/article/auszeichnung-fuer-einen-wertvollen-beitrag-zur-wahrung-unserer-grundrechtsordnung/*

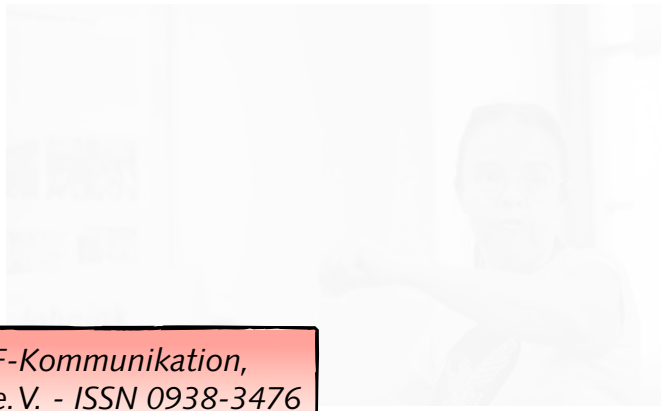
Sylvia Johnigk

Bürgerrechte nach dem NSA-Skandal

Geheimdienste und Militär nutzen die Verpflichtung von Telekommunikationsunternehmen zur Lawful Interception *und die Kollaborationsbereitschaft von Unternehmen aus, um flächendeckend Informationen abzuschnorcheln. Somit dienen die Informations- und Kommunikationstechnik und insbesondere das Internet und die Online-Dienste zur massenhaften und flächendeckenden Ausforschung und Überwachung.*

Geheimdienste und Militär wollen unsere Metadaten

Dabei stehen Netzknotenpunkte im Fokus, wie zum Beispiel der weltweit größte Internetknotenpunkt DE-CIX, der in Frankfurt betrieben wird. Dieser wird von verschiedenen Betreibern unterhalten, unter anderem ist auch *Level(3)* dabei, ein Kollaborateur des britischen Geheimdienstes GCHQ. Ferner werden Glasfaserkabel an zentralen Orten wie den transatlantischen Unterseekabeln nahezu vollständig auf Metadaten und partiell auf Inhaltsdaten abgeschnorchelt.



…ierten Referat, Foto: Sven Lüders

Insbesondere interessieren sich d… tadaten. Es scheint so, als wapp… die Zukunft. In den nächsten Jah… tadaten erzeugt, *Smart Phone*, *Smart Pad*, *Smart TV*, *Smart Grid*, *Smart Fridge*, *Smart Power*, *Smart Car*, *Smart App*. Das sind unfassbar viele Informationen, die die Geheimdienste zu einem gigantischen Verhaltensprofil zusammen führen wollen.

Geheimdienste und Militär schwächen unsere IT

Geheimdienste und Militär schwächen aktiv Software-, Krypto- und Hardwareprodukte, indem sie bei den herstellenden Unternehmen bewusst Schwachstellen einbauen lassen, die sie für ihre Zwecke nutzen.

Zusätzlich werden gezielt Endgeräte, Netzwerkgeräte, Server, Tastatur, Monitor, USB, Smartphone, etc. von Nutzern durch die Geheimdienste mit Wanzen und anderem Ungeziefer ausgestattet. Der Bestellvorgang im Online-Shop und die Bezahlung per Kreditkarte erleichtern es den Geheimdiensten, gezielt die bestellte Ware einer bestimmten Person auf dem Versandweg abzufangen und zu infiltrieren.

Hierfür gibt es für Geheimdienste einen Bestellkatalog[1], aus dem sie die richtigen Tools für ein bestimmtes Gerät auswählen können. Eine weitere Möglichkeit ist das Erzeugen von *Windows*-Fehlermeldungen und so das potenzielle Abgreifen von privaten Informationen über die Versendeoptionen *Melden des Fehlers* an den Provider.

Die aktuelle Konzeption und Implementierung von IuK-Netzwerken und IuK-Technik sind offen für das Ausspähen von Daten. Viele Endgeräte sind aktuell nicht sicher, so dass es schwierig ist, auf diesen Endgeräten Krypto- und andere Sicherheitsanwendungen sicher zu installieren und zu benutzen.

Geheimdienste und Militär betreiben *Bot-Netze* und infizieren 100.000 private Rechner, um sie im Ernstfall für einen Cyberangriff nutzen zu können.[2]