www.jusletter-it.eu

Rolf H. Weber / Dominic N. Staiger

Spannungsfelder von Datenschutz und Datenüberwachung in der Schweiz und in den USA

Edward Snowden brought to light the extensive National Security Agency surveillance which raises numerous issues in regard to the protection of fundamental rights. The article contrasts the surveillance capabilities of Swiss authorities with those of their American counterparts focusing in particular on data protection concerns. Moreover technical solutions in minimizing monitorability as well as organizational changes are addressed with the aim of reducing exposure to foreign surveillance.

Category: Articles
Field of law: Data Protection; Data Security
Region: Switzerland

Citation: Rolf H. Weber / Dominic N. Staiger, Spannungsfelder von Datenschutz und Datenüberwachung in der Schweiz und in den USA, in: Jusletter IT 15 May 2014

Inhaltsübersicht

1 Einleitung

[Rz 1] In letzter Zeit sind der Schutz der Privatsphäre und der Datenschutz durch die Veröffentlichungen Edward Snowdens vermehrt in den Fokus der Medien gerückt. Insbesondere die umfangreiche Datenüberwachung durch die National Security Agency (NSA) hat als Anlass gedient, auch die Arbeitsweisen der europäischen Geheimdienste und Behörden kritisch zu hinterfragen.

[Rz 2] Der vorliegende Beitrag geht auf die schweizerische Gesetzgebung zur Datensammlung und Überwachung sowie deren praktische Alltagsanwendungen ein. In Vergleich dazu gesetzt werden die amerikanischen Überwachungskompetenzen, aber gleichzeitig auch Fragestellungen, welche sich für die Schweiz aus den unterschiedlichen Perzeptionen ergeben, identifiziert.

[Rz 3] Aufgrund der bevorstehenden Revision des Bundesgesetzes zur Überwachung des Post- und Fernmeldeverkehrs (BÜPF) kommen weiter die Verwertung von Daten, welche sich durch besondere Software oder real-time Aufzeichnungen sammeln lassen, zur Sprache.

[Rz 4] Die rechtsvergleichende Betrachtungsweise und die Berücksichtigung anhängiger Gesetzesvorlagen sind nicht zuletzt deshalb von Bedeutung, weil viele früher kaum hinterfragte Praktiken von der Öffentlichkeit heute verbreitet in Zweifel gezogen werden. Zu den zentralen Diskussionsthemen zählen die massenweise Abfrage von Personen- und Standortdaten im Internet sowie die Nutzung von Mobilfunkdaten (Geo- und Nutzerdaten). Dabei zielt die Überwachung nicht auf eine bestimmte Person ab, sondern der gesamte Nutzerkreis wird einer pauschalen Überwachung ausgesetzt. Dieses Vorgehen untergräbt den Schutz der Privatsphäre und wirft Fragen hinsichtlich der Legitimität der angewandten Massnahmen auf. Die fortschreitende technische Entwicklung begünstigt den flächendeckenden Einsatz dieser Überwachungsformen. Es bedarf daher klarer Vorgaben und Abläufe, um den Einsatz solcher Überwachungsvorkehren zu legitimieren. Eine ausufernde Überwachung nach amerikanischem Verständnis ist jedenfalls zu

verhindern.

2 Grundrechtliche Ausgangslage

[Rz 5] Von Bedeutung für das Thema der Überwachung ist aus verfassungsrechtlicher Sicht, dass die Sichtweisen Amerikas und Europas beim Schutz der Privatsphäre und der Daten sehr unterschiedlich sind. Die amerikanische Verfassung setzt einen Schwerpunkt auf die individuellen Entfaltungsfreiheiten des Einzelnen; der Grundsatz der freien Meinungsäusserung erhält dabei ein viel stärkeres Gewicht, als dies in Europa angesichts des gleichwertigen Schutzes der Privatsphäre der Fall ist.

[Rz 6] Insoweit im Vordergrund steht Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) von 1950, welcher das Recht des Einzelnen auf Privatsphäre statuiert.[1] In der Schweiz ist dieses Recht durch Artikel 13 der Bundesverfassung (BV) gewährleistet und steht daher unter besonderem Schutz.[2]

[Rz 7] Der Grossteil der amerikanischen Unternehmen nimmt diesen gesetzmässig verankerten Schutz der Privatsphäre oftmals erst wahr, wenn europäische Behörden sie zur Einhaltung höherer Datenschutzstandards auffordern.[3] Facebook wird z.B. des Öfteren von europäischen Datenschutzbehörden wegen unzureichender Datenschutzeinstellungen gerügt. Die Identifizierbarkeit von Personen in Googles Dienstleistung Street View führte bei der Erstellung des Bildmaterials für das europäische Produkt zu starken Protesten und vereinzelten Klagen von Verbrauchern und Datenschützern. Gerügt worden sind unter anderem die Befahrung von Privatstrassen sowie das Sammeln von Daten aus ungesicherten WLAN-Netzen.[4] Anfangs zog sich Google auf das Argument zurück, die Daten seien in Kalifornien erfasst und nicht dem örtlich zuständigen Recht unterstellt. Erst auf Druck der Datenschutzbehörden hin wurde Google aktiv und schuf eine Beschwerdemöglichkeit zur Löschung von aufgenommenem Bildmaterial.[5]

[Rz 8] Eine Übermittlung personenbezogener Daten in die USA gemäss europäischer Datenschutz-Richtlinie (95/46/EG)[6] oder Art. 6 Bundesgesetz über den Datenschutz (DSG) ist nur gestattet, wenn das US-Unternehmen dem entsprechenden Safe Harbor Abkommen beigetreten, d.h. Safe Harbor zertifiziert, ist. Mit diesem Abkommen hat die EU bzw. die Schweiz die Möglichkeit geschaffen, personenbezogene Daten trotz des inadäquaten amerikanischen Datenschutzniveaus

---

1 Vgl. die Pressemitteilung der Europäischen Kommission vom 25. Januar 2012, in welcher hervorgehoben wird, dass der Schutz der personenbezogenen Daten ein Grundrecht aller Europäer ist, die EU-Bürger jedoch nicht immer das Gefühl haben, dass sie die Kontrolle über Ihre personenbezogenen Daten besitzen; http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0uage=DE&guiLanguage=en(alle Internetquellen zuletzt besucht am 19. März 2014); zum grundsätzlichen Verhältnis von Art. 8 und 10 EMRK vgl. Rolf H. Weber/Markus Sommerhalder, Das Recht der personenbezogenen Information, ZIK Bd. 35, Zürich/Basel/Genf 2007.

2 Art. 10 Abs. 2 BV ist hier ebenso von Bedeutung, weil die Selbstbestimmungsfreiheit durch den Verlust der Herrschaft über die eigenen Daten eingeschränkt wird.

3 Zum Datenzugriff in der Cloud aus deutscher Sicht vgl. Paul Voigt, Weltweiter Datenzugriff durch US-Behörden, MMR 3/2014, S. 158–161.

4 Oliver Jorns/Zhendong Ma, Wo bin ich, wo sind wir, wo ist alles? – Ortsbezogene Dienste bieten Vorteile und immense Möglichkeiten, allerdings auch Gefahr des Verlusts der Privatsphäre, digma 2011 S. 30, 32.

5 Thilo Weichert, Der Fall «Street View» in Deutschland, digma 2009, S. 102–106.

6 Vgl. zum Safe Harbor Abkommen die Entscheidung der Europäischen Kommission; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DE:PDF.

in die USA transferieren zu können. Das Daten empfangende US-Unternehmen muss sich dabei verpflichten, die EU- oder Schweizer Datenschutzstandards einzuhalten und eine entsprechende Zertifizierung nachzuweisen. Der höhe Schutzstandard stellt aber lediglich eine vertragsrechtliche Zusicherung dar, welche der amerikanischen Gesetzgebung untergeordnet ist. Damit besteht weiterhin eine Zugriffsmöglichkeit der amerikanischen Behörden auf die Daten und das Risiko einer potenziellen Verwendung entgegen den europäischen Datenschutzbestimmungen.

[Rz 9] Nach Veröffentlichung des amerikanischen Überwachungsprogramms wurde die Zulässigkeit der von Apple und Facebook durchgeführten EU-US Datentransfers in Frage gestellt. Die irische Datenschutzbehörde überprüfte daraufhin, ob Übermittlungen in die USA weiterhin, gemäss der Safe Harbor Vereinbarung, möglich seien. Ihrer Meinung nach sei sich die Europäische Kommission durchaus bewusst gewesen, dass die amerikanischen Behörden auf die Daten, welche unter dem Safe Harbor Abkommen transferiert werden, zugreifen könnten. Weil dies somit bereits zum Zeitpunkt des Abkommens bekannt war, gebe es für die irische Behörde keinen Grund, die Datenübermittlungen nicht zu gestatten.[7]

[Rz 10] Die kürzlich aufgedeckten Spionagetätigkeiten der USA sind vorerst gemäss amerikanischem Recht auf ihre Zulässigkeit hin zu untersuchen. Meist ist es ausdrücklich Aufgabe der Geheimdienste, ausländische Verbindungen, seien dies Daten oder Kommunikationen, ohne Einschränkungen abzuhören und aufzuzeichnen. Im Inland sind sie jedoch an die jeweiligen verfassungs- und gesetzmässigen Grenzen gebunden; sie dürfen die Kommunikation ihrer eigenen Bürger nur innerhalb dieser strengen Grenzen überwachen.

3 Datenüberwachung in der Schweiz

[Rz 11] Die Abfrage und Auswertung von Personendaten ist in der Schweiz vornehmlich durch das BÜPF sowie durch die Strafprozessordnung (StPO) geregelt; parallel können gestützt darauf sowohl verwaltungsrechtliche als auch strafrechtliche Vorschriften zur Anwendung kommen.

3.1 Inlandsüberwachung

[Rz 12] Das BÜPF regelt den Ablauf einer Datenabfrage und die Speicherung von Identifikationsdaten (sog. Vorratsdatenspeicherung).[8] Die zugehörige Verordnung (VÜPF) präzisiert die Pflichten der Kommunikationsanbieter in Relation zu deren angebotenen Dienstleistungen. So untersteht z.B. ein Internet-Zugangsanbieter anderen Verpflichtungen als ein Postanbieter.[9]

[Rz 13] Zurzeit wird das BÜPF revidiert, um der technischen Entwicklung Rechnung zu tragen (z.B. Internet). Dabei ist der Gesetzgeber nach eigener Aussage darauf bedacht, die Überwachung zu verbessern, sie aber nicht auszuweiten.[10] Ob diese Aussage zutrifft, ist mit Blick auf die mass-

7 Schriftsatz des irischen Data Protection Commissioners vom 23. Juli 2013; http://www.europe-v-facebook.org/Response_23_7_2013.pdf.

8 Art. 2 E-BÜPF.

9 Vgl. Art. 11 VÜPF; Art 15 VÜPF.

10 Erläuternder Bericht zur Änderung des Bundesgesetzes vom 6. Oktober 2000 betreffend dieÜberwachung des Post- und Fernmeldeverkehrs (BÜPF), S. 2 http://www.ejpd.admin.ch/content/ejpd/de/home/themen/sicherheit/ref_gesetzgebung/ref_fernmeldeueberwachung.html.

geblichen Gesetzesänderungen im vorliegenden Kontext nachfolgend zu analysieren.

3.1.1 Problembereiche in der BÜPF-Revision

[Rz 14] Um die Identifikationsdaten oder den Datenverkehr eines Nutzers erhältlich zu machen, ist die Staatsanwaltschaft verpflichtet, einem mehrstufigen Prozess zu folgen. Im ersten Schritt ist der Kreis der Anbieter, welcher zur Herausgabe von Informationen verpflichtet werden kann, genau zu umschreiben. Gemäss Art. 2 BÜPF sind die Anbieter von Fernmeldedienstleistungen sowie die Internet-Zugangsanbieter dem BÜPF unterstellt. Im revidierten BÜPF wird der persönliche Anwendungsbereich des Gesetzes indessen signifikant ausgedehnt. Neu sollen auch nicht beim Schweizer Bundesamt für Kommunikation (BAKOM) registrierte Fernmeldedienstanbieter sowie die Anbieter (einschliesslich Privater), welche einen Zugang zum Internet ermöglichen, vom Gesetz erfasst werden. Dies schliesst Schulen, Krankenhäuser und Cyber Cafés mit ein.[11] Hinsichtlich der Sicherstellung des Zugangs zu Informationen gelten für sie hingegen spezifische Anforderungen, welche in den Artikeln 19–30 BÜPF näher erläutert sind.[12]

[Rz 15] Von Bedeutung für die Strafverfolgungsbehörden ist insbesondere die Speicherung von Verbindungsdaten durch die Fernmeldedienstanbieter.[13] Der Speicherungszeitraum dieser Daten soll durch die BÜPF-Revision von 6 Monaten auf 12 Monate verlängert werden, was nicht unproblematisch ist.[14]

[Rz 16] Um eine Überwachung bzw. Abfrage von Verbindungsdaten zu veranlassen, muss ein Strafverfahren eingeleitet, ein Rechtshilfeersuchen gestellt, oder die Rettung einer vermissten Person veranlasst sein.[15] Im Rahmen der Revision wird dieser Aufzählung die Fahndung nach einer Person, die zu einer Freiheitsstrafe verurteilt wurde, hinzugefügt.[16] Die Sachlage im jeweiligen Strafverfahren bleibt ausschlaggebend für den Umfang der anzuordnenden Überwachung. Dabei hat der dringende Verdacht einer Straftat gemäss Art. 269 Abs. 2 StPO zu bestehen und die Schwere der Tat die Überwachung zu rechtfertigen.[17] Ferner müssen die vorgehenden Untersuchungshandlungen erfolglos gewesen sein oder die Untersuchung ohne die Überwachung in unverhältnismässiger Weise erschwert werden.[18] Die Straftatbestände schliessen den Grossteil aller Straftaten, wie z.B. auch den einfachen Diebstahl oder die Rassendiskriminierung, mit ein.[19]

[Rz 17] Der Antrag zur Überwachung einer Person wird von der Staatsanwaltschaft oder von einer durch die Kantone zu bezeichnenden Behörde[20] gestellt und durch das Zwangsmassnahmengericht genehmigt.[21] Dieses weist den Dienst für die Überwachung des Post- und Fernmeldever-

---

11 Anja Hasler, Gesetzgebung 03/2013, forumpoenale 3/2013, S. 191.

12 Zu unterscheiden sind insbesondere die Auskunftspflichten des Fernmeldedienstanbieters gemäss Art. 26 BÜPF von den Mitwirkungspflichten der Kommunikationsdienstanbieter unter Art. 27 BÜPF.

13 Rolf H. Weber/Christoph A. Wolf/Ulrike I. Heinrich, Neue Brennpunkte im Verhältnis von Informationstechnologien, Datensammlungen und flexibilisierter Rechtsordnung, in: Jusletter 12. März 2012.

14 Art. 12 Abs. 2 BÜPF; Art. 26 Abs. 5 E-BÜPF; kritisch zur Verlängerung Weber/Wolf/Heinrich(Fn. 13), Rz. 18.

15 Art. 1 BÜPF.

16 Art. 1 Abs. d E-BÜPF.

17 Art. 269 Abs. 1 Zif. b StPO.

18 Art. 269 Abs. 1 Zif. c StPO.

19 Art. 139 Ziff. 1 StGB, Art. 261 StGB.

20 Art. 14 Abs. 2 BÜPF; Art. 15 Abs. a E-BÜPF.

21 Art. 272 Abs. 1 StPO.

kehrs (Dienst) an, die entsprechenden Daten, welche die Telekommunikationsanbieter liefern, entgegenzunehmen und der Behörde zur Verfügung zu stellen. Der Dienst filtert unter Umständen, gemäss Anweisung der Genehmigungsbehörde, Informationen heraus, die aufgrund des Berufsgeheimnisses geschützt sind oder eine unbeteiligte Drittpartei betreffen.[22]

[Rz 18] Der Dienst stellt die erhaltenen Daten der untersuchenden Behörde zur Verfügung. Dabei kann der Dienst auf die Nutzungsdaten, welche die Internet Provider zurzeit 6 Monate lang gespeichert haben, zurückgreifen.[23] Auf eine Strafbestimmung, anzuwenden bei Missachtung der Aufbewahrungsvorschrift durch die Telekommunikationsanbieter, will der Gesetzgeber im revidierten BÜPF verzichten. Jedoch müssen die Kosten von ihnen übernommen werden, wenn sie der Aufbewahrungspflicht nicht nachkommen können und die Speicherung infolgedessen einem Dritten zu übertragen ist.[24]

[Rz 19] Die Identifizierbarkeit der Zielperson muss durch die Herausgabe der Daten des Telekommunikationsanbieters möglich sein. Bei sogenannten Antennensuchläufen, in welchen alle Mobiltelefonnutzer innerhalb eines bestimmten geographischen Gebiets pauschal erfasst sind, ist dies nicht der Fall, was in der Vergangenheit zu vermehrten Klagen der Netzbetreiber geführt hat. Die betroffenen Personen werden überwacht, um überhaupt erst einen Verdacht zu begründen. Das Bundesgericht hat aufgrund dieser Problematik strenge Voraussetzungen für die Nutzung von Suchläufen geschaffen. Unerlässlich sind dabei die Individualisierbarkeit der gesuchten Person sowie die ausschliessliche Auswertung von Verbindungsdaten ohne inhaltliche Überwachung.[25]

3.1.2 Eingeschränkte Anfechtung bzw. Überprüfung

[Rz 20] Eine zentrale Problematik dieser Überwachung besteht im Mangel einer Anfechtungsmöglichkeit mit Bezug auf die erteilte Verfügung.[26] Es existiert keine Verwaltungsbehörde, welche in Anwendung des massgeblichen Rechts prüft, zu welcher Überwachung der Fernmeldedienstanbieter verpflichtet werden kann.[27] Die Anordnung durch die Strafverfolgungsbehörde ist an den Dienst gerichtet, der nur prüft, ob die ausstellende Behörde zuständig ist und ob ein für die Überwachung notwendiges Strafverfahren vorliegt. Somit bestimmt die Behörde nicht nur über die Durchführung einer Massnahme, sondern legt ebenfalls fest, welche Massnahmen ein Fernmeldedienstanbieter auszuführen in der Lage sein muss. Selbst bei klar unrichtigen oder unbegründeten Anordnungen ist nur eine Kontaktaufnahme mit der ausstellenden Behörde vorgesehen.[28]

[Rz 21] Der Formulierung von Art. 13 BÜPF folgend ist somit eine Prüfung der rechtlichen Zulässigkeit der Überwachung nicht möglich.[29] Beschwerden gegen Verfügungen des Diensts lassen

---

22 Art. 13 Abs. 1 lit. f BÜPF .

23 Art. 13 Abs. 3 BÜPF.

24 Art. 34 Abs. 1 E-BÜPF.

25 Urteil des Bundesgerichts 1B_376/2011vom 3. November 2011, E. 6.1.

26 Simon Schlauri, Fernmeldeüberwachung à discrétion?, Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht 4/2012, S. 239.

27 Andreas Heiniger, Schrankenlose Fernmeldeüberwachung aufgrund eines konzeptionellen Fehlers im BÜPF?, in: Jusletter 17. September 2012, S. 2.

28 Art. 13 Abs. 1 lit. a BÜPF.

29 Heiniger(Fn. 27), S. 3.

sich nur gemäss den allgemeinen Bestimmungen der Bundesrechtspflege einreichen. Die entsprechende Problematik besteht darin, dass die überprüfende Instanz ebenfalls an die eingeschränkte Kognition des Diensts gebunden ist und somit die Grundlage der Verfügung lediglich prüfen kann, wenn eine unechte Gesetzeslücke besteht.[30] In der Rechtsprechung hat dies zuweilen zu Begründungsproblemen, insbesondere in Bezug auf die Nachprüfung der Zulässigkeit der eingangs genannten Antennensuchläufe, geführt.[31]

[Rz 22] Der Dienst ist nicht ermächtigt, eine durchgehende oder pauschale Überwachung oder Speicherung des Schweizer Datenverkehrs durchzuführen, denn er wird nur auf Anweisung einer Behörde und mit Genehmigung des Zwangsmassnahmengerichts aktiv. Eine erlassene Verfügung kann die Aufzeichnung des gesamten Datenverkehrs einer Person über einen vorgegebenen Zeitraum anordnen.[32] Die Massnahme ist auf maximal drei Monate beschränkt, lässt sich jedoch beliebig oft um jeweils bis zu drei weiteren Monaten verlängern.[33]

[Rz 23] Gemäss Art. 24 VÜPF vermag der Umfang einer genehmigten Internetüberwachung sehr gross zu sein. Unter anderem lassen sich E-Mails inklusive deren Attachments überwachen. Im Einzelfall ist indessen darauf zu achten, dass die Ermittlungsbehörde den richtigen Überwachungstyp wählt, damit die Daten, welche für ein späteres Verfahren notwendig sind, zur Aufzeichnung gelangen.[34]

3.1.3 Spezifische Diskussionsthemen (Trojaner, GovWare)

[Rz 24] Fraglich bleibt weiterhin die Verwendung von Trojanern (Spyware), welche auf dem Rechner des Ziels installiert werden, um z.B. eine Skype-Konversation abzuhören oder Zugriff auf Festplattendaten zu nehmen.[35] Der Einsatz von Spyware oder GovWare ist unter dem geltenden BÜPF nicht vorgesehen, jedoch gemäss Entwurf des revidierten BÜPF durch eine Anpassung der StPO möglich. Momentan scheint daher nur die Überwachung eines Skype-Anrufs rechtlich erlaubt, weil sie sich unter Artikel 269 StPO subsumieren lässt. Ein Zugriff auf Festplattendaten fällt dagegen nicht mehr unter die Definition der Überwachung des Post- und Fernmeldeverkehrs. Vielmehr könnte unter Umständen die ermittelnde Behörde durch einen solchen Eingriff in das fremde Computersystem selbst eine strafbare Handlung begehen.[36] Um Rechtssicherheit zu schaffen, ist daher eine ausdrückliche Genehmigung im revidierten BÜPF zu begrüssen.[37]

[Rz 25] GovWare birgt neben einer Eingrenzung der umfassenden Überwachungsmöglichkeiten weitere Herausforderungen, die sich aufgrund der technischen Komplexität ergeben. So ist es wahrscheinlich, dass durch das Einschleusen einer Software auf dem Zielcomputer Sicherheits-

30 Da in der nachträglichen Verwaltungsrechtspflege eine Beschwerdeinstanz nicht über eine umfassendere Kognition verfügen kann als die Vorinstanz, ist davon auszugehen, dass die Beschwerdeinstanz ihre Kognition in der gleichen Weise beschränkt sieht wie der Dienst. Auf dem Instanzenzug kann sich die Kognition höchstens verengen, allenfalls gleich bleiben, nicht aber ausweiten.

31 Urteil des Bundesgerichts 1B_376/2011vom 3. November 2011.

32 Vgl. zur Unterscheidung der möglichen Überwachungsarten Schlauri(Fn. 26), S. 240.

33 Art. 274 Abs. 5 StPO.

34 Thomas Hansjakob, BÜPF/VÜPF Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, 2. Aufl. St. Gallen 2006, S. 447.

35 Weber/Wolf/Heinrich(Fn. 13), Rz. 25.

36 Art. 143 StGB.

37 Weber/Wolf/Heinrich(Fn. 13), Rz. 26.

lücken erzeugt, welche von Dritten ebenfalls zum Eindringen in das Computersystem genutzt werden können.[38] Es wird zwar von Seiten des Bundesamts für Justiz betont, dass eine solche Software nur eingesetzt werde, wenn sie «sauber» funktioniere; indessen ist in der Praxis davon auszugehen, dass, wenn die rechtlichen Rahmenbedingungen einmal geschaffen sind, GovWare auch angewandt wird. Von zentraler Bedeutung ist daher die im Ständerat diskutierte Einschränkung der Nutzung auf einen bestimmten Kreis von schweren Straftaten.[39] Weiterhin sehen die Mitwirkungspflichten im revidierten BÜPF vor, dass abgeleitete Kommunikationsdienste (etwa reine E-Mail-Provider) sowie Personen, die ihren Internetzugang Dritten zur Verfügung stellen (etwa Internet-Cafés oder Hotels, aber auch Private), von den Pflichten im BÜPF ebenfalls erfasst sind. Der Bundesrat besitzt jedoch die Möglichkeit, kleine Anbieter von einzelnen Pflichten zu befreien, um Unverhältnismässigkeiten in der Anwendung des Gesetzes zu verhindern. Hierzu sind klare Regelungen aufzustellen.[40]

[Rz 26] Als weiterer wichtiger Unterschied wurde im Entwurf der revidierten Fassung des Gesetzes eine Entschädigung für Telekommunikationsanbieter entfernt. Die Kosten müssen damit die Konsumenten zukünftig selbst übernehmen. Dies könnte zu einem generellen Anstieg der Überwachungen führen, weil die Behörden für ihre Überwachungsmassnahmen kein Budget mehr zur Verfügung stellen müssen. Durch dieses Vorgehen würde eine wichtige finanzielle Einschränkung der Überwachungen abgeschafft und damit die Grundlage für noch umfassendere Massnahmen geschaffen. Bereits im Jahr 2013 fand ein signifikanter Anstieg (22%) der Einzelüberwachungen statt, welcher Kosten von rund 14.7 Millionen Franken erzeugte.[41] Im Rahmen der Diskussionen im Ständerat wurde nun der vom Bundesrat vorgeschlagene Mittelweg gewählt, welcher eine angemessene Entschädigung der Mitwirkungspflichtigen für die Kosten der einzelnen Überwachungen vorsieht. Damit wird einer möglichen ausufernden Anwendung von Überwachungsmassnahmen ein finanzieller Riegel vorgeschoben.[42]

3.2 Auslandsüberwachung

[Rz 27] Auf die Überwachungstätigkeiten des Schweizer Nachrichtendienstes im Ausland kommt das Bundesgesetz über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG) sowie dessen Verordnung (V-NDB) zur Anwendung. Im Ausland besitzt der Nachrichtendienst ein weites Spektrum an einsetzbaren Überwachungsmöglichkeiten. Er kann alle technischen Hilfsmittel verwenden, die zur Ausübung seiner Funktionen nötig sind.[43] Innerhalb der Schweiz setzt Artikel 14 des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS[44])

[38] Vgl. Ausschreibung des FBI zur Entwicklung eines neuen Trojaners https://www.fbo.gov/index?s=opportunity&mode=form&id=5b4b8745e39bae3510f0ed820a08c8e2&tab=core&_cview=0.

[39] NZZ, Grünes Licht für Staatstrojaner, NZZ Nr. 66, 20. März 2014, S. 12.

[40] Jan Flückiger, Der Bundesrat will die Telefon- und Internetüberwachung der technologischen Entwicklung anpassen. Kritiker sehen darin einen Angriff auf die Grundrechte. Auch bei den Dienstanbietern regt sich Widerstand, NZZ 26. Februar 2014; http://www.nzz.ch/ aktuell/schweiz/trotz-umstrittenen-massnahmen-nur-wenig-kritik-1.18252789.

[41] Mario Stäuble, Strafverfolger brechen Abhör-Rekord, Tages-Anzeiger, 3.März 2014, S. 5.

[42] Schweizer Radio und Fernsehen, Ständerat votiert für Schnüffel-Software, 11 März 2014, http://www.srf.ch/news/schweiz/session/staenderat-votiert-fuer-schnueffel-software.

[43] Art. 16 V-NDB.

[44] Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit, SR 120.

der Überwachung jedoch Schranken, weil nur öffentliche bzw. allgemein zugängliche Quellen verwendet werden dürfen.[45] Soll Zugriff auf einen Computer bzw. eine Verbindung im Inland genommen werden, müssen die Verfahrensvorschriften des BÜPF eingehalten und dessen Anwendungsvoraussetzungen erfüllt sein.

4 Datenüberwachung in den USA

[Rz 28] Die amerikanischen Behörden, insbesondere die National Security Agency (NSA), sind rechtlich und technisch in der Lage, weitreichende Überwachungsmassnahmen durchführen. Diese enorme Kompetenzkonzentration wird durch die komplexe Struktur der Gesetzgebung, den «Executive Orders» (EO), sowie der zum Grossteil unklaren Rechtsprechung ermöglicht.

4.1 Inlandsüberwachung

4.1.1 Rechtsgrundlagen

[Rz 29] Die Überwachung von Kommunikationsdaten in den USA beruht vornehmlich auf dem Patriot Act[46] und dem Foreign Intelligence Surveillance Act (FISA). Immerhin setzt der vierte US-Verfassungszusatz der Überwachung Grenzen. Gemäss Verfassung ist jeder amerikanische Staatsbürger vor unverhältnismässigen Durchsuchungen und Beschlagnahmungen geschützt. Eine komplette Überwachung des Datenverkehrs aller Bürger dürfte, selbst bei sehr einseitiger Interpretation, als unverhältnismässig zu qualifizieren sein.

[Rz 30] Der Patriot Act[47] wurde im Nachgang zu den Anschlägen des 11. September 2001 verabschiedet, um konsequent gegen den internationalen Terrorismus vorgehen zu können. Im Grunde ist er ein Sammelsurium an Änderungen bestehender Gesetzgebungen. So ersetzt der Abschnitt 215 des Patriot Act[48] den Abschnitt 501 des FISA. Er beschreibt die sogenannte «business records» Regel, welche es den Geheimdiensten erlaubt, die Herausgabe jedweder Sache («any tangible thing») zu verlangen, wenn dies für eine internationale Anti-Terror-Ermittlung relevant ist. Die Praxis hat gezeigt, dass die Behörden diese Kompetenz bis zum Höchstmass ausschöpften, indem eine expansive Auslegung der Bedeutung des Worts «relevant» erfolgte.

[Rz 31] Die Überwachung unter Abschnitt 215 des Patriot Act[49] muss von einem Gericht genehmigt werden. Sie darf nicht ausschliesslich auf die Aktivitäten einer amerikanischen Person abzielen, welche durch den ersten Verfassungszusatz (freedom of speech) geschützt ist. In Ausführung der Überwachung sind die Geheimdienste an die Executive Order 12333 und deren Ergänzungen gebunden. Unter anderem spezifizieren diese Orders des Präsidenten die praktische Umsetzung von Gesetzen und stellen eine direkte Weisung an die Exekutivorgane dar.

[Rz 32] Weil sowohl die Ausführung der Überwachung als auch der richterliche Entscheid (Se-

45 Art. 14 BWIS i.V.m. Art. 16 Abs. 3 V-DNB.

46 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001; http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

47 Patriot Act (Fn. 46).

48 Patriot Act (Fn. 46).

49 Patriot Act (Fn. 46).

cret Court[50] Verfahren) streng geheim sind, wurde eine Überwachungsmöglichkeit durch den Kongress (bestehend aus Senat und Repräsentantenhaus) geschaffen.[51] Der Generalstaatsanwalt muss die zwei Geheimdienstkomitees des Senats und Repräsentantenhauses halbjährlich über alle erteilten Überwachungsverfügungen informieren. Aufgrund des starken Eingriffs der Behörden in die Persönlichkeitsrechte der amerikanischen Bevölkerung vermag die Legitimation eines so kleinen Komitees jedoch nicht zu überzeugen.

4.1.2 Speicherung von Metadaten

[Rz 33] Im Jahr 1979 wurde der wohl bedeutendste Gerichtsentscheid, welcher die heutige amerikanische Überwachung erst ermöglichte, gefällt. Der Fall Smith v. Maryland, 442 U.S. 735 (1979), hob hervor, dass Telefonnummern kein Privatsphärenschutz zukommt. Das Gericht formulierte erstmals ein Konzept, nach welchem die Informationen mit einer angemessenen Erwartung auf Privatsphäre bzw. Geheimhaltung verknüpft sein müssen, um den Schutz des vierten Verfassungszusatzes (protection against unreasonable search and seizure) zu geniessen. Dieser Schutz findet aber auf Telefondaten keine Anwendung, weil mit ihnen keine Erwartung nach Privatsphäre verbunden ist. Teilnehmer geben Telefonnummern bereits zur Verbindungsherstellung dem Telefonanbieter heraus und verlieren spätestens zu diesem Zeitpunkt ihren Schutz.

[Rz 34] Dieser Gerichtsentscheid erlaubt es den Geheimdiensten, die Identifikationsdaten von Telefonnutzern ohne weitere Umstände abzufangen und auszulesen. Jedoch hob die US-Supreme Court Richterin Sotomayor in einem kürzlich veröffentlichten Urteil hervor, dass eine solche Interpretation angesichts der freien Herausgabe von Informationen, z.B. im Internet, nicht mehr zeitgemäss erscheine.[52] In einer kürzlich angestrengten Klage gegen die massenhafte Aufzeichnung von Metadaten wurde der Versuch unternommen, den Fall Smith v. Maryland von der heutigen Überwachung und Aufzeichnung abzugrenzen. Im Gegensatz zu heute konnte in diesem Fall die Person, welche überwacht wurde, direkt mit der Tat in Verbindung gebracht werden. Unter anderem war das Fahrzeug von Smith zweimal in der Strasse des Opfers zu sehen, Smith hatte sein Telefon bereits vorher benutzt, um sein Oper anzurufen; zudem wurden die Telefonverbindungen nur für 13 Tage aufgezeichnet und nach Abschluss des Strafverfahrens vernichtet. Ebenso konnte mit den aufgezeichneten Verbindungen nicht der Standort identifiziert werden, was heute durch die Metadaten möglich ist. Des Weiteren wurden Landleitungen und nicht Mobiltelefone wie heute überwacht. Im Lichte dieser doch grossen Unterschiede ist eine Neuinterpretation des Entscheids in dem von Senator Paul angestrengten Verfahren durchaus denkbar, was zur Einschränkung der zukünftigen Metadatenspeicherung führen könnte.[53]

[Rz 35] Derzeit ist jedoch noch unklar, welchen genauen Umfang die Verbindungsdatenaufzeichnung der Behörden in den USA aufweist. Aufgrund der im Verizon Fall[54] getroffenen geheimen Verfügung ist jedoch davon auszugehen, dass die Metadaten aller amerikanischen Telefonverbindungen durch die Geheimdienste aufgezeichnet werden. Eine Speicherung erfahren insbesondere

[50] Vgl. Website des Gerichts zu den aktuellsten Fällen; http://www.uscourts.gov/uscourts/courts/ fisc/index.html.

[51] Section 215 Patriot Act ersetzt Section 502 FISA.

[52] United States v. Jones, 565 U. S. (2012), 132 S.Ct. 945.

[53] Paul v. Obama; http://s3.amazonaws.com/freedomworks.org/files/nsa_complaint.pdf.

[54] Verfügung Nr.: 13–80 des FISC; http://www.theguardian.com/world/interactive/2013/jun/06/ verizon-telephone-data-court-order.

die Telefonnummer, der Standort, der Zeitpunkt und die Dauer des Gesprächs.

[Rz 36] Die Verfügung des Gerichts im Verizon Fall ist besorgniserregend, weil sie nicht eine bestimmte Personenidentifizierung verlangt, sondern die Metadaten aller Nutzer über einen dreimonatigen Zeitraum einschliesst. Es ist anzunehmen, dass solche Verfügungen gegen alle Mobilfunkanbieter erlassen wurden. Dianne Feinstein, Mitglied des Geheimdienstkomitees des Senats, sagte sogar öffentlich, dass die Verizon Verfügung seit 7 Jahren bestand, d.h. alle drei Monate verlängert worden sei.[55] Diese kontinuierliche Massnahme sei notwendig, um im Falle eines Terroranschlags schnell Verdächtige identifizieren zu können, was selbst durch eine Notverfügung des Gerichts nicht schnell genug geschehen könnte.[56] Laut Aussage der NSA haben lediglich 22 Personen Zugang[57] zu den Verizon Daten, jedoch hat die NSA nicht transparent gemacht, unter welchen Umständen und für welche Zwecke der Zugriff auf diese Datensätze erlaubt ist. Ebenfalls wurde kürzlich bekannt, dass ein identisches Vorgehen wie bei Verizon auch zur Abfrage von Auslandsüberweisungsdaten der Western Union zum Einsatz kam.[58]

[Rz 37] Durch eine ähnlich gelagerte Verfügung des Foreign Intelligence Surveillance Court (FISC) könnten die Geheimdienste, sobald die Kapazitäten für eine Inhaltsüberwachung geschaffen worden sind, die gesamte Kommunikation, welche auf amerikanischen Datennetzen übertragen wird, analysieren. Bereits durch die Metadaten der Verbindungen sind die Behörden in der Lage, Beziehungen zwischen Personen und deren Verhältnis zueinander zu verstehen. Die wachsenden Rechnerkapazitäten erlauben es, in Verbindung mit Hochleistungssoftware ausgeklügelte Modelle zu entwickeln, anhand derer sich Risikopersonen identifizieren lassen. Diese Personen sind dann weiteren Überwachungsmassnahmen ausgesetzt. Laut aktueller Forschung genügen vier Verbindungdatensätze (inkl. Geo-Daten), um eine individuelle Person mit 95%-iger Genauigkeit anhand dieser Daten identifizieren zu können.[59] Hinzu kommt die Möglichkeit, individuelle Merkmale in den Tagesabläufen zu erfassen, wie z.B. den Besuch der Kirche oder der Anonymen Alkoholiker.[60] Dies wird durch die Geo-Daten ermöglicht, welche zwar nicht offiziell durch die Behörden abgefragt werden, jedoch gemäss einem Berichtsentwurf des Inspektors des FBI dennoch in den übertragenen Metadaten enthalten sind.[61] Geo-Daten lassen sich dabei in zwei Kategorien einteilen, nämlich GPS Daten, welche in die Kategorie der Kommunikationsinhalte fallen, und Geo-Daten von Sendeeinrichtungen (Antennenstandorte), welche als Metadaten zu qualifizieren sind. Nur Geo-Daten der Sendeinrichtungen können gemäss der genannten Ausnahme für Metadaten

---

55 Dan Roberts/Spencer Ackerman, Anger swells after NSA phone records court order revelations, The Guardian, Friday 7 June 2013; http://www.theguardian.com/world/2013/jun/06/obama-administration-nsa-verizon-records.

56 Susan Landau, Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations, Copublished by the IEEE Computer and Reliability Societies, July/August 2013, S. 58; http://www.computer.org/cms/Computer.org/ComputingNow/pdfs/ MakingSenseFromSnowden-IEEESecurityAndPrivacy.pdf.

57 Timothy B. Lee, Here's everything we've learned about how the NSA's secret programs work, Washington Post Wonkblog, 25 June 2013; http://www.washingtonpost.com/blogs/wonkblog/ wp/2013/06/25/heres-everything-weve-learned-about-how-the-nsas-secret-programs-work.

58 Reuters, CIA spioniert Geldtransfers aus, NZZ online 15. November 2013; http://www.nzz.ch/aktuell/international/auslandnachrichten/cia-spioniert-auch-bei-geldtransfers-1.18186077.

59 Yves-Alexandre de Montjoye/César A. Hidalgo/Michel Verleysen/Vincent D. Blondel, Unique in the Crowd: The privacy bounds of human mobility, Sci. Rep. 3 (2013), S. 1–5; http://www.nature.com/srep/2013/130325/srep01376/pdf/srep01376.pdf.

60 Landau(Fn. 56), S. 57.

61 Office of the Inspector General, National Security Agency, Central Security Service, ST-09-0002 Working Draft, National Security Agency, 24 March 2009; http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection.

durch die Behörden direkt abgerufen werden.

4.1.3 Anfechtung der Datenherausgabe

[Rz 38] Seit 2006 besteht die Möglichkeit für die betroffenen Unternehmen, Herausgabeverfügungen anzufechten, wenn diese gegen ein Gesetz verstossen oder unverhältnismässig repressiv sind.[62] Das entsprechende Beschwerdeverfahren unterliegt strengster Geheimhaltung.[63] Kürzlich entschied eine kalifornische Richterin, dass die Geheimhaltung, welche ab Erhalt der Verfügung gilt, gegen die Verfassung der Vereinigten Staaten verstosse, weil sie in unangemessener Weise die freie Meinungsäusserung einschränke und das Prinzip der Gewaltenteilung unterlaufe.[64] Das FBI hat bereits Einspruch gegen das Urteil eingelegt.

[Rz 39] Im April 2013 wurde wegen eines gerichtlichen Schwärzungsfehlers die Anfechtung einer Herausgabeverfügung durch Google bekannt.[65] Es scheint somit, dass die IT-Konzerne trotz aller Schwierigkeiten versuchen, die Rechte ihrer Kunden zu schützen. Momentan sind jedenfalls mehrere Fälle beim FISC anhängig, in welchen US-Konzerne (Facebook, LinkedIn etc.) das Recht einfordern, die Öffentlichkeit über die Menge und Art der von den Behörden geforderten Datenherausgaben zu informieren.[66] Unter Auflage des Klagerückzugs wurde diesen Herausgabeanträgen kürzlich in begrenztem Umfang aussergerichtlich stattgegeben.[67]

[Rz 40] Neben der Herausgabe aufgrund einer richterlichen Verfügung hat der Gesetzgeber jedoch eine weitere sehr wichtige Zugangsmöglichkeit für die NSA geschaffen. Gemäss dem Patriot Act[68] können US-Unternehmen freiwillig und ohne Haftungsrisiko den Behörden eine direkte Verbindung zu ihren Daten gestatten. Die Behörden verhandeln in einem solchen Szenario mit den IT-Konzernen über die Modalitäten der Datenherausgabe. Aufgrund des Reputationsschadens, welcher den Unternehmen durch eine Bekanntgabe der Teilnehmer des Programms entstehen könnte, ist diese Liste als top-secret eingestuft. Presseinformationen deuten darauf hin, dass Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube und Apple an dieser freiwilligen Datenherausgabe partizipieren.

[Rz 41] Dieses, von Edward Snowden aufgedeckte, Programm wird als Special Source Operation (SSO) bezeichnet und ist Teil des grösseren PRISM Überwachungsprogramms. Es kommt nicht zur Ausstellung einer Verfügung oder zur Ausübung einer richterlichen Kontrolle, weil das Vorgehen auf freiwilliger Basis geschieht. Der Kunde des Unternehmens wird zu keinem Zeitpunkt informiert. Gemäss Statistik (Dezember 2009) finden rund 20% der amerikanischen Überwachungsmassnahmen über dieses System statt. Weitere 23% nutzen die gerichtlichen Verfügungen gemäss FISA.[69] Die zwei Programme stehen damit für fast die Hälfte der amerikanischen Über-

---

62 18 U.S.C. Section 3511 (a).

63 18 U.S.C. Section 2709.

64 In Re National Security Letters, Order No. C 11-02173 SI, U.S. District Court, Northern District of California (San Francisco); http://de.scribd.com/doc/130610269/NSL-Order.

65 Petition to Set Aside Legal Process, 13-80063, U.S. District Court, Northern District of California (San Francisco).

66 FISC, Motion for Publication of this court's decision Nr. 105B(g07-01), 14 June 2013; http://www.uscourts.gov/uscourts/courts/fisc/105b-g-07-01-motion-130614.pdf.

67 Siehe 6. Aktuelle Entwicklungen in der Überwachungspolitik.

68 Patriot Act (Fn. 46).

69 The New York Times in collaboration with Tagesanzeiger, No Morsel is too Small for U.S. National Security Agency, 11. November 2013, S. 4.

wachungsmassnahmen.

[Rz 42] Aufgrund der aktuellen Medienberichterstattung zu PRISM veröffentlichten alle grösseren IT-Unternehmen Pressemitteilungen, in denen sie eine Kenntnis der umfassenden NSA Überwachung abstritten. Diese Aussage kann sogar korrekt sein, weil meist nur ein paar Personen innerhalb eines Konzerns (u.U. nicht einmal die Geschäftsleitungsmitglieder) die notwendige «Clearance» besitzen, um Geheiminformationen über die Überwachungsprogramme zu erhalten. Indessen könnte es sich auch nur um ein Schutzargument handeln, um die Kunden zu beruhigen.

[Rz 43] Neben den auf erwähntem Abschnitt 215 des Patriot Act beruhenden Verfügungen und der freiwilligen Datenherausgabe nutzen die amerikanischen Ermittlungsbehörden (insbesondere das Federal Bureau of Investigation) sogenannte National Security Letters (NSL). Diese werden direkt von der Behörde ausgestellt und unterliegen nicht der vorangehenden Zustimmung eines Gerichts. Mit ihnen werden Metadaten, welche nicht den Übertragungsinhalt einschliessen, eingeholt. Folgt der Empfänger der Aufforderung nicht, kann das Gericht die Herausgabe verfügen (Abschnitt 115, USA Patriot Improvement and Reauthorization Act of 2005).[70]

[Rz 44] Der Inspektor des FBI hat bereits in seinem Untersuchungsbericht Rechtsverstösse in der Anwendung der NSL gerügt.[71] Aufgrund einer fehlenden Reaktion der Regierung auf diesen Bericht ist anzunehmen, dass sie nicht mit Konsequenzen aus der expansiven Rechtsauslegung rechnet.

[Rz 45] Alle verwendeten Überwachungsmethoden müssen sogenannte «minimization processes» enthalten. Sie sollen sicherstellen, dass nur die zur Überwachung notwendigen Informationen gesammelt werden. Aufgrund der bestehenden Geheimhaltung kann die Einhaltung dieser Regeln jedoch nicht geprüft werden.[72] Des Weiteren haben einflussreiche Repräsentanten (z.B. Al Gore) des US-Kongresses ihre Skepsis darüber geäussert, ob die geheime Interpretation und Rechtsanwendung des FISC mit dem vierten Verfassungszusatz vereinbar sei.[73]

[Rz 46] Journalisten unterstehen dem umfangreichen Schutz des ersten Verfassungzusatzes (freie Meinungsäusserung), welcher ihnen garantiert, dass ihre Verbindungsdaten nur auf Anordnung des Generalstaatsanwalts herausgegeben werden. Diese Schutzvorkehr wurde jedoch bereits mehrfach unterlaufen, indem das FBI die Notfallklausel des Patriot Act nutzte, um so Zugang zu den Vebindungsdaten von Journalisten der Washington Post und der New York Times zu erhalten.[74]

4.2 Auslandsüberwachung

[Rz 47] Der FISA enthält spezifische Regelungen zur Überwachung von ausländischen Parteien durch die amerikanischen Geheimdienste. Von Bedeutung ist dabei der Abschnitt 702[75], welcher

---

70 Brian T. Yeh/Charles Doyle, USA Patriot Improvement and Reauthorization Act of 2005: A Legal Analysis, S. 15; http://www.fas.org/sgp/crs/intel/RL33332.pdf.

71 Office of the Inspector General, Oversight and Review Division, A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records, US Dept. Justice, Jan. 2010; http://www.justice.gov/oig/special/s1001r.pdf.

72 Landau(Fn. 56), S. 60.

73 Suzanne Goldenberg,Al Gore: NSA's Secret Surveillance Not Really «The American Way,» Guardian, 15 June 2013; http://www.theguardian.com/world/2013/jun/14/al-gore-nsa-surveillance-unamerican.

74 Susan Landau, Canaries in the Coal Mine, Huffington Post Blog, 6 June 2013; http://www.huffingtonpost.com/susan-landau/canaries-in-the-coal-mine_1_b_3397308.html.

75 50 USC Section 1881a.

die Voraussetzungen für eine Überwachung festlegt. Unter anderem muss der FISC über die Überwachung informiert werden und diese bestätigen. Dabei sind strenge Vorgaben zur Minimierung des Risikos einer Überwachung amerikanischer Bürger einzuhalten.[76]

[Rz 48] Zusätzlich zu den genannten Zugangsmethoden, etwa durch Anzapfen von Datenströmen in den USA, betreiben die amerikanischen Geheimdienste auch aktives «Hacking». Sie verschaffen sich dabei Zugang zu geschäftlichen und privaten Computern, Tablets und Smartphones, um an Daten zu gelangen. Dieses Vorgehen wird bei Zielen ausserhalb Amerikas hauptsächlich zur Wirtschaftsspionage angewandt.[77] Im Gegensatz zu China geben die amerikanischen Behörden die gewonnenen Informationen nicht an die eigene Industrie weiter, sondern sie verwenden diese z.B. für Verhandlungen über Handelsabkommen oder das Aufdecken von Wettbewerbsverletzungen.[78] Kürzlich wurde jedoch bekannt, dass die NSA über ihren Kontakt beim australischen Geheimdienst (ASD) Informationen zu Gesprächen zwischen der indonesischen Regierung und deren Rechtsanwaltskanzlei in Chicago erhielt. Dabei ging es um den Importstop von Nelkenzigaretten sowie Shrimps durch die US-Regierung. In beiden Fällen war das Handelsvolumen jedoch gering. Dennoch verstösst eine solche Überwachung gegen das Anwaltsgeheimnis. Zumindest ist davon auszugehen, dass diese Informationen nicht der Staatsanwaltschaft zugänglich gemacht werden dürfen. Eine Verwendung der Informationen für politische und wirtschaftliche Ziele der US-Regierung ist hingegen durchaus denkbar.[79]

[Rz 49] Dem Überwachen von ausländischen Datenströmen sind nur geringe Grenzen gesetzt. Einzig wenn die Massnahmen auf amerikanischem Boden, d.h. in einem amerikanischen Serverzentrum, stattfinden, muss sichergestellt sein, dass davon keine amerikanischen Staatsbürger betroffen sind.[80] Von Bedeutung ist die Möglichkeit, Zugriff auf Daten, welche von amerikanischen Firmen gehalten werden und nicht US-Staatsbürger betreffen, zu nehmen. Dieses Vorgehen ist denkbar, weil es sich bei den Daten, welche z.B. in einer amerikanischen Cloud gespeichert sind, nicht um Daten von US-Staatsbürgern handelt. Sie unterstehen somit keinem besonderen Schutz und ein Zugriff der Behörden ist auf Basis eines Gerichtsbeschlusses möglich.[81] Dabei muss keine spezifische Person als Ziel der Massnahme identifiziert sein; vielmehr legt das Gericht Wert darauf, dass Schutzvorkehren getroffen werden, um die Überwachung amerikanischer Staatsbürger zu verhindern.[82]

[Rz 50] Gezielt werden die Klassifizierungen der NSA genutzt, um Zugang zu gewissen Daten zu erhalten. So wurde zumindest versucht, z.B. Wikileaks als «malicious foreign actor» zu qualifizieren, was die Anforderung an eine Überwachung deutlich gesenkt hätte. Als weitere Option wurde ein gezielter Angriff auf die Piratebay Plattform als Möglichkeit in Erwägung gezogen. Hierzu gab die Rechtsabteilung der NSA ihre Zustimmung. Da eine solche Plattform von vielen Nutzern täglich bedient wird, wären unweigerlich auch Daten von amerikanischen Staatsbürgern

76 50 USC Section 1881a ss 2(A).

77 The New York Times in collaboration with Tages-Anzeiger (Fn. 69), S. 4.

78 William A. Owens/Kenneth W. Dam/Herbert S. Lin, Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities, National Academies Press, Washington D.C. 2009, S. 26.

79 Ansgar Graw, NSA interessiert sich sogar für Nelken-Zigaretten, Die Welt 16. Februar 2014; http://www.welt.de/politik/ausland/article124910220/NSA-interessiert-sich-sogar-fuer-Nelken-Zigaretten.html.

80 50 USC Section 1881a s (b).

81 Foreign Intelligence Surveillance Act (FISA) Amendments Act Reauthorization Act of 2012, Section 702.

82 Edward C. Liu, Reauthorization of the FISA Amendments Act, Congressional Research Service, S. 6; http://www.fas.org/sgp/crs/intel/R42725.pdf.

betroffen gewesen. Dies wurde ohne weiteres in Kauf genommen.[83]

[Rz 51] Verschiedene Reformvorschläge sind in den letzten Monaten publiziert worden und sollen bei entsprechender Mehrheit in naher Zukunft im amerikanischen Kongress debattiert werden. Hinsichtlich der in Abschnitt 215 enthaltenen Kompetenzen existiert der Vorschlag, die Voraussetzung einer «reasonable articulable suspicion» einzuführen, welche Massenabfragen von Metadaten eingrenzen würde. Regelungen über den Datenzugriff erhöhen ebenso die Rechtssicherheit. Zudem existieren weitergehende Vorschläge, welche die Voraussetzungen für die Erteilung einer Überwachungsbewilligung durch den FISC stark erschweren. Mit hoher Wahrscheinlichkeit würden diese Änderungen das Ende des NSA Metadatenprogramms nach sich ziehen.

[Rz 52] Gemäss der Washington Post sind die im Ausland abgefangenen Daten wie z.B. E-Mails von entscheidender Bedeutung für die Lokalisation von Terroristen. So wurde z.B. der Standort einer der Führungsmitglieder der al-Qaeda durch die E-Mail seiner Frau bestimmt. Dies erlaubte es der CIA, die fragliche Person mit einem gezielten Drohnenangriff auszuschalten. Risiken ergeben sich jedoch, wenn nur ein Mobiltelefon als Ziel dient und nicht mehr die Person selbst. Unter diesen Umständen könnten spätere Besitzer des Handys durch einen Drohnenangriff, der dem eigentlichen Eigentümer galt, getötet werden.[84]

[Rz 53] Weiterhin wurde bekannt, dass die USA ein Überwachungsprogramm mit Codenamen «Mystic» entwickelt und 2011 getestet haben. Dieses erlaubt die lückenlose Aufzeichnung und Auswertung des gesamten Telefonverkehrs eines Ziellands. Gemäss der von Edward Snowden zur Verfügung gestellten Informationen wurde jedoch nur 1 Prozent der gesammelten Gesprächsaufzeichnungen tatsächlich durch Geheimdienstmitarbeiter analysiert. Der Grossteil der Daten wurde für eine eventuell spätere Verwendung archiviert.[85]

5 Bedeutung für die Schweiz

5.1 Inlandsüberwachung

[Rz 54] Im Gegensatz zur NSA besitzen die Schweizer Nachrichtendienste im Inland nur sehr begrenzte Überwachungskompetenzen. Faktisch erfolgt eine Einschränkung insbesondere durch den vergleichsweise hohen Aufwand, der mit einer Genehmigung durch das Zwangsmassnahmengericht verbunden ist. Massenabfragen bzw. ein direkter Zugang zu Unternehmensservern sind somit in der Schweiz nicht möglich, weil für jede Abfrage eine spezifische Person als Ziel zu benennen ist.

[Rz 55] Anwendungsbezogen betrachtet unterscheiden sich die inländischen Überwachungsmöglichkeiten der Schweiz und der USA sehr stark. Von Bedeutung ist insbesondere die Differenzierung zwischen Verbindungsdaten (Metadaten) und inhaltlichen Daten. In der Schweiz ist der Zugang zu Metadaten nur innerhalb von 6 Monaten mit einer spezifischen Verfügung, in welcher

[83] NSA Überwacht Besucher der feindlichen Website Wikileaks, derStandard.at 18. Febraur 2014; http://derstandard.at/1392685430788/NSA-ueberwacht-Besucher-der-feindlichen-Webseite-Wikileaks.

[84] Greg Miller/Julie Tate/Barton Gellman, Documents reveal NSA's extensive involvement in targeted killing program, Washington Post, 17. Oktober 2013; http://www.washingtonpost.com/world/ national-security/documents-reveal-nsas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc_story.html?hpid=z3.

[85] NZZ, 100-prozentige Überwachung, NZZ Nr. 66, 20 März 2014, S. 5.

der Anschluss identifiziert wird, möglich. Hingegen erlauben die USA einen fast freien Zugang der Behörden zu diesen Daten, ohne Erfordernis der Identifizierbarkeit einer bestimmten Zielperson oder einer Beschränkung der Menge der abgerufenen Metadaten. Im Gegensatz zur Schweiz wird die Speicherung der Metadaten in den USA vornehmlich durch die Geheimdienste direkt durchgeführt.

[Rz 56] Mit Bezug auf das Abfangen und Speichern von gesendeten Daten müssen in der Schweiz, wie auch den USA, entsprechende Verfügungen vorliegen, welche einer gerichtlichen Genehmigung bedürfen, die in den USA augenscheinlich ohne besonders detaillierte Prüfung erteilt wird. Anstelle des Dienstes, welcher in der Schweiz alle Überwachungsdaten entgegennimmt bzw. aufzeichnet und diese an die betroffene Behörde weiterleitet, führen in den USA die Geheimdienste die Überwachungen selbständig aus. Dadurch entfällt eine gewisse Schutzfunktion, weil keine zwischengeschaltete Partei die aufgezeichneten Daten filtert. In der Schweiz hat der Dienst die Aufgabe, vor Herausgabe eine solche Filterung (z.B. Löschung von Daten, welche dem Berufsgeheimnis unterstehen) gemäss Anweisung des Gerichts vorzunehmen.[86]

[Rz 57] Des Weiteren lässt sich in den USA eine erforderliche Genehmigung durch die freiwillige Herausgabe der gewünschten Daten umgehen. Aufgrund des Patriot Act[87] sind nämlich kooperative Unternehmen vor Klagen hinsichtlich einer derartigen Datenherausgabe geschützt. Ein solches Vorgehen steht im starken Gegensatz zur europäischen Sichtweise und dem damit verbundenen Schutz der Privatsphäre. In der Schweiz ist eine freiwillige Herausgabe verboten, weil damit der Datenschutz der betroffenen Personen ausgehöhlt würde. Einzig eine Genehmigung des Zwangsmassnahmengerichts oder die Zustimmung des Betroffenen erlauben eine Herausgabe von Daten.

5.2 Auslandsüberwachung

[Rz 58] Die Kompetenzen der amerikanischen und schweizerischen Behörden, welche mit der Auslandsüberwachung betraut sind, weisen hinsichtlich der möglichen Überwachungsmassnahmen keine grossen Unterschiede auf. Allgemein ist jede Form der Überwachung im Ausland erlaubt;[88] es gelten lediglich Ausnahmen, wenn von Beginn an bekannt ist, dass eine Massnahme gegebenenfalls zu einer Überwachung eigener Staatsbürger führt.

[Rz 59] Vermehrt identifizieren die amerikanischen Geheimdienste ausländische Personen, welche eine besondere Funktion (z.B. IT-Wartung) innerhalb eines Unternehmens ausüben und über wichtige Informationen verfügen. Durch individuelle Strategien wird der Versuch unternommen, Zugang zu deren Computern und Mobilgeräten zu erhalten. Dabei stehen oftmals nicht die Terrorismusbekämpfung, sondern allgemeine amerikanische Interessen im Vordergrund.

[Rz 60] Um diesem wachsenden Spionagepotenzial Rechnung zu tragen, sollten Schweizer Unternehmen verstärkt ihre Mitarbeitenden hinsichtlich der bestehenden Risiken schulen. Eine strenge Abgrenzung zwischen privater und geschäftlicher IT-Infrastruktur muss dabei gewährleistet sein, um Sicherheitslücken und Eindringungsmöglichkeiten einzuschränken. Der Zugang zu sensiblen Datensystemen sollte nicht durch ein wählbares Passwort erfolgen, sondern durch einen

86 Art. 13 BÜPF.

87 Patriot Act (Fn. 46).

88 Art. 14 Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit, SR 120.

externen Token Schlüssel (mit enthaltener Kodierung). Dieser hätte keine Funktion für den privaten PC und könnte in regelmässigen Abständen einfach gewechselt werden, was die Benutzung der gleichen Passwörter ausschliesst. Weiterhin sollten Personen mit weitreichender Zugangsberechtigung den Firmencomputer nicht für internetbasierende Anwendungen nutzen. Hierfür müsste ein separater Rechner mit grundlegend verschiedenem Passwort und Sicherheitssystem zur Verfügung stehen.

[Rz 61] Das Eindringen in ein fremdes Computersystem und die Sabotage dessen ist zwar in der Schweiz strafbar[89], jedoch erfolgen die Angriffe oft von den USA aus und sind kaum nachzuverfolgen. Trotz eventuellem Vorliegen einer Strafanzeige werden dadurch die Täteridentifikation und eine Bestrafung kaum möglich sein.

[Rz 62] Aufgrund der wachsenden amerikanischen Spionage haben sich die Vereinten Nationen entschlossen, eine Resolution unter Führung von Brasilien und Deutschland zu forcieren, in welcher das Recht des Einzelnen auf Privatsphäre (Menschenrecht) und dessen Einhaltung durch alle Staaten ausdrücklich statuiert wird.[90] Der Entwurf spricht sich klar gegen eine universelle Überwachung der eigenen Bevölkerung durch den Staat aus. Insbesondere im Hinblick auf die Terrorismusbekämpfung sollen zudem die Grundsätze des Völkerrechts eingehalten werden. Die entsprechende Resolution wurde kürzlich in etwas abgeschwächter Form durch die UN Vollversammlung angenommen.[91] Die amerikanische Überwachung ist in dem Entwurf nicht ausdrücklich erwähnt.

[Rz 63] Die Wirkung einer solchen Resolution wird indessen als gering eingeschätzt. Sie dient vornehmlich der politischen Zeichensetzung, wonach die gängigen Überwachungsmethoden der USA nicht länger hinnehmbar seien.

[Rz 64] Das Problem soll auch im Rahmen der Verhandlungen zwischen den EU und USA zu einem Freihandelsabkommen (Transatlantische Handels- und Investment-Partnerschaft) thematisiert werden. Jedoch hat der amerikanische Chefunterhändler Michael Froman bereits signalisiert, dass der Datenschutz kein ausdrückliches Handelsthema sei und daher unabhängig vom Freihandelsabkommen Lösungsansätze für die Datenschutzproblematik entwickelt werden müssten. Eine parlamentarische Ablehnung des Freihandelsabkommens durch einige europäische Mitgliedsstaaten ist indessen zumindest denkbar. Das kurze Zeitfenster bis zu den amerikanischen Kongresswahlen im Herbst 2014 erschwert die Verhandlungen zusätzlich.

6 Aktuelle Entwicklungen in der Überwachungspolitik

[Rz 65] Kontinuierlich veröffentlichen Journalisten die von Edward Snowden erhaltenen Dokumente zur Spionagetätigkeit der amerikanischen Geheimdienste sowie deren Verbündeten.[92] Dabei müssen die einzeln ausgesuchten Journalisten beurteilen, ob das von Snowden erhaltene Datenmaterial aufgrund eines überwiegenden Interesses der Öffentlichkeit publiziert werden soll.

[Rz 66] Eindeutig ist jedoch, dass der Umfang und die Tiefe der amerikanischen Überwachung

89 Art. 143 StGB.

90 Resolutionsentwurf A/C.3/68/L.45; http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45.

91 Sixty-eighth General Assembly, Plenary, 70th Meeting (PM); http://www.un.org/News/Press/docs//2013/ga11475.doc.htm.

92 Die verbündeten Geheimdienste der USA werden auch als «Five Eyes» bezeichnet. Dazu gehören Australien, Neuseeland, das Vereinigte Königreich, Kanada und die USA.

weit über das hinausgeht, was von einem Geheimdienst im Allgemeinen erwartet wird. Unter anderem hat die NSA nicht nur die Telefone von Staats- und Regierungschefs überwacht, sondern auch massenhaft Daten direkt an Hauptverbindungspunkten abgegriffen. Diese Daten wurden zwischengespeichert und ohne Rechtfertigungsgrund systematisch durchsucht.

[Rz 67] Noch gravierender sind die Berichte, welchen zufolge die britischen Geheimdienste ihre amerikanischen Partner darin ausbildeten, wie sie die Nutzung von Social-Media-Websites in Echtzeit verfolgen könnten. Dabei ist es wohl etablierte Praxis in den Geheimdiensten, dass der Partnerdienst eine Überwachung einer Person oder einer Kommunikationsverbindung in Fällen, in denen im eigentlichen Überwachungsland keine Rechtsgrundlage für die Überwachung existiert, übernimmt. Die so gewonnenen Informationen werden dann dem Partnerstaat im Zuge des Informationsaustausches der Geheimdienste zur Verfügung gestellt. Mit diesem Vorgehen gelingt es, die in den nationalen Gesetzen statuierte Kompetenzeinschränkung der Geheimdienste zu umgehen.

6.1 Reaktion der US-Regierung auf die NSA Affäre

[Rz 68] Aufgrund der kontroversen Berichterstattung über die Speicherung aller amerikanischen Anrufverbindungsdaten hat eine vom US-Präsidenten ins Leben gerufene Expertenkommission den Nutzen dieser Aufzeichnungen für die nationale Sicherheit untersucht. In deren Bericht wurde das Sammeln fast aller Telefondaten (Metadaten) durch die National Security Agency als gesetzeswidrig und unnütz bezeichnet. Ihre Empfehlung zur Einstellung der Datenspeicherung ist jedoch nicht bindend für den Präsidenten.[93] Weiterhin wurde in den 46 Empfehlungen der Kommission der Verzicht auf Aktionen, die private Softwareprogramme anfällig für Hackerangriffe machen, sowie die Unterstellung der NSA unter zivile Führung gefordert. Die zweite Forderung hat Präsident Obama strikt abgelehnt.[94] Jedoch haben die Internetkonzerne nun das Recht, die Zahl der Anfragen zur Datenherausgabe in Blockzahlen zu veröffentlichen. Die Zahl der Anträge lag dabei zwischen 0–999 und betraf 5'000–15'999 Nutzer-Accounts je nach Anbieter und Dienst.[95] Mit seinen über 1 Milliarde Nutzern stellt Facebooks Herausgabe von 5'000–5'999 Mitgliederprofilen jedoch lediglich einen sehr kleinen Prozentsatz der eigentlichen Nutzer dar. Hingegen erhielt Apple nur zwischen 0–249 Verfügungen des FISA Gerichts und des FBI, welche 0–249 Nutzerkonten betrafen. Im Zuge von nicht geheimdienstlichen Ermittlungsmassnahmen wurden 927 weitere Anträge gestellt, die in 81% der Fälle zur Datenherausgabe führten. Dabei handelte es sich aber um Strafermittlungen und Massnahmen, welche durch reguläre Gerichte genehmigt wurden.[96]

[Rz 69] Im amerikanischen Senat regt sich allmählich Widerstand gegen die US-Überwachungsprogramme. Dies ist u.a. bedingt durch Senatorin Feinsteins Aussage, die CIA habe vorsätzlich Unterlagen dem Sicherheitskomitee vorenthalten und behindere dessen Arbeit. Hingegen vertritt der CIA Direktor John Brennan öffentlich die Meinung, dass die aufgedeckten Spionagetätigkeiten nicht den Umfang angenommen hätten welcher allgemeinhin angenommen würde. Weiterhin müsse

93 Weitere kritische Stimme zur NSA, NZZ Nr. 19, 24. Januar 2014, S. 6.

94 Vgl. Peter Winkler, Für engere Grenzen beim staatlichen Datensammeln, NZZ Nr. 296, 20. Dezember 2013, S. 3.

95 Vgl. Daten zu Anfragen der US-Geheimdienste, NZZ Nr. 29, 5. Februar 2014, S. 6.

96 Apples Statement ist abrufbar unter: http://www.apple.com/pr/pdf/140127upd_ nat_sec_and_law_enf_orders.pdf.

die Arbeit der Geheimdienstmitarbeiter gewürdigt und nicht durch unbedachte Aussagen diskreditiert werden.[97]

[Rz 70] Von politischer Seite verstärkt auch die Opposition in den USA ihren Druck auf die Regierung mit dem Ziel, die Überwachung einzugrenzen. Unter anderem hat z.B. Senator Rand Paul kürzlich eine Klage auf Unterlassung gegen Obama und die Leiter des FBI und der NSA eingeleitet.[98] Eine direkte Anzeige der Führungskräfte ist notwendig, weil aufgrund der US-Verfassung eine Klage gegen die Institutionen selbst unter Umständen nicht möglich ist. Jedoch können die Verantwortlichen in den Institutionen direkt verklagt werden, um eine Änderung der Praxis zu erreichen.[99]

6.2 Reformbemühungen der USA

[Rz 71] In seiner Rede zur Reform der Geheimdienste hat der US-Präsident die zentralen Forderungen der Expertenkommission nicht im Detail angesprochen. Metadaten von Telefongesprächen sollen zukünftig indessen nicht bei der Überwachungsbehörde, sondern beim Telekommunikationsanbieter vor Ort lagern und nur auf Anfrage herausgegeben werden.[100] Gemäss Meinung des Weissen Hauses sind Metadaten weiterhin notwendig, um Terroranschläge zu verhindern; so wäre es z.B. möglich gewesen, den Anruf des 9/11 Attentäters zu einer bekannten Zelle in Jemen festzustellen und entsprechende Schlüsse zu ziehen. Diese Einschätzung steht jedoch im Gegensatz zur Beurteilung der Kommission, welche die Effektivität der Datenaufzeichnung untersuchte.

[Rz 72] Die nun neu geschaffene Direktive des Präsidenten (Executive Order) zur Arbeit der Geheimdienste hat zum Ziel, die angespannte Beziehung zu den europäischen Partnerstaaten zu verbessern. Inhaltlich verspricht sie kaum Neuerungen. In Bezug auf das Ausspionieren von Nichtamerikanern wurde der Geheimdienstkoordinator angewiesen, zumindest eine teilweise Gleichbehandlung mit den amerikanischen Bürgern sicherzustellen. Was dies in der Praxis bedeutet, ist jedoch offen.[101] Weil es sich bei der Anweisung nur um eine Direktive handelt, kann diese vom Präsidenten oder dessen Nachfolgern jederzeit wieder geändert werden. Rechtssicherheit fehlt somit weiterhin.

[Rz 73] Kürzlich ist immerhin zur Überwachung der Arbeit der NSA die Stelle einer Datenschutzbeauftragten innerhalb des Geheimdienstes geschaffen und mit Rebecca Richards besetzt worden: Sie soll zwar die datenschutzkonforme Ausführung der NSA-Tätigkeiten überwachen; dennoch ist sie an bestehende Kontrollsysteme und Regeln gebunden.[102] Die Effektivität ihrer Tätigkeit ist damit von Anfang an in Frage gestellt.

[Rz 74] Die von Obama vorgeschlagene Übergabe von Kompetenzen an private Anbieter würde überdies ohne entsprechende Rekursmöglichkeiten der Betroffenen zu weiteren Problemen

---

97 The Economist, Di-spy, 15. März 2014, S. 38.

98 Die Klage ist abrufbar unter: http://s3.amazonaws.com/freedomworks.org/ files/nsa_complaint.pdf.

99 Republikanischer Senator verklagt Obama wegen NSA-Affäre, Tages-Anzeiger 13. Februar 2014; http://www.tagesanzeiger.ch/ausland/amerika/Republikanischer-Senator-verklagt-Obama-wegen-NSAAffaere/story/14011918.

100 David Hesse, Obama verteidigt das Ziel und ändert den Weg, Tages-Anzeiger, 18. Januar 2014, S. 9.

101 Peter Winkler, Obama skizziert Reformen für die NSA, NZZ Nr. 14, 18. Januar 2014, S. 3.

102 Tobias Bühlmann, NSA erhält eine Datenschützerin, NZZ Nr. 24, 30. Januar 2014, S. 24.

führen, etwa wenn die Telekommunikationsanbieter staatliche Funktionen ausüben, gleichzeitig aber nicht denselben Pflichten wie der Staat unterliegen und zum Teil gegenläufige wirtschaftliche Interessen haben.[103]

[Rz 75] Im Vergleich zur Kommunikation anderer international tätiger Geheimdienste stellt die Direktive jedoch die am weitest gehende Stellungnahme zu nationalen Überwachungskompetenzen dar, welche im öffentlichen Raum verfügbar ist. Die Direktive lässt sich deshalb als Beginn eines Prozesses sehen, der zu einer breiten gesellschaftlichen Debatte über die grundlegenden Rechte der Bürger auf Privatsphäre und der Notwendigkeit staatlicher Überwachung führt. Bereits 2012 veröffentlichte die US-Regierung zudem einen Entwurf für ein Datenschutzgesetz, welches bis anhin das wohl umfangreichste seiner Art gewesen wäre. Aufgrund des Lobbyismus der Internet- und Telekommunikationsfirmen hat der Kongress das Gesetz bisher jedoch nicht verabschiedet.[104]

6.3 Auswirkungen auf die US-Wirtschaft und -Medien

[Rz 76] Die wirtschaftlichen Einbussen durch geringere Bestellungen amerikanischer IT Hardware und Software tragen ihren Teil zum Umdenken in den USA bei.[105] Die Realität zeigt jedoch auch, dass die Kapazitäten der USA im Bereich der Spionage den europäischen Geheimdiensten weit voraus sind. Zum Teil wird Hardware direkt beim Hersteller abgefangen und mit winzigsten Schaltkreisen ergänzt, welche dann den Zugang über einen Funksender erlauben. Diese Technik soll unter anderem auch bei iranischen Zentrifugen eingesetzt worden sein.[106] Sie wird durch die Spezialeinheit Advanced Network Technology bereitgestellt und nützt z.B. Lücken in der Windows Umgebung (z.B. die Problemberichte an Microsoft) aus, um sich passiv Zugriff zu den Rechnern zu verschaffen.[107] Es fehlt somit aufgrund der bestehenden nachrichtendienstlichen Abhängigkeit ein geeignetes Druckmittel gegenüber den USA. Hinzu kommt, dass eine propagierte Aussetzung des Freihandelsabkommens mit der EU wenig effektiv erscheint, weil mehrheitlich die EU von einem solchen Handelsabkommen profitieren würde.[108] Vielmehr sind es die Beschwerden der US-Konzernchefs, die ein Umdenken in der US-Administration bewirken können.[109]

[Rz 77] Ein weiterer zentraler Punkt ist die potenzielle Überwachung der Presse in den USA. Gemäss einer im Oktober 2013 durchgeführten Studie unter US-Schriftstellern sind 85% besorgt über die Intensität der amerikanischen Überwachung. Insbesondere bei sensiblen Recherchen zu heiklen Themen, die eine öffentliche Kritik an der Regierung enthalten, ist grösste Vorsicht geboten. So kontaktieren diese Schriftsteller ihre Informanten nicht mehr telefonisch oder per E-Mail, sondern treffen sie wie zu Sowjet-Zeiten an öffentlichen Orten. Ebenso sagen 40% aus, dass sie ihre Präsenz im Internet eingeschränkt haben und nicht mehr mit bestimmten Personen

[103] New rules for spooks, The Economist, 25. Januar 2014, S. 33.

[104] Christof Münger, Als Obama noch ein Datenschützer war, Tages-Anzeiger, 17. Januar 2014, S. 7.

[105] Walter Niederberger, Internet-Riesen wehren sich gegen Massenspionage, Tages-Anzeiger, 10. Dezember 2013, S. 41.

[106] Peter Winkler, Die NSA kann Computer auch offline ausspähen, NZZ Nr. 12, 16. Januar 2014, S. 3.

[107] Vgl. Martin Kilian, Tages-Anzeiger 31. Dezember 2013, S. 9.

[108] Joachim Riecker, Empörung und Ratlosigkeit, NZZ Nr. 13, 17. Januar 2014, S. 3.

[109] David Hesse, Bei aller Freundschaft, Tages-Anzeiger, 17. Januar 2014, S. 6.

kommunizieren.[110] Diese Entwicklung ist im Lichte der Meinungsfreiheit äusserst bedenklich.

6.4 Reaktion der EU auf die NSA Affäre

[Rz 78] Vermehrt wird die Anpassung der EU-Datenschutzbestimmungen im Datentransfer zu den USA gefordert. Im Einzelnen geht es dabei um die Selbstverpflichtungen, welche die amerikanischen Unternehmen freiwillig unter dem Safe Harbor Abkommen eingehen. Aufgrund der inadäquaten Kontrolle des US-Handelsministeriums sollen die Aufsichtsmechanismen verschärft und bei Verstössen den Bürgern in Europa die Möglichkeit zur Klage vor amerikanischen Gerichten eingeräumt werden.[111]

[Rz 79] In gewisser Hinsicht stehen die Aussagen der EU-Repräsentanten im Gegensatz zu deren Handlungen. So fordern EU-Vertreter z.B. die Abschaffung der Massendatensammlung, doch halten sie am SWIFT Abkommen weiterhin fest. Die EU-Innenkommissarin Malmström ist der Meinung, dass die Verfolgung der Terrorfinanzierung nicht durch ein eigenes EU-System erfolgen könne, weil dadurch neue Datenschutzprobleme kreiert würden.[112] Mit diesem Vorgehen wird jedoch die Abhängigkeit zu den USA mit deren oftmals nicht datenschutzkonformen Überwachungsmassnahmen in Kauf genommen.

[Rz 80] In Europa werden vermehrt Stimmen laut, welche für ein «europäisches Internet» plädieren.[113] Diese verkennen jedoch die technischen Gegebenheiten des Internets, welche gerade darauf abstellen, die Daten durch die schnellstmögliche Verbindung zu routen. Eine Anpassung der europäischen Netze mit dem Ziel, den innereuropäischen Datenversand nur über Verbindungen in der EU zu routen, ist denkbar, würde aber einen grossen Eingriff in die Struktur und die Neutralität des Internets darstellen. Die Nutzung von Apps auf Mobiltelefonen, welche zu den US-Servern ihrer Anbieter Verbindung halten, senden ständig Informationen. Die US-Geheimdienste verwenden diesen Umstand, um Standort, Tagesplanung und Adresslisten auszuspionieren. Eine europäische Cloud würde hier keine Lösung bieten. Einzig technische Möglichkeiten, welche die Zugriffsrechte der Apps beschränken, sind hier eine denkbare Lösung.[114]

[Rz 81] Die Einhaltung von EU-Datenschutzstandards durch private Unternehmen wie Google wird zurzeit von diesen nicht ausreichend ernst genommen. Ausschlaggebend sind dafür die geringen Strafen, welche auferlegt werden können. So musste Google erst kürzlich die Maximalstrafe in Frankreich wegen der Überwachung ihrer Nutzer in der Höhe von 150'000 Euro bezahlen. Dies schien Google jedoch angesichts eines Geschäftsgewinns im Milliardenbereich nicht zu stören.[115] Immerhin formt sich ein gewisser Widerstand gegen die exzessive Datennutzung. In Kalifornien wurde kürzlich eine Klage gegen Facebook eingereicht, welche das automatische Auslesen der als «Private Mails» bezeichneten Kommunikation zwischen den Nutzern rügt. Gefordert werden dabei sehr hohe Schadenersatzbeträge von bis zu 10'000 US Dollar pro Verstoss.[116] Die EU ist

[110] Vgl. hierzu den Pen Report: http://www.pen.org/sites/default/files/Chilling%20 Effects_PEN%20American.pdf.

[111] Sarah Nowotny, Schweiz will US-Spionage bekämpfen, NZZ am Sonntag, 1. Dezember 2013, S. 15.

[112] Niklaus Nuspliger, Die EU verlangt mehr Datenschutz in den USA, NZZ Nr. 277, 28. November 2013, S. 5.

[113] Vgl. Aussage von Verkehrs- und Internetminister Alexander Dobrindt und Wolfgang Bosbach in: David Nauer, Deutschland ist verärgert über die sturen US-Spione, Tages-Anzeiger 16. Januar 2013, S. 7.

[114] Vgl. Peter Winkler, NZZ Nr. 23, 29. Januar 2014, S. 3.

[115] Vgl. Tages-Anzeiger 9. Januar 2014, S. 39.

[116] Die Klage ist abrufbar unter: http://docs.justia.com/cases/federal/district-courts/california/candce/5:2013cv05996/

sich der Datenschutzproblematik bewusst und sieht im Entwurf einer neuen Datenschutzgrundverordnung nun Strafen von bis zu 2% des jährlichen Umsatzes eines Unternehmens vor.

[Rz 82] Auf europäischer Seite wird als Konsequenz der US-Überwachung die Arbeit der nationalen Geheimdienste verstärkt. So hat es sich Deutschland auf die Fahnen geschrieben, nun auch seine Freunde einer «Sockelüberwachung» zu unterziehen und seine Kompetenzen in der Spionageabwehr auszubauen.[117] Auch private Unternehmen in Europa rüsten sich gegen Spionage und IT Sicherheitsrisiken. So hat sich das Budget der Unternehmen im Bereich IT Sicherheit seit Bekanntwerden der Snowden Affäre um 50% erhöht. Auch die Universitäten und Hochschulen reagieren auf die steigende Nachfrage, indem sie neue Abschlüsse und Spezialisierungen anbieten, wie z.B. das Fach IT Sicherheit und Hacking an der ETH Zürich.[118]

[Rz 83] Von gesellschaftlicher Seite sollte eine verstärkte Auseinandersetzung mit dem Thema Datennutzung stattfinden. Zukünftig muss insbesondere in der Bevölkerung ein Bewusstsein für den Umgang, Nutzung und zur Verfügung Stellung von Informationen geschaffen werden.[119]

[Rz 84] Der Gerichtshof der Europäischen Union (EuGH) hat mit seinem Entscheid die Richtlinie über die Vorratsspeicherung von Daten für ungültig zu erklären der grenzenlosen Verbindungsdatenaufzeichnung in der EU einen Riegel vorgeschoben. Unter anderem rügten die Richter das fehlende Erfordernis die gesammelten Daten in der EU zu speichern sowie die Unverhältnismässigkeit der Richtlinie.[120]

7 Fazit für Schweizer Unternehmen und Privatpersonen

[Rz 85] Schweizer Unternehmen und Privatpersonen müssen sich der Tatsache bewusst sein, dass alle Daten, die in die USA gesendet oder über die USA geleitet werden, von den amerikanischen Behörden abrufbar sind. Dies gilt insbesondere für die vermehrt genutzten Cloud Lösungen, welche sich oftmals amerikanischer Server bedienen. Hat der Cloud-Anbieter seinen Serverstandort in Europa, ist dennoch eine Überwachungsmöglichkeit nicht auszuschliessen, wenn es sich um ein amerikanisches Unternehmen handelt, weil dieses auch zur Herausgabe von Daten verpflichtet ist, die auf ausländischen Servern lagern.[121]

[Rz 86] Die im Jahr 2011 beschlossene Auslagerung des Kommunikationsnetzes des Bundes an private Anbieter sollte mit Blick auf die Informationssicherheit nochmals genau evaluiert werden. Insbesondere sind die Sicherheitsstandards regelmässig zu prüfen und eine lückenlose Verschlüsselung sicherzustellen. Ob die angestrebten Kosteneinsparungen gegenüber dem Eigenbetrieb des Bundes erreicht werden können ist aufgrund der erhöhten Sicherheitsanforderungen

273216/1; Vgl. Matthias Huber, Nutzer verklagen Facebook, Tages-Anzeiger 4. Januar 2014, S. 41.

[117] NSA-Affäre: Regierung plant Einsatz von Spionageabwehr gegen die USA, Spiegel Online 16. Februar 2014; http://www.spiegel.de/politik/deutschland/nsa-affaere-regierung-plant-einsatz-von-spionageabwehr-gegen-usa-a-953734.html.

[118] Wie aus Studenten Hacker werden, FAZ Online 13. Februar 2014; http://www.faz.net/aktuell/ berufchance/arbeitswelt/it-spezialisten-wie-aus-studenten-hacker-werden-12800228.html.

[119] Ahti Saarenpää, Openess, Access, Interoperability and Surveillance: Transparency in the New Digital Network Society, in: Erich Schweighofer/Franz Kummer/Walter Hötzendorfer (Hrsg.), Transparenz, IRIS 2014, S. 246; abrufbar unter: http://jusletter-eu.weblaw.ch/issues/2014/ IRIS/2517.html.

[120] EuGH C-293/12 und C-594/12, Pressemitteilung Nr. 54/14 vom 8. April 2014, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054de.pdf.

[121] Patriot Act (Fn. 46).

fraglich.[122]

[Rz 87] Weiter verbleibt das Risiko der Installation von «Hintertüren» in amerikanischer IT-Hardware, welche auch in Schweizer Serverzentren zur Anwendung kommt.[123] «Hintertüren» sind Zugangsmechanismen in Form von Programmierungen, welche zum Betrieb der Hardware notwendig sind. Sie ermöglichen es, unabhängig vom Standort des Servers Zugriff auf die gespeicherten Serverdaten zu nehmen bzw. entsprechende Überwachungsprogramme einzuschleusen. Aufgrund der Komplexität der Hardware sind sie nur sehr schwer zu entdecken.

[Rz 88] Die Aufdeckung der amerikanischen Überwachung hat bereits durch sinkende Umsätze Auswirkungen auf die führenden US-Hardwareanbieter gezeitigt. Deren Marktanteil weltweit soll gemäss Schätzungen der Information Technology & Innovation Foundation bis 2016 um 20% zurückgehen.[124] Als Hauptgrund hierfür gilt die zunehmende internationale Skepsis gegenüber der weltweit grössten Volkswirtschaft.[125] Für die europäischen und asiatischen Anbieter stellt die aktuelle Lage eine ideale Möglichkeit dar, ihre neuen Produkte (Cloud/Internet of Things) in diesen Regionen zu etablieren und damit der amerikanischen Konkurrenz wichtige Marktanteile abzunehmen.

[Rz 89] Schweizer IT-Unternehmen können Schutzmassnahmen ergreifen, um die Zugriffsmöglichkeiten von Dritten zu minimieren. Unter anderem sollten nur Server innerhalb Europas, welche europäische Anbieter betreiben, genutzt werden. Des Weiteren wäre in Betracht zu ziehen, alle Datentransfers mit einer eigenen speziellen Software zu verschlüsseln. Die von Snowden initiierten Veröffentlichungen zeigten, dass die Verschlüsselung der grossen Kommunikationsanbieter in diesem Bereich unzureichend ist und dass die Unternehmen selbst für die entsprechende Verschlüsselung sorgen müssen. Würden IT-Unternehmen entsprechende Vorkehren treffen, könnten sie durch dieses Vorgehen es den Behörden erschweren, die gesendeten Daten auszulesen. Schwachstelle bleiben zwar der Empfänger und der Sender der Daten, weil dort die entsprechenden Schlüssel zum Dekodieren gespeichert sind. An diesen Punkten wären weiterhin strenge Sicherheitsmassnahmen einzurichten, um zu verhindern, dass der Schlüssel in die falschen Hände gelangt. Ein Versand der Daten über die USA bzw. die Weitergabe lässt sich kaum verhindern, weil die Datenströme im Internet eigenen Regeln folgen. Durch die Verschlüsselung wird aber erreicht, dass die abgefangenen Daten für die Behörden unbrauchbar sind.

[Rz 90] Unternehmen, wie auch Private, müssen genau abwägen, welche Daten sie der amerikanischen Infrastruktur bzw. dem Zugriff der US-Behörden unterstellen wollen. Weil vornehmlich alle sogenannten Social Media Sites (z.B. Facebook, Twitter, LindedIn) von US-Unternehmen betrieben werden, ist damit zu rechnen, dass die Daten auf deren Servern unter Umständen den Behörden zur Verfügung stehen.

[Rz 91] Neben den hardwareseitigen Vorkehren ist auch dem Nutzer die Verschlüsselung seiner Daten zu empfehlen. Dies lässt sich verhältnismässig einfach durch ein Programm (z.B. PGP) realisieren. Die Kosten hierfür sind minimal (ca. 50–100 CHF p.a.)[126], erlauben aber einen ver-

[122] Fabian Baumgartner, Riskanter Poker um das Datennetz des Bundes, NZZ 13. November 2013, S. 11.

[123] Marco Metzler, Schweizer Daten-Zentren boomen, NZZ am Sonntag 10. November 2013, S. 33.

[124] Matthew Schofield, U.S. share of cloud computing likely to drop after NSA revelations, Miami Herald online 12. Februar 2014; http://www.miamiherald.com/2014/02/12/3927603/us-share-of-cloud-computing-likely.html.

[125] Christiane Hanna Henkel, Amerikas Technologiekonzerne leiden unter der Spionageaffäre, NZZ Nr. 266, 15. November 2013, S. 23.

[126] Eric Gujer, Kein Stacheldraht im Internet, NZZ Nr. 267, 16. November 2013, S. 1.

gleichsweise sicheren Schutz vor dem Zugriff Dritter. Generell kann jede Verschlüsselung geknackt werden, die dazu nötigen Ressourcen sind jedoch, selbst für die NSA, begrenzt. Je mehr Nutzer ihre Daten verschlüsseln, desto schwieriger wird es für die Behörden, die Daten mit den vorhandenen Ressourcen zu entschlüsseln.

[Rz 92] In Anbetracht der in den USA erlaubten freiwilligen Datenherausgabe ist es fraglich, ob die amerikanischen Unternehmen, welche dem Safe Harbor Abkommen (mit der Schweiz und mit der Europäischen Union) beigetreten sind, den von der Schweiz und der EU geforderten Mindestschutz einhalten. Eine Herausgabe von Daten untergräbt die Grundprinzipien des DSG[127] und lässt sich nicht mit dessen Ziel, nämlich dem Schutz von persönlichen Daten, in Einklang bringen. Des Weiteren sind die Möglichkeiten der amerikanischen Behörden zur Einsichtnahme viel zu umfangreich, um noch in einem adäquaten Verhältnis zur Gefahrenabwehr und zum Privatsphärenschutz zu stehen. Auf die Daten ausländischer Parteien vermögen sie fast uneingeschränkt Zugriff zu nehmen.

[Rz 93] Der Schweizer Gesetzgebung unterliegende Unternehmen, welche von der revidierten Definition des Art. 2 BÜPF (Entwurf) erfasst sind, müssen künftig in der Lage sein, Kommunikationsdaten an den Dienst zu liefern. Unter anderem sind dabei auch die längeren Aufbewahrungsfristen von Nutzerinformationen zu beachten. Aufgrund des Aufkommens weiterer Überwachungsmassnahmen wie z.B. GovWare ist mit zusätzlichen technischen Herausforderungen hinsichtlich der bereitzustellenden Infrastruktur zu rechnen.

[Rz 94] Als problematisch erscheint, dass die Schweizer Behörden aufgrund fehlender Kapazitäten im IT-Markt auf externe Dienstleister aus dem Ausland angewiesen sind. Dies birgt die Gefahr, dass die zumeist amerikanischen Unternehmen wie z.B. die international tätige Computer Science Corporation (CSC) Zugriff auf sensible Schweizer Daten erhalten. Eine mögliche Weitergabe von Informationen an die NSA, welche Hauptkunde der CSC ist, kann nicht ausgeschlossen werden.[128]

Prof. Dr. iur. Rolf H. Weber ist Ordinarius für Privat-, Wirtschafts- und Europarecht an der Universität Zürich, Visiting Professor an der Hong Kong University und praktizierender Rechtsanwalt in Zürich.
MLaw Dominic N. Staiger ist Assistent und Doktorand am Lehrstuhl von Prof. Rolf H. Weber an der Universität Zürich und als Attorney-at-law im Bundesstaat New York (USA) zugelassen.
Ein erster Aufsatz zu diesem Thema wurde in Jusletter veröffentlicht (vgl.: Rolf H. Weber / Dominic N. Staiger, Datenüberwachung in der Schweiz und den USA, in: Jusletter 25. November 2013); der vorliegende Beitrag führt die Diskussion unter Berücksichtigung der neueren Entwicklungen weiter.

---

[127] Art. 1 Bundesgesetz über den Datenschutz, SR 235.1.

[128] Fabian Eberhard, Zudienerin der NSA arbeitet auch für den Bund, Tages-Anzeiger, Freitag 22. November 2013, S. 3.