FAQ-Liste zu Sicherheit und Unsicherheit im Internet

eines Arbeitskreises der Gesellschaft für Informatik e.V. (GI)

2. September 2013, Version 1.0

Inhalt

2. September 2013, Version 1.0

FAQ zu Sicherheit und Unsicherheit im Internet

Vorbemerkung

Die Offenlegungen des früheren NSA-Mitarbeiters Edward Snowden haben Politik und Gesellschaft anscheinend aus einem Dämmerschlaf gerissen. Plötzlich wird vielen Menschen bewusst, in welchem Maße Nachrichtendienste die technischen Errungenschaften der Informatik zur Terror- und Verbrechensbekämpfung einsetzen und wie rasch solche Eingriffe des Staates zur Gewährleistung von Sicherheit die Persönlichkeitsrechte des Einzelnen und die Privatsphäre gefährden können.

Die politische Bedeutung des Themas erschwert eine sachliche Diskussion, berührt sie doch die Grundlagen unseres Lebens im digitalen Zeitalter. Daher sehen sich Mitglieder der Gesellschaft für Informatik veranlasst, dem interessierten Bürger und verantwortungsbewussten Informatiker Hintergrundinformationen zum Kontext der IT-gestützten Ausspähung bereitzustellen. Im Fokus stehen dabei folgende Leitfragen:

- Wer überwacht wie und in welchem Maße unsere Kommunikation?
- Wer dringt wie und in welchem Maße in unsere Computer ein?
- Auf welcher rechtlichen Grundlage geschieht dies?
- Wie können wir uns davor schützen?

Wir nähern uns diesen Leitfragen mit einer Sammlung von fast 40 detaillierteren Fragen und Antworten, die wir in vier Rubriken eingeteilt haben: Neben allgemeinen und politischen Fragen stehen technische und ökonomische sowie rechtliche. Eine Rubrik mit Fragen zur möglichen Abwehr rundet die FAQ-Liste ab.

Wir nehmen sachlich zu den Fragen Stellung und belegen dort, wo es uns möglich ist, unsere Aussagen mit Fakten. Allein aus der Tatsache, dass Geheimdienste in der Regel im Geheimen agieren, lässt sich aber ableiten, dass wir an manchen Stellen auch den Mut haben müssen, vor dem Hintergrund unserer fachlichen Kompetenz Einschätzungen zu treffen. Diese kennzeichnen wir aber auch als solche. In einer späteren Ausgabe lassen sich manche der Annahmen möglicherweise noch konkretisieren.

Zu den verwendeten Begrifflichkeiten noch so viel: Viele sprechen angesichts der aktuellen Enthüllungen von einem „Abhörskandal“. Wir halten das Wort „abhören“ im Zusammenhang mit der erlaubten oder unerlaubten Speicherung digitaler Informationen und der algorithmischen Suche nach Schlüsselworten für verharmlosend, suggeriert es doch, dass ein menschliches Wesen synchron mithört, also einen Vorgang, der Missbrauch im ganz großen Stil gar nicht zulässt. Wir verwenden stattdessen den Begriff des Ausspähens von Daten. Des Weite-

2. September 2013, Version 1.0

ren verwenden wir die Begriffe „Nachrichtendienst“ und „Geheimdienst“ synonym. Während „Nachrichtendienst“ der korrekte Begriff ist, wird in den Medien meist von „Geheimdienst“ gesprochen. Gemeint sind Behörden, die im In- oder Ausland Aufklärung für die Sicherheit des Staates oder andere staatliche Ziele (z.B. Förderung der heimischen Wirtschaft) betreiben und dazu u.a. mit nachrichtendienstlichen Mitteln arbeiten, d.h. im Verborgenen Informationen sammeln und auswerten. Ihr Auftrag ist von Land zu Land sehr unterschiedlich und kann sich auch auf die Sammlung wirtschaftsbezogener Informationen erstrecken.

Kommentare und Rückfragen sind willkommen. Gerne per E-Mail an cornelia.winter@gi.de.

Redaktionsteam: Rudolf Bayer, Albert Endres, Hannes Federrath, Herbert Fiedler, Oliver Günther, Agata Królikowski, Peter Löhr, Hartmut Pohl, Kai Rannenberg, Helmut Redeker, Simone Rehm (Leitung), Alexander Roßnagel, Joachim Schrey, Gerhard Weck, Ernst-Oliver Wilhelm, Cornelia Winter

2. September 2013, Version 1.0

A. Allgemeine und politische Fragen

A 1: Wie und wo erfolgt staatlicherseits die Ausspähung und welche Staaten sind aktiv?

Ob Seekabel, Überlandkabel, Richtfunk oder Satellit - all diese Verkehrswege können mit geeigneten technischen Einrichtungen angezapft und laufend überwacht werden. Auch wenn derzeit insbesondere der amerikanische und britische Geheimdienst ins Visier der Medien geraten sind, gehen wir davon aus, dass im Prinzip alle Länder, die einen Geheimdienst betreiben, solche Einrichtungen zur Nachrichtenbeschaffung nutzen. Dies sind neben großen Ländern wie z.B. den USA, Russland und der Volksrepublik China auch kleine Länder wie z. B. die Niederlande und Luxemburg.

Was heißt das für uns? Deutsche Unternehmen, die Daten (z.B. Konstruktions- oder Vertriebsdaten) über das Internet an Tochterunternehmen oder Filialen im Ausland versenden und dort verarbeiten lassen, müssen ebenso mit Überwachung rechnen wie deutsche Bürger, die international kommunizieren. Dasselbe gilt auch in der umgekehrten Richtung. Überwacht werden, so muss man befürchten, nicht nur die Verkehrswege, sondern auch die Server von Telekommunikationsanbietern und den Betreibern sozialer Netze.

A 2: Was wird ausgespäht?

Das 2001 vom Europaparlament nachgewiesene, weltweit eingesetzte Abhörsystem ECHELON wird seit ca. 1970 betrieben und dient der Überwachung von Satellitenkommunikation. Mit den jetzt aufgedeckten Spähprogrammen wie PRISM und Tempora lässt sich auch drahtgestützte Kommunikation flächendeckend ausspähen. Nutzerdaten können in Echtzeit abgegriffen, gesammelt und später zusammengeführt werden. Geräte, die über das Internet erreichbar sind wie z.B. Telefon, Handy, Fax, Kopierer und Scanner, können ebenso ausgespäht werden wie Internetdienste. Dies können Dienste für Video-Konferenzen sein, Internet-Mail und Dateiaustausch über das Netz, Social Media, Video- und Bilddienste, YouTube, Cloud-Dienste oder finanzielle Transaktionsdienste (SWIFT). Betroffene Daten sind u.a. Kreditkartendaten, Fluggastdaten, Passwörter oder URLs besuchter Webseiten, mit dem jeweiligen Aufenthaltsort des Handelnden sowie Datum und Uhrzeit der Aktivitäten. Das Ausspähen solcher Geräte und Dienste fällt technisch leicht, weil die analoge Datenübertragung zunehmend der digitalen weicht und immer öfter das Internet-Protokoll (IP) verwendet wird. Technisch aufwändiger ist – nicht nur aufgrund der schieren Datenmenge – die Analyse und das Zusammenführen der Daten.

A 3: Was geschieht mit den ausgespähten Daten?

Auch wenn es monströs erscheint, die technischen Mittel lassen zu, dass weltweit die digitale Kommunikation überwacht wird. Das heißt, dass sich Kommunikationsvorgänge im Inter-

net aufzeichnen lassen, und die Verbindungsdaten, d.h. Datum, Sender- und Empfängerdaten sowie Lokationsdaten gespeichert werden können. Dies ist insofern unmittelbar einleuchtend, da diese Verbindungsdaten zum Aufbau der Kommunikationsverbindung notwendig sind und daher in der Kommunikation enthalten sein müssen. In welchem Umfang dies tatsächlich geschieht und inwiefern diese Verbindungsdaten danach auch gezielt ausgewertet werden, entzieht sich unserer Kenntnis. Unbestritten ist, dass dies geschehen kann und offenbar in viel stärkerem Maße geschieht als bisher angenommen – und zwar abhängig von der jeweiligen Bedarfslage legitimiert oder auch nicht legitimiert. Die Inhalte der Kommunikation können ebenfalls gescannt und abgefangen bzw. gespeichert werden, wobei eine komplette anlasslose Speicherung und Aufbewahrung von Verbindungsdaten und Inhalten sehr kostenintensiv ist und nicht nur in Deutschland auch gegen geltendes Recht verstößt (Stichwort: Vorratsdatenspeicherung). Sind Daten allerdings erst einmal aufgezeichnet, lassen sie sich auch einfach manipulieren: man kann sie löschen, unkenntlich machen oder inhaltlich verändern. Dies alles fällt unter den Tatbestand der Sabotage.

Langfristig lassen sich auch Jahre und Jahrzehnte zurückliegende Aktivitäten aus gespeicherten Daten bei Bedarf in einem einzigen Dossier zusammenfassen. Dies lässt sich nicht verhindern, selbst Verschlüsselung kann gebrochen werden (z.B. SSL, TLS, S/MIME, Skype).

A 4: Ist das Ausspähen durch eigene Geheimdienste (oder die befreundeter Staaten) die einzige oder größte Bedrohung im Netz? An welche anderen Gefahren muss der Nutzer denken?

Es gibt eine Vielzahl von Gefahren, die oft erheblich mehr Schaden anrichten können als das Ausspähen. Denn es gibt kaum eine Straftat, die heute nicht im Internet ihre eigene Ausprägung gefunden hat. Das gilt für Diebstahl, Betrug und Erpressung ebenso wie für Drogenhandel, Päderastie und Kinder-Pornografie. Außer den Ausspähungen befreundeter Geheimdienste müssen Nutzer mit Aktionen rivalisierender Länder, diverser Kleinkrimineller, konkurrierender Unternehmen oder der organisierten Kriminalität (z.B. Mafia, Drogenkartelle) rechnen. Je wertvoller ein Inhalt im Netz, umso größer ist das Interesse daran. Der Wert hängt wiederum von der Stellung einer Person oder der Größe, bzw. dem Tätigkeitsfeld eines Unternehmens ab. Die derzeitige Diskussion enthält die Gefahr, dass viele dieser Bedrohungen vergessen oder in den Hintergrund gedrängt werden.

A 5: Wie weit kann unser Staat (Bund, Länder) Bürger und Unternehmen gegen Angriffe aus dem Netz schützen? Was geht nur durch internationale Kooperation?

Im Internet sind Landesgrenzen irrelevant; interessanter sind Sprachgrenzen. Für Terror und organisiertes Verbrechen treten diese jedoch in den Hintergrund. Die Vorbereitung eines Verbrechens kann in einem anderen Land geschehen als die Durchführung. Unser Staat kann

Bürger und Unternehmen bestenfalls dann vor Datenklau schützen, wenn die Daten sein Territorium nicht verlassen. Alle anderen Schutzmaßnahmen bedürfen der internationalen Kooperation.

A 6: Welche Eigenschaften und Funktionen des Internets spielen eine besondere Rolle bei der Vorbereitung, Durchführung, Verhinderung und Aufdeckung von Verbrechen und Terror?

Das Internet ist ursprünglich vom Paradigma guter Nachbarschaft geprägt, die bei seiner heutigen Nutzung nicht immer angenommen werden kann. Maßnahmen zum Schutz der Internetanbindung Einzelner gegen Sabotage sind nicht vorgesehen. Nutzer müssen sich nicht identifizieren. Sie können sich also leicht hinter einem Pseudonym verstecken, was missbraucht werden kann. Weiterhin ist das Internet nicht zur Absicherung von Rechtsgeschäften, wie z. B. Verträgen, und zur Absicherung von Rechtsansprüchen konzipiert worden. Die entgeltfreie Nutzung ermöglicht zudem die millionenfache Duplizierung von Nachrichten (mit der Auswirkung als Spam-Problem). Das Ignorieren nationaler Grenzen macht die Anwendung nationaler Gesetze und nationaler Kontrollen sehr schwierig, da das anzuwendende Recht in der Regel durch den Standort des Servers bestimmt wird, was straf- und zivilrechtliche Verfolgung behindert. Auch ist die Verbrechensbekämpfung durch nationale Behörden somit erschwert, wenn nicht sogar unmöglich.

A 7: Dürfen Polizei und Geheimdienste die neueste Technik nutzen, um Verbrechen aufzudecken oder zu verhindern? Müssen Polizei und Geheimdienste über gute Internet-Kompetenz und moderne Analyse-Möglichkeiten verfügen?

Polizei und Geheimdienste dürfen die neueste Technik nutzen, um Verbrechen aufzudecken oder zu verhindern, wenn dafür eine gesetzliche Grundlage besteht.

Erfahrungsgemäß benutzen Straftäter fast immer die neueste Technik. Nur eine Gleichheit der ‚Waffen' gestattet es den Sicherheitsbehörden, Straftaten zu verhindern oder zeitnah aufzuklären. Muss die Polizei einem Autodieb per Fahrrad folgen, sind ihre Erfolgsaussichten beschränkt. Gegen Täter, die das Internet zur Vorbereitung und Durchführung von Verbrechen benutzen, kann nur mit hoher Informatik-Kompetenz und entsprechender Ausstattung begegnet werden. Der internationale Charakter des Internets, seine Datenmengen und das große Verkehrsaufkommen wecken auch bei Sicherheitsbehörden das Interesse an der Beherrschung moderner Analysemethoden, wie sie etwa mit dem Begriff ‚Big Data' umschrieben werden.

A 8: Ist es politisch verantwortbar zu verlangen, dass Polizei und Geheimdienste alles immer offen legen, was sie über die Tätigkeit von Terroristen und Verbrechern wissen? Dürfen sie die evtl. geplanten Gegenmaßnahmen geheim halten?

Viele Maßnahmen der für die Verbrechensverhütung und Verbrechensverfolgung zuständigen Organe sind nur dann sinnvoll, wenn sie im Geheimen geplant und ausgeführt werden können. Eine Katze, der man eine Schelle umhängt, ist beim Mäusefangen schlecht dran. Nachrichtendiente müssen geheim arbeiten. Ihre Tätigkeit entzieht sich deshalb in großen Teilen der medialen Berichterstattung und damit dem Bewusstsein der Öffentlichkeit. Einem Missbrauch dieses Privilegs soll durch eine Kontrolle seitens der zuständigen Parlamente entgegengewirkt werden. Auf Ebene des Bundes ist dies das Parlamentarische Kontrollgremium (PKGr) des Deutschen Bundestages, das allerdings unter Ausschluss der Öffentlichkeit tagt.

A 9: Was kann eine Fachgesellschaft wie die Gesellschaft für Informatik (GI) tun? Was hat die GI bisher unternommen?

Für die meisten Laien, aber auch für viele Fachleute, sind Sicherheitsfragen (Bedrohungen, Gegenmaßnahmen) ein rotes Tuch. Sie sind unangenehm und man geht ihnen gern aus dem Weg. Es gibt einen Fachbereich der GI, in dem sich viele Fachleute, die sich mit Sicherheitsfragen befassen, austauschen. Ein dem GI-Präsidium zuarbeitender Arbeitskreis wird aktiv, wenn Themen anstehen, zu denen Stellungnahmen der GI erforderlich oder wünschenswert sind.

Zwei neue Vorschläge ergeben sich aus der augenblicklichen Situation:

(1) Die GI sollte sich dafür einsetzen, dass es eine Art Ombudsmann für Sicherheit und Vertrauen in der Informatik gibt, an den sich GI-Mitglieder (und andere Bürger) wenden können, die sich allein gelassen fühlen.

(2) Über ihre Schwestergesellschaften in Europa und weltweit kann sie sich dafür einsetzen, dass politische Vereinbarungen getroffen werden, die die Bürger eines Landes vor Übergriffen der Geheimdienste anderer Länder schützen.

Als Reaktion auf die derzeitige Aufmerksamkeit der Medien gibt es eine Initiative (von Prof. Rudolf Bayer, TU München, angestoßen), die sich bemüht, für die bekannten asymmetrischen Verschlüsselungsverfahren gute und vertrauenswürdige Implementierungen zu finden und diese im massenhaften Einsatz zu testen. Man hofft, dadurch bei GI-Mitgliedern (und Informatikern allgemein) zu einer breiteren Anwendung und Akzeptanz von Schutzmaßnah-

men zu gelangen und Anwender von Verschlüsselung von dem Verdacht zu befreien, sie täten Verbotenes.

Mehr dazu finden Sie unter http://www.gi.de/aktuelles/meldungen/detailansicht/article/gi-fellow-bayer-zur-e-mailverschluesselung-ein-selbstversuch-und-eine-anleitung.html.

B. Technische und ökonomische Fragen

B 1: Ist es technisch möglich, den Telefon- und E-Mailverkehr aufzuzeichnen? Nur die Verbindungsdaten oder auch die Inhalte?

In gegenwärtigen Mobilfunknetzen werden Mobiltelefone vom jeweiligen Netzbetreiber fortlaufend geortet, um bei Bedarf eine Verbindung aufbauen zu können. Dabei sind dem Netzbetreiber alle technischen Daten des Telefons bekannt und auch die Daten des jeweiligen Gesprächs zusammen mit den sogenannten Verkehrsdaten Datum, Uhrzeit, sowie der Telefonnummern des jeweiligen Gesprächspartners.

Nach bisherigem Recht müssen die Anbieter die Verbindungsdaten nach Beendigung der Verbindung unverzüglich wieder löschen, es sei denn sie benötigen sie zu Abrechnungszwecken. Auch Gesprächsinhalte dürfen nicht anlasslos aufgezeichnet und gespeichert werden.

Verkehrsdaten und Gesprächsinhalte können von den Servern des Netzbetreibers zwar unberechtigt in Echtzeit kopiert werden; dieses Vorgehen wäre allerdings strafbar.

B 2: Was ist leichter abzuhören: eine WLAN-Verbindung oder eine Verbindung mittels Kabel, oder macht das keinen Unterschied?

Eine unverschlüsselte WLAN-Verbindung kann von allen Computern innerhalb der Sendereichweite mitgelesen werden. Eine verschlüsselte Verbindung müsste erst entschlüsselt werden; diese ist also sicherer – aber nicht hundertprozentig sicher, weil sie mit entsprechenden Verfahren entschlüsselt werden kann. Auch eine Kabelverbindung ist nicht sicher gegen Abhörversuche, insbesondere wenn der Angreifer physischen Zugriff auf das Kabel hat und so die Daten abgreifen oder die Abstrahlung ausnutzen kann.

B 3: Kann aus Bestellungen im Internet (etwa bei Amazon oder bei eBay) auf meine Interessen und Lebensverhältnisse geschlossen werden?

Ja, das ist sogar ein wesentlicher Teil des Geschäftsmodells dieser Firmen. Der Verkäufer hat eine vollständige Auflistung aller Käufe und wertet die Liste auch aus; das ist an dem Satz zu erkennen „Käufer dieses Produkts kauften auch …“. Aus der Wohngegend wird auf die wirtschaftliche Leistungsfähigkeit des Käufers geschlossen. Diese personenbezogenen Daten dürfen nach den Datenschutzgesetzen nicht weitergegeben werden, ohne dass der Kunde zustimmt. Oft enthalten die Geschäftsbedingungen von Internethändlern allerdings die Be-

stimmung, dass der Händler die Daten an Kreditauskunfteien weiter geben darf, wenn es Schwierigkeiten mit der Zahlung gibt.

Einem ausländischen Unternehmen anvertraute Daten deutscher Unternehmen können genauso wie private Daten Deutscher den zuständigen (ausländischen) nationalen Behörden weitergegeben werden.

B 4: Ist es möglich, Nachrichten nach Entstehungszeit und -ort zu klassifizieren?

Alles, was über das Internet geht, wird mit dem Erstellungs- und Versendedatum sowie der Uhrzeit versehen. Der Ort der Versendung lässt sich bei mobilen Geräten aus verschiedenen Quellen (z.B. GPS oder Ortungsdaten des Mobilfunknetzbetreibers) ermitteln. Auch bei stationären Geräten lässt sich oft aus der IP-Adresse auf den Standort schließen.

B 5: Können E-Mails manipuliert werden?

Das SMTP-Protokoll, das für die meisten Mails verwendet wird, bietet keinerlei Schutz vor Manipulation; es können beliebige Empfänger- und Sendedaten eingegeben werden. Eine andere Form der Manipulation ist das Vor- oder Zurückstellen des Datums im Computer. Werden mit dem auf diese Weise manipulierten Rechner E-Mails versandt, tragen sie das manipulierte Datum.

B 6: Was nützen Firewalls, Intrusion Detection und Protection Systeme?

Die Verwendung solcher Sicherheitssoftware entspricht dem Stand der Technik. Wer seinen Rechner vor dem Eindringen Unbefugter schützen will, muss derartige Software einsetzen. Aber: Sicherheitssoftware erhöht zwar die Sicherheit – enthält aber meist noch nicht veröffentlichte, möglicherweise auch sicherheitsrelevante Fehler (Sicherheitslücken), die für Angriffe ausgenutzt werden können.

B 7: Existieren Hintertüren, undokumentierte Funktionen in Standardsoftware und Betriebssystemen (Windows, Unix/Linux, iOS) und unveröffentlichte Sicherheitslücken (Zero-Day-Vulnerabilities).

Softwarehersteller kennen nicht alle Sicherheitslücken ihrer Software. Die Hersteller patchen aus wirtschaftlichen und/oder strategischen Gründen auch nur einen Teil der ihnen bekannten Sicherheitslücken; z.T. werden auch bereits veröffentlichte Sicherheitslücken erst nach Jahren behoben. Software kann auch Hintertüren (back doors) und andere undokumentierte, dem Anwender nicht bekannte Funktionen (covert functions wie covert channels) enthalten. Da sie noch nicht veröffentlicht sind, kann sich niemand gegen sie schützen. Tatsächlich kann unter Ausnutzung dieser Sicherheitslücken unerkannt in Computer und Systeme eingedrungen werden.

B 8: Gibt es hundertprozentige Sicherheitsmaßnahmen gegen Penetration und Überwachung?

Nach dem aktuellen Stand der Technik kann (fast) jedes – auch mit Firewalls, Virensuchprogrammen etc. abgesicherte - System erfolgreich angegriffen werden. Wir gehen davon aus, dass es gegen Penetration (Eindringen in Computer) und Überwachung keinen wirksamen Schutz gibt, denn mit genügend Aufwand kann jedes System geknackt werden. Nach dem aktuellen Stand der Technik können auch aus verschlüsselten Nachrichten Inhalte abgeleitet werden, ohne die Verschlüsselung zu brechen. Auch Anonymisierungsdienste wie TOR haben kaum verlässliche Wirkung, weil die dafür relevanten Netzknoten überwacht werden können.

B 9: Was ist mit Datensparsamkeit gemeint? Wie sinnvoll ist sie?

Datensparsamkeit ist ein Konzept aus dem Datenschutz und beschreibt die Grundidee, bei der Verarbeitung von Daten nur so viele personenbezogene Daten zu sammeln, wie die jeweilige Anwendung tatsächlich braucht. Will man diese Idee auf den Schutz vor Überwachung ausdehnen, hieße das, dass nur Daten in IT-Systemen und Netzwerken, die mit dem Internet verbunden sind, gespeichert und übertragen werden dürfen, bei denen das für die Anwendung unabdingbar ist. Speziell für global agierende Unternehmen ist diese Forderung jedoch unrealistisch. Am sichersten wäre es dennoch, wenn man die wertvollsten Daten von Unternehmen auf so genannten „stand-alone Systeme“ speichern könnte – ohne Anschluss an das Internet.

B 10: Was bedeutet Wirtschaftsspionage? Welche Folgen hat Wirtschaftsspionage? Ist auch Sabotage möglich?

Wirtschaftsspionage ist die Beschaffung von Informationen durch konkurrierende Organisationen. Die Informationsgewinnung geschieht entweder von außen oder von innen. Neben der Informationsgewinnung (Schutzziel Vertraulichkeit) sind auch Manipulationen und Störungen des Betriebs (Schutzziele Integrität und Verfügbarkeit) sowie Sabotage denkbar. Wirtschaftsspionage ist vor allem auf strategische Ziele gerichtet und beinhaltet z.B. das Stehlen von Konstruktionszeichnungen, geplanten Patenten oder Finanzplanungsdaten.

B 11: Weiß man, nach welchen Kriterien von staatlichen Stellen überwacht wird, bzw. nach welchen Stichworten gesucht wird?

Wortlisten sind nicht veröffentlicht. Benutzt werden vermutlich Begriffe z.B. der organisierten Kriminalität sowie von Terroristen für Straftaten, Rauschgift, Waffen, und es werden Namen, Adressen, Telefonnummern zu Suche einschlägig aktiver Personen eingesetzt.

B 12: Können Nachrichtendienste aus den Unmengen gespeicherten Daten überhaupt etwas herausfinden, oder macht die schiere Masse das sowieso unmöglich?

Die massenhafte Überwachung von Teilnehmeranschlüssen führt zu einem sehr großen Datenvolumen, das weitergeleitet, gespeichert und ausgewertet werden kann. Für die Auswertung sind die Indizierung und der Zeitbedarf für die Auswertung relevant. Suchmaschinen im Internet machen beispielsweise nichts anderes für alle weltweit über das Internet erreichbare Daten.

B 13: Wie harmlos ist es, wenn "nur" Verbindungs- oder Metadaten ausgespäht werden?

Aus den Verbindungsdaten ergibt sich, wann wer mit wem wie viel oder wie lange kommuniziert hat. Daraus ergibt sich oft auch der Aufenthaltsort und es kann auf Aktivitäten wie Geschäftsverbindungen geschlossen werden; insgesamt kann das individuelle Nutzerverhalten genau analysiert werden. Es können aber, wie erwähnt, nicht nur Verbindungsdaten, sondern auch vollständige Inhalte aufgezeichnet werden.

C. Ausspähung und mögliche Abwehr

C 1: Wie telefoniere ich sicherer: vom Festnetz oder vom Handy aus? Nützt es etwas, wenn ich am Telefon die Rufnummernanzeige unterdrücke?

Bei der Mobilkommunikation wird in Deutschland im Allgemeinen die Funkstrecke bis zum nächsten Sende-/Empfangsmast verschlüsselt; im Festnetz wird die übertragene Information nicht verschlüsselt.

Mit der Rufnummernunterdrückung wird nur erreicht, dass die (mitgesendete) Nummer beim Gesprächsempfänger nicht angezeigt wird. Der Netzbetreiber und andere Berechtigte – so z.B. die Polizei – können die Nummer sehen. Rufnummernunterdrückung ist also nur eine Sicherheitsmaßnahme gegen Missbrauch seitens des Gesprächsempfängers.

C 2: Ist es hilfreich, im Browser standardmäßig https einzustellen?

Mit dem Protokoll https wird (im Gegensatz zu http) eine verschlüsselte Verbindung zum Server aufgebaut, wenn der Server dies unterstützt.

Allerdings liegt die übertragene Nachricht im sendenden Computer und im empfangenden Computer unverschlüsselt vor und kann bei Eindringen in den Computer ausgelesen werden.

C 3: Was sind Apps und wie sicher sind sie?

Apps sind Anwendungsprogramme auf mobilen Geräten. Apps werden - je nach Art der App - nicht standardmäßig auf Sicherheit geprüft. Außerdem hängt die Sicherheit von Apps stark von der Sicherheit des Betriebssystems und des AppStores (Plattform, von der die App her-

untergeladen werden kann) ab. Viele Apps sind darauf ausgelegt, laufend Daten über Nutzung und Nutzerverhalten an die App-Entwickler und/oder den AppStore zu übermitteln. Nutzer wissen dies oft nicht.

C 4: Mit welchen Sicherheitsmaßnahmen kann ich mich privat oder mein Unternehmen schützen? Meine Kommunikation und meine gespeicherten Daten?

Hundertprozentige Sicherheit gibt es nicht. Das bedeutet, dass ein Angreifer mit hinreichendem Aufwand (an Geld und Zeit) fast immer erfolgreich sein wird. Für praktische Verschlüsselungsverfahren werden heute Zusicherungen von höchstens 30 Jahren gemacht. Die mathematischen Verfahren der Verschlüsselung gelten somit zwar als relativ sicher. Dennoch müssen diese implementiert und angewendet werden, und da Software nie fehlerfrei ist, garantiert auch der Einsatz von Verschlüsselungssoftware keinen hundertprozentigen Schutz.

Ziel muss also sein, das Sicherheitsniveau so zu heben, dass der Angreifer mehr Aufwand treiben muss, als die gespeicherten und übertragenen Daten ihm wert sind.

Das bedeutet im Privaten: Verschlüsseln aller gespeicherten und übertragenen Daten. Starke Zugriffskontrolle (Passworte mit mehr als 12 Zeichen, mit alphabetischen, numerischen und Sonderzeichen, Passwort möglichst häufig wechseln). Die Rollen Administrator und Anwender trennen. Möglichst anonym surfen. Hierzu findet man im Internet einschlägige Tipps zu Software und Verfahren.

Generell gilt: Risikovermeidung ist der erste Schritt zu mehr Sicherheit. Daten, die nicht unbedingt elektronisch gespeichert und übermittelt werden müssen, sind auf Papier sicher vor Netzüberwachung.

C 5: Wie verschlüssele ich? Muss mein Kommunikationspartner auch verschlüsseln oder reicht es, wenn ich das tue?

Gespeicherte Daten sollten symmetrisch verschlüsselt werden – d.h. ein einziger Schlüssel wird zum Verschlüsseln und Entschlüsseln benutzt. Dieser Schlüssel muss vor Dritten sorgfältig verborgen werden und darf keinesfalls auf dem Computer gespeichert werden.

Übertragene Daten sollten asymmetrisch verschlüsselt werden - d.h. es wird je ein Schlüssel zum Verschlüsseln und ein anderer entsprechender zum Entschlüsseln benutzt. Einer der beiden Schlüssel (der sogenannte private Schlüssel) muss vor Dritten sorgfältig verborgen werden, darf also nicht auf dem Computer gespeichert werden. Der Kommunikationspartner muss dasselbe Verfahren benutzen.

Verschlüsselungsprogramme ermöglichen die Verschlüsselung von Dateien und E-Mails. Allerdings erfordern Installation und Benutzung einiges an Sachkenntnis. Tipps zu Verschlüsselungsprogrammen finden sich im Internet.

C 6: Machen sich Anwender von Verschlüsselung verdächtig?

Verschlüsselte und unverschlüsselte Nachrichten sind leicht unterscheidbar. Das heißt, Überwachungsorgane können erkennen, dass Verschlüsselung eingesetzt worden ist. Was sie daraus schließen, bleibt offen.

C 7: Gibt es Unterschiede bei Suchmaschinen im Internet, was Datenspeicherung und Überwachung angeht?

Grundsätzlich gehen wir davon aus, dass alle Suchmaschinen im Internet überwacht werden. Ein höheres Sicherheitsniveau als beim Marktführer Google wird von Suchmaschinen wie Metager2, ixquick, StartPage, DuckDuckGo erreicht, die zwar ebenfalls überwacht werden (können), aber weder IP-Adressen noch andere personenbezogene Daten der Anfragenden speichern. Systeme wie TOR zur Abwehr von Überwachung zu benutzen, macht es für einen Überwacher einer Suchmaschine schwerer, festzustellen, wo eine Anfrage herkommt. Eine Überwachung von Systemen wie TOR ist natürlich prinzipiell ebenfalls möglich, allerdings ist die dezentrale Auslegung dieser Systeme ein sinnvoller Schutz.

D. Rechtliche Fragen

D 1: Welche Rechte haben deutsche Behörden?

Sofern Deutsche ausspähen, sind das Telekommunikationsgeheimnis und das Bundesdatenschutzgesetz berührt; rechtliche Grundlagen für ein Ausspähen, Abhören oder „Mitlesen“ von Telekommunikationsinhalten ergeben sich aus mehreren Gesetzen. Ein Ausspähen (von Metadaten und Inhalten) ohne explizite gesetzliche Grundlage ist in Deutschland aufgrund des grundgesetzlich geschützten Telekommunikationsgeheimnisses verboten.

Auch ohne Wissen der Betroffenen dürfen von den Strafverfolgungsbehörden gemäß § 100a Abs. 1 Strafprozessordnung (StPO) Telekommunikationsvorgänge überwacht und aufgezeichnet werden, wenn Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine schwere Straftat begangen hat oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder dadurch eine weitere Straftat vorbereitet hat. Die Straftaten, die in diesem Sinne als „schwere Straftaten“ gelten, sind in § 100a Abs. 2 StPO aufgelistet. Sie reichen von Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtstaats über Straftaten gegen die sexuelle Selbstbestimmung, Mord und Totschlag, Raub und Erpressung, gewerbsmäßige Hehlerei, Betrug und Computerbetrug bis hin zu gefährlichen Eingriffe in den Straßenverkehr, Brandstiftung etc. Zu den schweren

Straftaten im Sinne dieser Vorschrift gehören aber auch Steuerstraftatbestände wie Steuerhinterziehung, gewerbsmäßiger, gewaltsamer und bandenmäßiger Schmuggel oder Steuerhehlerei sowie zahlreiche Straftaten aus Spezialgesetzen, wie beispielsweise dem Außenwirtschaftsgesetz, dem Betäubungsmittelgesetz, dem Kriegswaffenkontrollgesetz, dem Waffengesetz oder dem Völkerstrafgesetzbuch. Das Abhören des Telekommunikationsverkehrs bedarf in allen genannten Fällen jeweils der richterlichen Anordnung, die schriftlich abzufassen ist. Nur in Fällen der Gefahr im Verzug darf auch die Staatsanwaltschaft selbst das Abhören von Telefongesprächen und sonstigen Telekommunikationsvorgängen anordnen; in diesem Falle muss aber die Anordnung richterlich innerhalb von 3 Werktagen bestätigt werden (§ 100b Abs. 1 StPO).

Nach den Bestimmungen in den §§ 94 ff. StPO können bei den E-Mail-Dienstanbietern auch die dort gespeicherten E-Mails beschlagnahmt werden. Auch hierfür bedarf es grundsätzlich der richterlichen Anordnung; nur bei Gefahr im Verzug darf auch die Staatsanwaltschaft die Beschlagnahme anordnen.

Nach den Bestimmungen in § 3 des sogenannten Artikel-10-Gesetzes (diesen Titel hat das Gesetz von Artikel 10 des Grundgesetzes, in dem das Telekommunikationsgeheimnis verbrieft ist) sind der Bundesverfassungsschutz, der Bundesnachrichtendienst und der militärische Abschirmdienst berechtigt, Telekommunikationsvorgänge, also insbesondere Telefongespräche, abzuhören und aufzuzeichnen, wenn dies erforderlich ist, um Straftaten gegen die freiheitlich demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Bundeslandes abzuwehren oder aufzuklären. Dafür müssen tatsächliche Anhaltspunkte gegeben sein, die den Verdacht rechtfertigen, dass jemand eine Straftat, wie sie in § 3 des Artikel-10-Gesetzes aufgelistet ist, plant, begeht oder bereits begangen hat. Gemäß § 5 des Artikel-10-Gesetzes können von den genannten Behörden auch grenzüberschreitende Telekommunikationsvorgänge abgehört und aufgezeichnet werden. Die entsprechenden Anordnungen solcher Maßnahmen nach dem Artikel-10-Gesetz dürfen nur durch die höchsten Bundes- oder Landesbehörden getroffen werden; bei Aktivitäten des Bundesverfassungsschutzes ist das Bundesinnenministerium die maßgebliche Behörde. Die nach § 3 des Artikel-10-Gesetzes getroffenen Maßnahmen unterliegen der Kontrolle des parlamentarischen Kontrollausschusses. Eine Weitergabe der vom Bundesnachrichtendienst auf diese Art und Weise erhobenen Daten an Strafverfolgungsbehörden des In- oder Auslandes ist unter den Voraussetzungen von § 7 (Übermittlung an Strafverfolgungsbehörden) bzw. § 7a des Artikel-10-Gesetzes (im Falle der Übermittlung an ausländische Nachrichtendienste) zulässig. Die Übermittlung an ausländische Nachrichtendienste beispielsweise bedarf zusätzlich zu weiteren rechtlichen Kriterien (zu denen auch die Vereinbarkeit mit dem deutschen Datenschutzrecht gehört) der Genehmigung durch das Bundeskanzleramt.

Nach den Vorschriften des Bundesverfassungsschutzgesetzes, des Gesetzes über den Bundesnachrichtendienst sowie des Gesetzes über den militärischen Abschirmdienst darf unter bestimmten Voraussetzungen die Herausgabe von Bestands- und Verkehrsdaten von Telekommunikationsdiensteanbietern verlangt werden. Auch hierfür bedarf es der ausdrücklichen Anordnung des Bundesinnenministeriums, wobei auch diese Vorgänge wiederum der Aufsicht des parlamentarischen Kontrollgremiums des deutschen Bundestages unterliegen.

Ausländische Nachrichtendienste (Geheimdienste) haben in Deutschland keine Rechte und würden sich strafbar machen (§§ 202a, 202b oder 206 StGB). Ausländische Nachrichtendienste dürfen in Abhängigkeit ihrer nationalen Gesetze abhören. Dies tun daher auch die Nachrichtendienste der EU-Staaten - mit mehr oder weniger finanziellem Aufwand. Darüber hinaus kann davon ausgegangen werden, dass die organisierte Kriminalität Abhörmaßnahmen durchführt und Daten auch manipuliert.

D 2: Gibt es ein „Super“grundrecht auf Sicherheit?

Eine erste Feststellung: Supergrundrechte gibt es nicht. Alle Grundrechte sind im Grundgesetz (GG) gleichgestellt – es gibt keines, das mehr wert ist als ein anderes.

Die zweite Feststellung: Wer das Grundgesetz liest, wird kein Grundrecht auf Sicherheit finden.

Einfache Antwort also: Es gibt kein Grundrecht auf Sicherheit.

So einfach ist es aber nicht. Auch ein Grundrecht auf informationelle Selbstbestimmung kommt im Text des Grundgesetzes nicht vor. Dieses Recht hat das Bundesverfassungsgericht als besonderen Ausdruck des in Art. 2 Abs. 1 GG geschützten Rechts auf freie Entfaltung der Persönlichkeit geschützt. Später hat es aus Art. 2 Abs. 1 GG auch noch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgeleitet. Es gibt also Grundrechte, die im Text der Verfassung nicht ausdrücklich erwähnt sind.

Nur: Ein Grundrecht auf Sicherheit gibt es in der Rechtsprechung des Bundesverfassungsgerichts nicht. Es spricht auch nicht viel dafür, dass sich das ändert: Grundrechte schützen in erster Linie Bürger vor dem Staat – wer vom Grundrecht auf Sicherheit spricht, will staatliche Eingriffe legitimieren. Das passt nicht zusammen. Ein Grundrecht auf Sicherheit gibt es nicht.

Aber: Es gibt ein Grundrecht auf Leben und persönliche Unversehrtheit (Art. 2 Abs. 2 GG). Auch die persönliche Freiheit (Art. 2 Abs. 2 GG) und das Eigentum (Art. 14 GG) sind grundrechtlich geschützt. Diese Rechte schützen zwar in erster Linie vor staatlichen Eingriffen. Aber: Grundrechte verpflichten den Staat nach übereinstimmender Meinung aller Juristen auch, die Bürger vor Eingriffen Dritter in diese Rechte zu schützen. Deswegen sind Mord,

Freiheitsberaubung und Diebstahl strafbar. Deswegen werden aber auch Verkehrsregeln aufgestellt oder Datenschutzregeln für Private. Historisch ist dieser Schutz nicht die einzige, aber eine der wichtigsten Aufgaben des modernen Staates: Der Staat stellt einen Rahmen zur Verfügung, in dem der einzelne sich entfalten kann, ohne (übermäßigen) Gefahren ausgesetzt zu sein. Tut der Staat das nicht, verliert er seine Legitimation, z.B. kann er das Gewaltmonopol nicht mehr für sich beanspruchen. Alle klassischen Western zeigen Situationen, in denen es noch keinen funktionierenden Staat gab – in der Regel gewinnt der Stärkere. Nichtmehrstaaten wie Somalia zeigen auch heute, was dann passiert.

Deswegen: Die Gewährleistung von Sicherheit ist eine wichtige staatliche Aufgabe. Der Staat muss auch die Mittel bekommen, sie durchzusetzen. Dazu gehören auch personenbezogene Daten über Bürgern des Staates, aber auch von denen anderer Staaten – die Bekämpfung von Gefahren wäre sonst unmöglich. Nur: Auch hier gibt es Grenzen. Der Staat kann und darf nicht bei jeder noch so geringen Gefahr für den Bürger eingreifen. Absolute Sicherheit gibt es nicht. Die Grenzen staatlichen Handelns werden juristisch von den Grundrechten der betroffenen Bürger gezogen. Die Gewährleistung von Sicherheit rechtfertigt nicht jedes staatliche Handeln. Der Staat darf nicht foltern. Auch die Todesstrafe ist verboten. Strafen werden in einem Prozess verhängt, der bestimmte Rechte auch des Angeklagten gewährleistet. Der Staat darf auch nicht zum Überwachungsstaat werden und im Interesse der Sicherheit die Freiheit abschaffen. In Deutschland ist deswegen die Rasterfahndung vom Bundesverfassungsgericht immer wieder verboten worden. Auch bei anderen Eingriffen hat es Grenzen gezogen. Andere Eingriffe (etwa Durchsuchung und Beschlagnahme auch bei Unverdächtigen) waren und sind zulässig. Auch hier wird über die Grenzen staatlichen Handelns intensiv politisch und juristisch gestritten.

Insgesamt gilt: Ein Grundrecht auf Sicherheit gibt es nicht. Die Gewährleistung von Sicherheit ist aber eine wichtige Aufgabe des Staates. Die Eingriffe des Staates zur Gewährleistung der Sicherheit haben aber ihrerseits Grenzen durch die Grundrechte der Betroffenen.

D 3: Habe ich das Recht, etwas verbergen zu wollen?

Kurze Antwort: Rechtlich dürfen Sie meist, aber nicht immer, etwas verbergen – oder genauer, Sie müssen nicht antworten oder dürfen sogar falsch antworten. Nur in wenigen Situationen müssen Sie korrekt antworten. Rechtlich dürfen Sie also oft etwas verbergen. Ob Sie das tun wollen oder sich moralisch verpflichtet fühlen, trotzdem die Wahrheit zu sagen, bleibt dann Ihre eigene Entscheidung.

Erste Aussage einer genaueren Analyse: Von sich aus müssen Sie nur ganz selten etwas sagen. Aber auch auf Fragen müssen Sie in den meisten Fällen überhaupt nicht antworten –

auch falsche Antworten sind rechtlich nicht verboten. Fragt Sie jemand, ob es Ihnen gut geht, müssen Sie nicht antworten – sie können auch falsch antworten. Ob Sie jemandem vorspiegeln, dass es Ihnen gut geht, obwohl Sie krank sind oder anders herum – solange es um gesellschaftliche Kontakte geht, mischt sich das Recht nicht ein. Wenn Sie allerdings lügen, um einen finanziellen Vorteil zu erlangen, ist das verboten und sogar strafbar. Das ist nämlich Betrug. Wenn Sie nur lügen, damit andere besser von Ihnen denken, oder, um Mitleid zu erregen, oder aus ganz anderen Gründen, ist das rechtlich nicht verboten. Schweigen dürfen Sie fast immer. Manche müssen es auch: Seelsorger, Ärzte, Rechtsanwälte und andere Berufsgruppen sind zum Schweigen über das verpflichtet, was sie beruflich erfahren. Sie dürfen also nicht etwas verbergen, sie müssen es sogar.

Es gibt aber Situationen, in denen Sie antworten müssen: Wer als Zeuge vor Gericht geladen ist, muss richtig antworten. In Konfliktfällen gilt das aber nicht: Als Angehörige von Parteien müssen Sie nicht antworten. Ärzte, Seelsorger, Rechtsanwälte und andere spezielle Berufsträger dürfen über das schweigen, was sie beruflich erfahren. Außerdem muss sich niemand als Zeuge selbst belasten. Lügen dürfen Sie dann aber auch nicht: Wenn Sie nicht schweigen, müssen Sie die Wahrheit sagen. Kurz gesagt: Sie müssen nichts aufdecken, sie dürfen aber auch nichts verstecken. Auch als Prozesspartei müssen Sie die Wahrheit sagen. Nur ein Beschuldigter oder Angeklagter im Strafverfahren darf sogar lügen.

Reden müssen Sie aber auch in anderen Situationen: Wer ein Haus verkauft, muss den Käufer auf Hausschwamm hinweisen, wenn er davon weiß. Ein Handelsvertreter muss über seine Vermittlungen berichten, sein Prinzipal muss die Vergütung abrechnen. Wer hier schweigt, falsche Auskunft gibt oder falsch abrechnet, muss Schadensersatz oder andere zivilrechtliche Konsequenzen befürchten – oft macht er sich sogar strafbar. Hier gibt es keine Zeugnis- oder Auskunftsverweigerungsrechte. Schweigen ist nie zulässig. Das gilt auch, wenn ein Arbeitgeber Korruptionsvorwürfen nachgeht: Ein Arbeitnehmer ist arbeitsrechtlich verpflichtet, wahrheitsgemäß Auskunft darüber zu geben, was er getan hat, auch wenn er sich selbst, Kollegen, Freunde oder Angehörige belastet. Das macht sich oft auch die Staatsanwaltschaft zu Nutze: Sie lässt den Arbeitgeber ermitteln und beschlagnahmt dann die Unterlagen, um sie gegen den Arbeitnehmer zu verwenden. Das Schweigerecht des Beschuldigten, das Aussageverweigerungsrecht von Zeugen wird so umgangen. Unzulässig ist solch ein Vorgehen nach der Mehrheitsmeinung der Juristen nicht, obwohl viele Strafverteidiger das anders sehen.

Manchmal dürfen Sie freilich auch in solchen Situationen nicht nur schweigen, sondern sogar lügen, dann nämlich, wenn ihr Vertragspartner eine unzulässige Frage stellt und nur eine Lüge Ihnen hilft: Das klassische Beispiel ist die Frage an die Arbeitsplatzbewerberin nach ei-

ner Schwangerschaft: Eine Schwangere darf die Schwangerschaft verleugnen. Es muss um unzulässige Fragen und gravierende Nachteile gehen.

Alles in allem gilt folgendes: Rechtlich dürfen Sie oft etwas verbergen – ob sie das tun oder nicht, müssen Sie selbst entscheiden.

Im Internet wird in diesem Zusammenhang oft eine spezielle Frage diskutiert: Gibt es ein Recht auf Anonymität im Netz? Nach der geltenden Gesetzeslage ist die Antwort einfach: ja. § 13 Abs. 5 Telemediengesetzt lautet nämlich: „Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren." Diese Norm gilt praktisch für alle Anbieter im Internet. Sie sieht die anonyme Nutzung des Internets vor.

Ob das so bleiben soll, ist unter Juristen umstritten: Der Deutsche Juristentag 2012 hat mit knapper Mehrheit beschlossen, dass es ein Recht auf Anonymität im Internet nicht geben soll. Man muss zwar nicht unter dem eigenen Namen handeln müssen. Jeder soll aber identifizierbar bleiben, damit Rechtsverstöße verfolgt werden können. Der Gesetzgeber hat dieses Votum aber bislang nicht umgesetzt.

Hier gibt es auch verständliche Konflikte: Wer beleidigt wird, möchte wissen, wer das getan hat. Das gilt auch für den, der im Internet betrogen wurde. Nahezu jeder will, dass der gefunden wird, der Mordaufrufe oder Kinderpornographie im Internet verbreitet. Das geht aber nicht, wenn es wirklich anonym geschieht. Umgekehrt: In vielen Staaten wird legitime Kritik an den Herrschenden oder auch in ihren Freunden in der Wirtschaft brutal bestraft – hier muss es möglich sein, sich anonym zu äußern. Ähnliches gilt auch für Staaten, in denen Andersgläubige (oder Nichtgläubige) verfolgt werden. Juristisch gesprochen geht es um Grundrechte und ihre Grenzen, aber auch um unterschiedliche Grundrechtsträger, deren Grundrechte widerstreitende Interessen schützen und die zum Ausgleich gebracht werden müssen – der Fachterminus ist der der praktischen Konkordanz von Grundrechten. Wie das geschieht, darüber wird im Einzelfall immer gestritten.

Ein Beispiel: Das Grundrecht auf informationelle Selbstbestimmung verlangt, dass nur das über eine Person aufgezeichnet wird, was der Betroffene will – wenn er sich anonym äußern will, ist das ein Ausdruck seiner informationellen Selbstbestimmung. Wenn er aber anonym in einem Meinungsforum seinen Nachbarn beschuldigt, Straftaten zu begehen, ist das ein Eingriff in dessen persönliche Ehre (und in dessen informationelles Selbstbestimmungsrecht). Die Ehre ist aber auch grundrechtlich geschützt. Man muss dann abwägen, welches Grundrecht vorgeht. Die jetzige Regelung ist so, dass die Anonymität geschützt ist, der

Diensteanbieter die Äußerung aber nach einem Hinweis des Nachbarn aus dem Forum entfernen muss („Notice and take down“, § 10 S. 1 TMG). Damit kann der Nachbar zwar erreichen, dass die Äußerung in diesem Forum gestrichen wird, nicht aber, dass es dem Äußernden verboten wird, sie weiterhin (z.B. in anderen Meinungsforen) zu machen, wenn sie falsch ist – auch ein Schmerzensgeld kann er nicht durchsetzen. Das reichte der Mehrheit des beim Deutschen Juristentag anwesenden Juristen nicht aus. Sie wollten, dass in einem solchen Fall die Anonymität aufgehoben werden muss und der Nachbar gegen den Äußernden vorgehen kann. Der Gesetzgeber ist diesem Begehren aber nicht nachgekommen.

D 4: Kann ich mich bei Fragen an den Bundesdatenschutzbeauftragten wenden?

Am Anfang die einfache Antwort: Wenn Sie sich mit Fragen an den Bundesdatenschutzbeauftragten wenden, wird er sie beantworten, u.U. aber auch nur mit dem Hinweis auf zuständige andere Behörden. Angesichts der komplizierten Zuständigkeiten beim Datenschutz ist das oft sehr hilfreich. Fragen mit Bezug zu Bundesbehörden wird der Bundesdatenschutzbeauftragte aber immer beantworten.

Geht man der Frage genauer nach, geht es in erster Linie um Zuständigkeiten: Zuständig ist der Bundesbeauftragte für Datenschutz und Informationsfreiheit – so heißt die Behörde exakt – nur für die Kontrolle der öffentlichen Stellen des Bundes, d.h. für Bundesbehörden, öffentliche rechtliche Körperschaften des Bundes wie der Bundesagentur für Arbeit und andere Einrichtungen öffentlichen Rechts (§ 24 Abs. 1 BDSG). Zu diesen öffentlichen Stellen des Bundes gehören auch das Bundeskriminalamt, das Bundesamt für Verfassungsschutz und der Bundesnachrichtendienst. Der Bundesdatenschutzbeauftragte ist nicht zuständig für die Aufsicht über Landesbehörden – dafür gibt es Landesdatenschutzbeauftragte. Er ist auch nicht zuständig für die Aufsicht über private Unternehmen. Dafür gibt es Aufsichtsbehörden. Das sind in vielen Ländern auch die Landesdatenschutzbeauftragten, in anderen aber auch die Bezirksregierungen. Für ausländische öffentliche Einrichtungen wie die NSA ist im Prinzip keine Behörde in Deutschland zuständig. Auch die Gerichte unterliegen weitgehend keiner Kontrolle durch die Datenschutzbeauftragten.

Besonderheiten gelten im besonders sensiblen Bereich der Telekommunikation, also für Telefon und Datenübermittlung auch im Internet: Hier führt der Bundesbeauftragte auch die Aufsicht über die privaten Telekommunikationsunternehmen (§ 115 Abs. 4 TKG). Soweit hier aber die Nachrichtendienste tätig sind, darf sie der Bundesbeauftragte nur eingeschränkt kontrollieren. Eigentlich ist nur die sog. G10-Kommission des Bundestages für Aufsicht und Kontrolle zuständig – sie kann aber den Bundesbeauftragten mit der Kontrolle beauftragen, er darf dann aber nur ihr berichten (§ 24 Abs. 2 S.3 BDSG).

Soweit der Bundesbeauftragte für Datenschutz und Informationsfreiheit für die Aufsicht zuständig ist, muss er auch Eingaben von Bürgern bearbeiten und Fragen beantworten (§ 21 BDSG). Damit er das kann, hat er auch eigene Ermittlungsrechte gegenüber den Behörden. Die Behörden müssen ihm Fragen beantworten und Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und die Datenverarbeitungsprogramme gewähren (§ 24 Abs. 4 S. 2 Nr. 1 BDSG). Für Sicherheitsbehörden gilt das nicht, wenn dadurch die Sicherheit des Bundes oder eines Landes gefährdet ist. Aber auch dann, wenn er Auskünfte erhält, darf er sie dem Bürger gegenüber nur so verwenden, dass Geheimhaltungsvorschriften nicht gefährdet sind. Für die Nachrichtendienste gilt außerdem, dass der Bundesbeauftragte im Bereich der Telekommunikation nur der G10-Kommission berichten darf.

Der Bundesbeauftragte arbeitet außerdem regelmäßig auf internationaler, insbesondere auf europäischer Ebene mit ausländischen Datenschutzbehörden zusammen. Auch dazu wird er Fragen beantworten.

Außerhalb seines Zuständigkeitsbereichs wird der Bundesdatenschutzbeauftragte Ihre Fragen inhaltlich nicht beantworten können.

D 5: Wo kann ich Bestimmungen zum Datenschutz nachlesen? Ist der Ausdruck „Datenschutz“ noch passend, wenn es primär um Kommunikationsverhalten geht?

Grundsätzlich gilt das Bundesdatenschutzgesetz (BDSG). Für den Umgang mit Telekommunikationsdaten gilt das Telekommunikationsgesetz (TKG) (§§ 88 - 115) und für den Umgang mit Internetdaten das Telemediengesetz (TMG) (§§ 11 – 15a). Die Texte sind z.B. nachzulesen unter http://www.datenschutz.de/.

Da es bei der Überwachung des Internet oder der Telekommunikation um die Verarbeitung von Kommunikationsdaten geht, betrifft diese Überwachung eine bestimmte Form des Datenschutzes.

Durch die Speicherung und Ausforschung von Telekommunikations- und Internetdaten ist nicht nur die informationelle Selbstbestimmung nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG betroffen, sondern auch das Grundrecht auf Schutz des Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG.

D 6: Wie lässt sich Privatsphäre definieren? Was ist rechtlich klar definierbar, was ist subjektives Gefühl und Wunschdenken? Gibt es Unterschiede zwischen Europa und USA?

In Deutschland werden Privatsphäre und Datenschutz von Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistet. Aus diesen Grundrechten auf freie Entfaltung der Persönlich-

keit und auf Schutz der Menschenwürde hat das Bundesverfassungsgericht spezifische Grundrechte konkretisiert. Für den Schutz des Persönlichkeitsrechts unterscheidet es Intimsphäre, Privatsphäre und Öffentlichkeitssphäre und gewährleistet einen nach betroffener Sphäre einen unterschiedlichen Schutz gegen das Eindringen der Öffentlichkeit (z.B. gegenüber den Medien). Für den Schutz gegenüber der automatisierten Datenverarbeitung hat sich diese räumliche Schutzkonzeption nach Sphären als wenig geeignet erwiesen. Es wurde für den Datenschutz durch das Volkszählungsurteil 1983 des Bundesverfassungsgerichts durch das Konzept der informationellen Selbstbestimmung abgelöst. Dieses beruht auf der Theorie sozialer Rollen und einem Konzept der Persönlichkeitsentwicklung in sozialer Kommunikation. Nach dem Grundrecht auf informationelle Selbstbestimmung steht jedem die Befugnis zu, selbst zu bestimmen, wer wann welche Daten über einen selbst erheben, verarbeiten, nutzen und veröffentlichen darf. Nach diesem Konzept gibt es keine nicht schützenswerten personenbezogenen Daten. Deren Schutzbedürftigkeit hängt nicht von den Daten, sondern vom Kontext ihrer Verwendung ab. Jeder Umgang mit Daten ohne Erlaubnis durch den Betroffenen oder den Gesetzgeber gilt als Grundrechtsverletzung und ist verboten.

In der Europäischen Grundrechtecharta wird in Art. 8 jeder Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten zugestanden. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Die europäischen Vorstellungen zum Datenschutz sind durch die deutschen Vorarbeiten stark geprägt und mit dem deutschen Konzept weitgehend inhaltsgleich.

In USA wird kein Grundrecht auf informationelle Selbstbestimmung anerkannt, sondern nur ein „Right to be left alone“. Dementsprechend gibt es in USA nur einzelne Gesetze, die dieses Recht in bestimmten Lebensbereichen ansatzweise schützen. Eine allgemeine und systematische Gesetzgebung zum Schutz dieser Form der Privatsphäre gibt es aber nicht.

D 7: Gibt es gesetzliche Auflagen, die Firmen aus den USA wie Amazon, Google und Facebook erfüllen müssen, um Geheimdienste oder Ermittlungsbehörden zu unterstützen? (a) Amerikanische Bürger betreffend (b) Nicht-Amerikaner betreffend. Kann ich im Internet ohne Bedenken Dienste in Anspruch nehmen, von denen bekannt ist, dass sie die Cloud-Funktionen bekannter amerikanischer Anbieter (wie Amazon und Google) nutzen?

Nach dem „Foreign Intelligence Surveillance Act (FISA)“ (50 U.S.C. § 1861) können US-Sicherheitsbehörden beim sog. FSI-Court eine Anordnung beantragen, die eine Person verpflichtet, die bei ihr befindlichen Geschäftsunterlagen (hierzu gehören auch alle gespeicherten Daten) herauszugeben. Anordnungen können gegenüber jeder beliebigen Stelle erlassen

werden und haben nur zur Voraussetzung, dass Unterlagen mit einer Untersuchung von Terrorismus und Spionage in Verbindung stehen. Der FSI-Court ist ein geheim tagendes Sondergericht, dessen einzige Aufgabe es ist, über Anordnungen nach dem FISA zu entscheiden. Eine Anordnung kann von US-Unternehmen auch verlangen, dass sie Daten herausgeben, die sich im Ausland befinden oder die sie sich im Ausland (z.B. von Konzerntöchtern) beschaffen können. Weigern sie sich, drohen ihnen empfindliche Sanktionen wegen einer Missachtung des Gerichts („Contempt of Court“). Der FISA bezweckt die Ausspähung von Nicht-US-Bürgern. Zur Herausgabe verpflichtet werden können aber nur Personen, die dem US-Recht unterliegen. Diesen Überwachungsmaßnahmen kann sich niemand entziehen, der personenbezogene Daten einem amerikanischen Unternehmen oder dessen deutschen Töchtern anvertraut, auch wenn die Daten in Deutschland oder Europa gespeichert werden.

Kommentare und Rückfragen sind willkommen. Gerne per E-Mail an cornelia.winter@gi.de.

Bonn, 28. August 2013

Gesellschaft für Informatik e.V. (GI)
Wissenschaftszentrum
Ahrstr. 45
53175 Bonn
Tel.: +49 (0)228/302-145 / Fax: +49 (0)228/302-167
E-Mail: gs@gi.de / WWW: http://www.gi.de