
Notwendigkeit und Chancen eines modernen europäischen Rechtsrahmens angesichts von „PRISM“ und „TEMPORA“

2

Alexander Dix

Nach dem nahezu täglich neue Details über die Aktivitäten des US-amerikanischen und des britischen Geheimdienstes bei der Überwachung der globalen Telekommunikation bekannt werden, stellt sich die Frage nach der „Beherrschbarkeit“ von Big Data und Cyber Security völlig neu.

Man kann geradezu von einem „doppelten Zauberlehrlings-Effekt“ sprechen: Demokratische Staaten wie die USA und Großbritannien und die mit ihnen kooperierenden Länder verfügen über Nachrichtendienste, die offenbar jedes Maß verloren haben und anlasslos die Telekommunikation und den gesamten Internet-Verkehr, auch soweit er nur deutsche Kommunikationspartner betrifft, überwachen. Schon dies hat der frühere Präsident Bundesamtes für Verfassungsschutz und des Bundesnachrichtendienstes, Hansjörg Geiger, mit Recht als „zutiefst verstörend“ bezeichnet. Die Richter des geheimen Foreign Intelligence Surveillance Courts haben zudem eingeräumt, dass sie keine Möglichkeit haben, die National Security Agency effektiv zu kontrollieren. Dieser Geheimdienst ist offenbar außer Kontrolle. Während Marc Zuckerberg jüngst noch beklagte, die US-Regierung habe seinem Unternehmen geschadet, weil sie betont habe, nur US-Bürger seien vor einer Ausspähung ihrer Kommunikation ohne richterliche Anordnung geschützt, belegen neueste Dokumente, deren Offenlegung die Electronic Frontier Foundation erzwungen hat, belegen, dass die NSA über Jahre rechtswidrig auch US-Amerikaner überwacht hat. Der Grund dafür sei, dass niemand innerhalb des Nachrichtendienstes „volles Verständnis dafür gehabt habe, wie das System arbeite.“² Offenbar ist also die NSA selbst nicht mehr in der Lage, die technischen Systeme zur heimlichen Kommunikationsüberwachung, die

¹ Vgl. dazu schon Bamford, *The Shadow Factory* (2008).

² Süddeutsche Zeitung v. 12.9.2013, S. 8 („Eingriff in die Privatsphäre“).

A. Dix (✉)
10787 Berlin, Deutschland
E-Mail: dix@datenschutz-berlin.de

sie selbst unter erheblichem Kostenaufwand nach dem 11. September 2001 geschaffen hat, zu kontrollieren.

Hinzu kommt folgendes: Wenn Hersteller von Sicherheitssoftware oder Netzknotenrechnern auf Veranlassung der Geheimdienste Schwachstellen und Hintertüren in ihren Produkte verstecken, kann nicht verhindert werden, dass auch Kriminelle diese Schwachstellen ausnutzen. So wird statt Sicherheit systematisch Unsicherheit erzeugt und Vertrauen zerstört. Dieser Vertrauensverlust ist – wie es der Bundesbeauftragte für den Datenschutz treffend formuliert hat – mit Händen zu greifen. Prognosen besagen, dass US-Anbieter von Cloud-Diensten aufgrund der Enthüllungen über die NSA-Aktivitäten in den nächsten drei Jahren bis zu US\$ 35 Mrd. Verlust machen könnten.

In diesem Zusammenhang ist es bemerkenswert, dass gerade von Seiten der Informatik betont wird, die Lösung könne nicht – jedenfalls nicht ausschließlich – durch Technik erfolgen, sondern müsse ganz wesentlich durch klare Regeln und Sanktionen gefunden werden, die letztlich übernational zu formulieren seien.

Deshalb ist die gegenwärtige Diskussion über einen neuen europäischen Rechtsrahmen von zentraler Bedeutung. Die Europäische Kommission hat mit ihrem Vorschlag für eine Datenschutzgrundverordnung vom Januar 2012 eine Initiative für eine grundlegende Modernisierung des Datenschutzrechts in Europa ergriffen, die längst überfällig war. Schon auf nationaler Ebene haben die Datenschutzbeauftragten, aber auch Verbraucherschützer mehrere Bundesregierungen vergeblich aufgefordert, das Datenschutzrecht den Anforderungen des 21. Jahrhunderts anzupassen. Vorschläge zur Modernisierung, die bereits auf dem Tisch lagen, verschwanden nach den Anschlägen des 11. September in den Schubladen des Bundesinnenministeriums. Das jetzt eine Debatte über ein zeitgemäßes und zugleich zukunftsoffenes Datenschutzrecht auf europäischer Ebene geführt wird, ist deshalb zu unterstützen.

Zwar hat die Europäische Kommission nicht die Kompetenz, die Tätigkeit von Geheimdiensten einzuschränken oder ihre Kontrolle zu verbessern; dies kann letztlich nur durch Regierungsabkommen oder völkerrechtliche Verträge geschehen. Auch habe ich Zweifel, ob die Initiative der Bundesregierung und der französischen Regierung, wonach Unternehmen verpflichtet werden sollen, über Anfragen von Nachrichtendiensten zu informieren, erfolgreich sein wird. Sowohl in den USA als auch in Großbritannien, aber auch in der Bundesrepublik selbst muss über solche Anfragen regelmäßig Stillschweigen bewahrt werden.

Dennoch bietet die Grundverordnung mittelbar die Chance, dass Europa seine Grundwerte in Sicherheitsstandards gießen bzw. über hohe technisch-organisatorische Anforderungen die Datenverarbeitung der Unternehmen gegen unkontrollierte Zugriffe von Nachrichtendiensten besser schützen kann.

Das setzt naturgemäß voraus, dass zunächst innerhalb Europas ein politischer Konsens darüber hergestellt wird, was Geheimdienste dürfen und was nicht. Natürlich müssen sie die Möglichkeit haben, den Telekommunikationsverkehr gezielt oder – wie der Bundesnachrichtendienst – durch Einsatz von Filterprogrammen *einen Teil* der grenzüberschrei-

tenden Kommunikationsverbindungen zu überwachen, wenn dies effektiv – übrigens auch durch Datenschutzbeauftragte – kontrolliert werden kann. Inakzeptabel ist dagegen, dass sämtliche Metadaten im Sinne eines „Full Take“ unterschiedslos und routinemäßig gespeichert werden, wie es das Programm TEMPORA des britischen GCHQ tut. Das Erschreckende an diesem Programm ist die Totalität der Überwachung.

Um keine Missverständnisse aufkommen zu lassen: Natürlich muss der Terrorismus effektiv und auch mit nachrichtendienstlichen Mitteln international bekämpft werden. Aber die jetzt bekannt gewordenen Aktivitäten der NSA und des GCHQ gehen weit darüber hinaus, was in einer demokratischen Gesellschaft zu diesem Zweck erforderlich ist. Diese Nachrichtendienste spähen nicht nur internationale Organisationen wie die EU und die Vereinten Nationen aus, sondern sie betrachten es auch als ihre Aufgabe, für die Stabilität des internationalen Finanzsystems zu sorgen und Wirtschaftsspionage zu betreiben.

Wenn die Datenschutz-Grundverordnung, die gegenwärtig noch im EU-Parlament und im Rat beraten wird, rechtzeitig vor der Neuwahl des Parlaments verabschiedet werden kann, bietet dies allerdings die Chance, dass Europa seinen Unternehmen einen erheblichen Vorteil im weltweiten Wettbewerb verschafft.

Das setzt die Umsetzung bestimmter Essentialia voraus:

1. Anbieter von Cloud-Diensten auf dem europäischen Markt werden künftig dem EU-Recht unabhängig davon unterliegen, wo ihre Server stehen. Darüber besteht offenbar bereits weitgehend Einigkeit sowohl im Parlament als auch im Rat. Google, Facebook und andere US-Unternehmen haben in der Vergangenheit lange Zeit argumentiert, sie unterlägen wegen des Sitzes ihrer Mutterkonzerne ausschließlich dem US-Recht (einschließlich der Zugriffsrechte der Nachrichtendienste nach dem Patriot Act). Dagegen entspricht das jetzt vorgesehene Markttortprinzip im Grunde einer Selbstverständlichkeit, die auch der US-Supreme Court für die umgekehrte Konstellation stets für richtig gehalten hat: Wer in den USA Geschäfte machen wolle, müsse sich an das dort geltende Recht halten.
2. Die Kommission hat vorgeschlagen, dass harte Sanktionen gegen solche Unternehmen verhängt werden können, die gegen europäisches Datenschutzrecht verstoßen: bis zu 2 % des globalen Umsatzes sollen die Aufsichtsbehörden als Geldbuße verhängen können. Hiergegen gibt es naturgemäß Widerstand von Seiten der Wirtschaftsverbände, aber es ist zu hoffen, dass auch dieser Vorschlag in die Grundverordnung übernommen wird. Denn nur wenn die Aufsichtsbehörden glaubwürdige Sanktionsmöglichkeiten haben, können sie den neuen europäischen Rechtsstandard auch durchsetzen.
3. Schließlich sollte die Grundverordnung verpflichtende Vorgaben für die Entwickler und Hersteller von Datenverarbeitungstechnik vorsehen, damit bis hin zu einer Produkthaftung „privacy by design“ bei der Herstellung von Hard- und Software nicht nur versprochen, sondern auch realisiert wird. Insofern ist ein Mix zwischen Regulierung und der Schaffung von Marktanreizen sinnvoll. Allerdings muss die Grundverordnung in diesem Punkt während der jetzt laufenden Beratungen im Europäischen Parlament

und im Rat noch deutlich präzisiert werden. Grundprinzipien des technischen Datenschutzes wie Anonymisierung und Pseudonymisierung sollten ebenso in den neuen Rechtsrahmen aufgenommen werden wie verbindliche Festlegungen zum Verfahren, zu den Kriterien und den Rechtsfolgen der Zertifizierung.

Zwar ist das vom Bundesverfassungsgericht entwickelte Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme eine spezifische Rechtsfigur des deutschen Verfassungsrechts. Es kann aber kein Zweifel daran bestehen, dass Informationssicherheit ein globales Problem ist, das nur durch die Setzung weltweiter Standards einer Lösung näher gebracht werden kann.

Letztlich muss die Frage beantwortet werden, die schon bei der Diskussion um die Online-Durchsuchung – wenn auch nur national – im Vordergrund stand: Wollen wir eine hochsichere, vertrauenswürdige Informationstechnik, bei der die Überwachung der Kommunikation die kontrollierte Ausnahme bleibt, oder wollen wir eine Gesellschaft, in der die unkontrollierbare Überwachung die Regel ist.

Alexander Dix ist seit Juni 2005 Berliner Beauftragter für Datenschutz und Informationsfreiheit. Zuvor war er sieben Jahre Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht in Brandenburg. Dr. Dix hat besondere Fachkunde im Bereich von Telekommunikation und Medien sowie für Fragen des grenzüberschreitenden Datenschutzes. Er ist Vorsitzender der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation (international auch bekannt als „Berlin Group“) und Mitglied der Artikel 29-Gruppe der Europäischen Datenschutzbeauftragten, in der er die Bundesländer vertritt. Außerdem leitet Dr. Dix die beiden Arbeitsgruppen des Düsseldorfer Kreises der Aufsichtsbehörden für den Datenschutz zum Internationalen Datenverkehr und zu Telemedien und Telekommunikation.

Beherrschbarkeit von Cyber Security, Big Data und
Cloud Computing

Tagungsband zur dritten EIT ICT Labs-Konferenz zur
IT-Sicherheit

Bub, U.; Wolfenstetter, K.-D. (Hrsg.)

2014, XI, 86 S. 20 Abb., Softcover

ISBN: 978-3-658-06412-9