Geschützt werden nicht nur die Daten, sondern das System insgesamt – Analyse und (Nicht-) Anwendung eines verschollenen Grundrechts

Rainer Rehak

Abstract

The security of our common digital infrastructure has been deliberately weakened by the secret services, for better “surveillability” and better “accessibility”. This project has not only been driven by our transatlantic or European partners but by the German secret services alike. Data gathered in this fashion will be stored for decades, traded amongst the services and used at will. This should concern citizens, authorities, businesses and other organizations, in Germany and elsewhere. All information being processed and digitally transferred is targeted, tax data, location data, health data, business data, communication data, simply put: all data.

But how does this go along with the clandestine-online-search-ruling of the German constitutional court in 2008, which brought to life the constitutional right to warranty of confidentiality and integrity of information systems? What should it protect, why is it missing in action and what are necessary conclusions from the current situation?

1. Einleitung

In der Denkweise der vorliegenden Arbeit hat das Fachgebiet „Informatik und Gesellschaft” grob zwei Ausrichtungen. Einerseits sollen die Grundlagen und Wirkungsweisen der Informationstechnik in die relevanten Diskurse der Gesellschaft getragen werden, damit technische Effekte, Wechselwirkungen und Implikationen sinnvoll diskutierbar gemacht werden.

Andererseits sollen die Zusammenhänge gesellschaftlicher, politischer, rechtlicher, politischer und wirtschaftlicher Strukturen wiederum in die Informatik gebracht werden, damit die Informatiktreibenden selbst die Wirkungsweisen und ihrer Handlungen abschätzen lernen (vgl. Coy 1989, S. 17), denn in komplexen technischen Zusammenhängen sind nur sie dazu in der Lage.

Um die Notwendigkeit dieser Herangehensweise auch von anderer Zeit und Stelle aus zu motivieren, sei folgender Abschnitt des Volkszählungsurteils von 1983 angeführt:

„Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. Ihrem Schutz dient [...] das […] allgemeine Persönlichkeitsrecht, das gerade auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen der menschlichen Persönlichkeit Bedeutung gewinnen kann.“ (BVerfG 1983, Abschnitt C II 1a)

Mit „moderne Entwicklungen“ sind natürlich vordergründig informationstechnische Entwicklungen im Bereich der elektronisch-automatisierten Datenverarbeitung gemeint, wobei das Gericht in diesem Urteil dementsprechend das Grundrecht auf informationelle Selbstbestimmung formulierte.

Für Analysen der „mit ihnen verbundenen neuen Gefährdungen“ ist jedoch technischer und „gesellschaftlicher“ Sachverstand vonnöten. Um eine spezielle Art der Gefährdung der menschlichen Persönlichkeit durch den Einsatz von Informationstechnik soll es im Folgenden gehen.

2. Der Weg zur Gewährleistung der Vertraulichkeit und Integrität

Im Jahr 2006 bekam das Landesamt für Verfassungsschutz Nordrhein-Westfalen durch ein neues Verfassungsschutzgesetz (VSG) die Ermächtigung zur Aufklärung des Internets, konkret durch „den heimlichen Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel“. Dies war der Startschuss für die „offizielle“ staatliche Nutzung heimlicher Online-Durchsuchungen - auch „Staatstrojaner“ genannt - durch Behörden, denn schon 2005 hatte der damalige Bundesinnenminister *Otto Schily* dem Bundesamt für Verfassungsschutz derartige Methoden per geheimer Dienstanweisungen ermöglicht (dpa 2007).

Im Jahr 2007 kam es zu einer Verfassungsbeschwerde, wobei die Regelung 2008 durch das Bundesverfassungsgericht für ungültig erklärt wurde, da das Gericht das (neue) *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* verletzt sah. Anzumerken ist hier, dass das Grundrecht zwei der drei Elemente traditioneller Datensicherheit abdeckt, Verfügbarkeit ist nicht dabei.

Auch aktuell ist bezüglich der heimlichen Online-Durchsuchungen eine Klage anhängig, denn das Bundeskriminalamt kann laut BKAG § 20 k (Verdeckter Eingriff in informationstechnische Systeme) und § 20l (Überwachung der Telekommunikation) heimliche Online-Durchsuchungen durchführen. Diese Normen werden u. a. angegriffen, weil der Gesetzgeber die vom Bundesverfassungsgericht für derartige Ermächtigungen vorgesehenen Beschränkungen nur lapidar wortwörtlich übernommen hatte ohne - in derartigen Gesetzen notwendige - Konkretisierungen vorzunehmen, so jedenfalls lautet die Kritik.

1.1 Informationstechnische Systeme

Was ist jedoch ein *informationstechnisches System (ITS)*? Laut Bundesverfassungsgericht ist es ein technisches System, das Informationen verarbeitet. Netzwerke und andere Verbünde dieser Geräte oder Netzwerke können ebenfalls als ITS gelten. Auch nicht-lokal vorgehaltene Daten werden als Teil eines informationstechnischen Systems verstanden, wenn die Nutzer es als eigenes nutzen und deshalb den Umständen nach davon ausgehen dürfen, dass sie darüber selbstbestimmt verfügen (BVerfG 2008, Absatz 206). Ein ITS in dieser Lesart ist folglich kein System im Hardware-Sinne, sondern ein abstraktes System - erzeugt durch den Nutzungszusammenhang - das sich über viele ~~dieser~~ „Hardware-Systeme“ erstrecken kann.

2.2 Der allgemeine I&G-Teil des Urteils

Zunächst erkannte das Gericht die allgegenwärtige Nutzung informationstechnischer Systeme an, was insbesondere durch ihre Totalität eine gesellschaftlich-rechtlich bemerkenswerte Feststellung darstellt. Weiter beschreibt es die vorher unabsehbare Bedeutung informationstechnischer Systeme für die persönliche Entfaltung des Einzelnen, da eine steigende Konzentration und Verlagerung individueller und sozialer Facetten einer Person in technische Systeme, die zudem über das Internet vernetzt sind, festzustellen ist. Für die ungehinderte Persönlichkeitsentfaltung, so das Gericht weiter, ist die einzelne Person auf die Vertraulichkeit und Integrität ihrer Systeme angewiesen, ja sogar davon abhängig.

Die Komplexität dieser Systeme ist dabei so hoch, dass fremde *Eingriffe* in der Regel weder wahrgenommen noch technisch verhindert werden können. Heimliche Eingriffe haben somit nicht den Charakter einer einzelnen Datenerhebung, die z. B. das Recht auf informationelle Selbstbestimmung berühren würde, sondern sie ziehen den vollständigen Kontrollverlust über den Kernbereich privater Lebensgestaltung nach sich. Auch hier findet sich wieder eine Totalaussage.

In der Konsequenz formuliert ~~es~~ das Gericht die verfassungsrechtliche Notwendigkeit eines von der konkreten Sicherheit des Systems unabhängigen Schutzes der Vertraulichkeits- und Integritätserwartung an das System. Dadurch öffnet sich zwar eine weit über die Technik hinausgehende Schutzdimension, die jedoch nur unter Einbeziehung der konkreten

Eigenschaften von Informationstechnik operationalisiert werden kann (Rehak 2013, S. 68 ff.). Aus diesem Grunde war die beanstandete Regelung für den heimlichen Zugriff auf informationstechnische Systeme in der Form verfassungswidrig.

2.3 Interpretation des Urteils

Die obige Beschreibung versteht also die Systemgrenzen als Grenzen einer - zur körperlichen und räumlichen Ausdehnung orthogonalen - informationstechnischen Manifestation und Ausprägung der Persönlichkeit der Nutzer. Eine Verletzung der *Integrität* des Systems ist in der Folge als Verletzung der Integrität der Person zu interpretieren. Anders ausgedrückt bedeuten heimliche Eingriffe „eine sukzessive Einschränkung und schließlich Auflösung dessen, was wir als Grundwert des Schutzes der Person, ihrer Autonomie, Freiheit und Würde kennen“ (Pfitzmann 2007).

2.4 Wie erwartet?

Wenn nun aber eine „Vertraulichkeits- und Integritätserwartung” der Nutzer an ihre Systeme nur dann geschützt wird, wenn sie

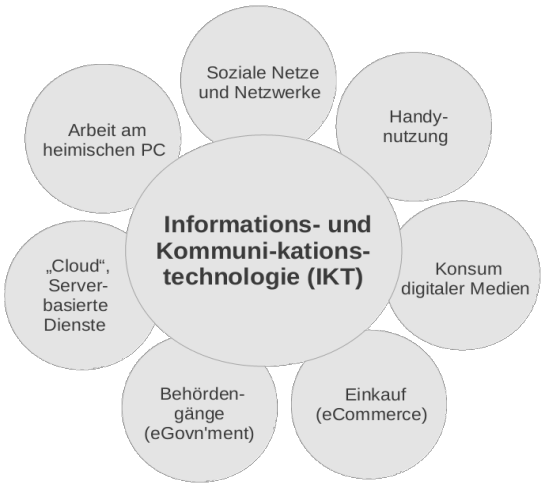

Abb. 1: Beispiele für informationstechnische Systeme einer Person (Quelle: Autor)

„den Umständen nach davon ausgehen dürfen, dass sie darüber selbstbestimmt verfügen“, so muss betrachtet werden, unter welchen Umständen wovon realistischerweise ausgegangen werden darf. Abb. 1 verdeutlicht in einer notwendigerweise unvollständigen Darstellung die Vielzahl informationstechnischer Systeme für eine einzige Person.

2. Geheimdienstexkurs: National Security Agency (NSA), Government Communications Headquarters (GCHQ) und Co.

Die Erkenntnisse über die Machenschaften US-amerikanischer, britischer, kanadischer, australischer und neuseeländischer Geheimdienste (die sogenannten „five eyes“) erhielten ohne Zweifel durch die (nach wie vor andauernden) Enthüllungen *Edward Snowdens* eine neue Detailtiefe. Aufgedeckte Programme wie PRISM, die den Diensten den vollständigen Direktzugriff auf die Daten bei Apple (iCloud), Google (gmail, Google calendar, youtube, Google docs), Facebook, Skype und Microsoft (Office 365) ermöglichen, ließen die Produkte der Informatik in einen neuen Licht erscheinen. Was bis dato von vielen aufmerksamen Kritikern vermutet worden war, wurde nun zu politisch diskutierbarem Wissen über die tatsächlichen „Umstände“ global vernetzter Informationsverarbeitung. Auch die Metadaten der Festnetz- und Mobiltelefonsysteme ganzer Länder landen in den Datensilos der Gemeindienste, Internetverbindungsmetadaten (z. B. HTTP-Header) durch die Zusammen-arbeit mit Providern wie Verizon oder Orange sowieso.

Auch die Rohdatenströme des Internets werden direkt an den interkontinentalen Kabelverbindungen analysiert und nach Bedarf ausgeleitet; Programme wie Tempora oder Upstream sorgen dafür, dass NSA-Rechenzentren wie das Utah-Data-Center in Bluffdale, Utah sich stetig ihrem Ziel annähern, den gesamten Internetverkehr für 100 Jahre zu speichern. Vor diesem Hintergrund wirkt der millionenfache Direktabgriff von Webcam-Daten des Yahoo-Videochat-Dienstes wie ein Trainingsmanöver.

2.1 Aktives Infiltrieren von Einzelsystemen und Infrastruktur

Doch die Zugriffe gehen weit über das passive Abgreifen von Datenströmen hinaus. Die Geheimdienste pflegen Exploitdatenbanken für Mobilsysteme wie Blackberry, Google Android, Apple iOS. Aber auch die Zusammenarbeit mit Herstellern wie Microsoft (MAPP-Programm) versorgt sie mit Möglichkeiten, verdeckt informationstechnische Systeme gezielt und großflächig zu infiltrieren. Auch der automatisierte Aufbau NSA-eigener Botnetze durch sogenannte Tailored Access Operations (TAO) ist nun gut dokumentiert. Programme wie QuantumInsert sorgen zudem durch die Imitation von Facebookservern dafür, dass Malware gezielt platziert werden kann. Übergeordnetes Ziel ist es, jedes netzwerkfähige Gerät weltweit verfolgen, einer Person zuweisen und bei Bedarf übernehmen zu können (Programm Treasuremap).

3.2 Manipulation von technischen Standards

Weiterhin ist auch die Beeinflussung des US-amerikanischen National Institute of Standards and Technology (NIST), das weltweit verwendete technische Standards definiert, öffentlich geworden. Dabei waren u. a. (zu) geringe Schlüssellängen (Data Encryption Standard [DES], Ende des letzten Jahrhunderts) und unsichere Zufallsgeneratoren (Dual_EC_DRBG, aktuell) die Folge.

Auch die direkte Zusammenarbeit mit Technologiefirmen für den Einbau von „Hintertüren“ wurde bekannt. So hatte die Firma RSA gegen eine Zahlung von zehn Millionen US-Dollar den oben angesprochenen unsicheren Zufallsgenerator in ihren Produkten als Standard konfiguriert. Und wo es nicht anders ging, wurden verdeckte Agenten in Technologiefirmen eingeschleust, um SSL/TLS-Schlüssel oder X.509-Zertifikate zu erbeuten, mit denen man verschlüsselte Verbindungen brechen kann.

Abgerundet wird die nahezu vollständige Datensammlung durch ein mächtiges Suchwerkzeug namens X-Keyscore, das ähnlich einer Bibliothekskatalogsuche alle Datenbestände wohl strukturiert durchsuchen kann. X-Keyscore basiert im Übrigen gänzlich auf freier Software.

3. Geheimdienstexkurs: Bundesnachrichtendienst (BND) und Bundesamt für Verfassungsschutz (BfV)

Auch wenn es angesichts der obigen Aufzählung so scheinen mag, als ob die verantwortlichen Stellen, die dafür sorgen, dass es keine Erwartung irgendeiner Sicherheit informationstechnischer Systeme geben könnte, ausschließlich jenseits des Atlantiks oder auf den britischen Inseln zu finden wären, doch Deutschlands Rolle in diesem Spiel ist keine passive oder gar opferhafte. Es agiert willentlich als Unterstützer globaler geheimdienstlicher Aktivitäten und hilft aktiv bei der *Ausspähung* der deutschen Politik, Wirtschaft und Bevölkerung gleichermaßen (vgl. FIfF-Kommunikation 1/2015, S. 35 ff.).

So leitete der BND am DE-CIX (Frankfurt a. M.) abgegriffene Daten von 2004 bis 2008 direkt an die NSA, genannt Operation „Eikonal“. Die „Selektoren“ genannten *Suchbegriffe* sind bis zum heutigen Tage trotz dringender Nachfragen des 1. Parlamentarischen Untersuchungsausschusses („NSA-Ausschuss") nicht öffentlich gemacht worden, da die Bundesregierung in totaler Blockadehaltung verharrt und mit Völkerrechts- und Dateneigentumsausflüchten versucht, sich aus der Verantwortung zu winden. Unter den Selektoren, die dennoch ihren Weg an die Öffentlichkeit fanden, finden sich wenig

überraschend die Namen von einflussreichen Personen aus der deutschen Politik genauso wie deutsche Firmen- und Produktnamen. Eine aktive Komplizenschaft ist demnach aktenkundig.

Zusätzlich verwenden sowohl BND als auch das Bundesamt für Verfassungsschutz (BfV) einen limitierten Zugang zum X-Keyscore-System und sind darüber hinaus in regem Austausch mit ihren US-amerikanischen Kollegen, was jedoch nicht auf die Reduktion der kontinuierlichen Angriffe auf informationstechnische Systeme abzielt(e).

Ganz im Gegenteil; als Reaktion auf die durch die Snowden-Veröffentlichungen belegten massenhaften Eingriffe in sämtliche ITS folgte kein Entwurf einer Defensivstrategie oder ein längst überfälliges Zur-Rechenschaft-Ziehen der entsprechenden US-Stellen, sondern finanzielle Forderungen seitens des BND für den Ausbau der Strategischen Initiative Technik (SIT). In diesem 26 Projekte umfassenden Paket fanden sich z. B. das Projekt SWOP (Operative Unterstützung von Switch-Operationen), womit Netze „fremder“ Internetanbieter infiltriert werden sollten, aber auch ein Projekt, um TLS/SSL-verschlüsselte Verbindungen zu knacken, indem auf dem "graue[n] Markt Informationen über Software-Schwachstellen ein[zu]kaufen" wären. Glücklicherweise (im Sinne des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme) wurde die SIT nicht mit dem geforderten Budget bedacht, dennoch ist die Richtung vorgegeben.

Auch das Bundesamt für Verfassungsschutz arbeitet mit seinem nicht-öffentlichen Haushalt derzeit an der Erstellung einer geheimen Referatsgruppe Erweiterte Fachunterstützung Internet (EFI) zur „Massendatenauswertung von Internetinhalten“, was den veröffentlichenden Journalisten Ermittlungen wegen Landesverrat einbrachte. Von Aktivitäten des Bundesamtes für Verfassungsschutz zum Schutze des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist nichts bekannt.

4. Mindesterwartungen

Kann die zwingende Konsequenz also nur sein, gesellschaftlich keinerlei „Vertraulichkeits- und Integritätserwartung” mehr zu haben? Dieser rein hypothetische Ansatz würde das Grundrecht in seiner jetzigen Form gänzlich ins Leere laufen lassen, aber wenn selbst das Bundesamt für Sicherheit in der Informationstechnik (BSI) schreibt: „Führen Sie Gespräche mit vertraulichem Inhalt nicht über Ihr Mobiltelefon.” (BSI 2015), so schlägt es in die gleiche Kerbe der Ausweglosigkeit. Diese Aussage ist jedoch nicht nur primär hoffnungslos, sie kommt zudem einer kompletten Kapitulation des Politischen gleich. Denn, um mit dem Bundesverfassungsgericht zu sprechen, wie könnte man insgesamt der „allgegenwärtigen Nutzung“ informationstechnischer Systeme entfliehen, wenn sie sämtlich unterwandert sind? Der ehemalige Bundesinnenminister *Friedrich* sagte dazu sinngemäß, man solle eben selbst verschlüsseln. Abgesehen davon, dass auf einem kompromittierten System grundsätzlich keine ordentliche Kryptographie mehr möglich ist (Anderson 2008, S. 147 ff.), verlangt diese Aussage, dass jeder Mensch Kryptoexperte sein sollte. Jeder sollte wissen, welche Schwachstellen gefunden worden sind, welche Verfahren komplett gebrochen worden sind, welche Produkte sich vielleicht gegenseitig stören, welche Implementation zu empfehlen ist usw. Analog dazu könnte man genauso fordern, dass Menschen unbekannt-importierte Medikamente selbst testen, bei jedem Restaurantbesuch die Küche selbst inspizieren oder gefährlich verschmutztes Trinkwasser selbst reinigen. All diese Beispiele verlangen individuelle Expertise auf den jeweiligen Gebieten, weil das Recht des Stärkeren gilt und Arbeitsteilung nicht möglich ist. Das kann kein *modernes Politikverständnis* sein.

Es ist also Vertrauen in staatliche/gesellschaftliche/organisationale Sicherungsstrukturen nötig, und dieses Vertrauen muss auch verdient werden, aber sicherlich nicht, indem das BSI (Schutz der Bürger) dem Innenministerium (Strafverfolgung, BKA, Staatstrojaner) unterstellt ist.

5. Gewährleistungsansprüche

Wie kann man aber konkret die „Gewährleistung“ im neuen Grundrecht verstehen? Grundrechte haben immer auch einen „Ermöglichungsaspekt“ („status positivus"), sie können in gewissem Umfang auch als Leistungsrechte verstanden werden. In eng definierten Bereichen oder wohldiskutierten Interpretatonen können folglich staatliche Handlungspflichten abgeleitet werden. Aus dem Grundrecht auf ~~K~~körperliche Unversehrtheit erwachsen beispielsweise anerkanntermaßen Ansprüche auf eine funktionierende Gesundheitsversorgung, aber auch die Schulpflicht, das Asylrecht oder der Schutz von Ehe und Familie entspringen dem Ermöglichungsaspekt bestimmter Grundrechte.

Gestützt wird dieses Konzept vom sogenannten Untermaßverbot. Als Gegenstück zum Übermaßverbot, was durch die Erforderlichkeit (im engeren Sinne) bei der Verhältnismäßigkeitsabwägung von Maßnahmen „Überreaktionen“ staatlichen Handelns verhindern soll, ist die Zielrichtung des Untermaßverbotes, dass staatliches Handeln rechtlich zugesicherte Mindeststandards faktisch realisiert. Das Bundesverfassungsgericht dazu: „Der Staat muss zur Erfüllung seiner Schutzpflicht ausreichende Maßnahmen normativer und tatsächlicher Art ergreifen, die dazu führen, dass ein – unter Berücksichtigung entgegenstehender Rechtsgüter – angemessener und als solcher wirksamer Schutz erreichbar wird." (BVerfG 1993, Leitsatz 6).

6. Konkrete Handlungsansätze

Tatsächlich ist es juristisch schwierig, staatliche Versäumnisse („Grundrechtsverletzungen durch Unterlassen“) bei der Umsetzung des Grundrechtes auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einzuklagen. Handlungsansätze wären z. B. eine echte Digitale Agenda, die nicht nur „aktiv begleitet", sondern politisch gestaltet; ein echtes IT-Sicherheitsgesetz, das Sicherheitsvorfälle

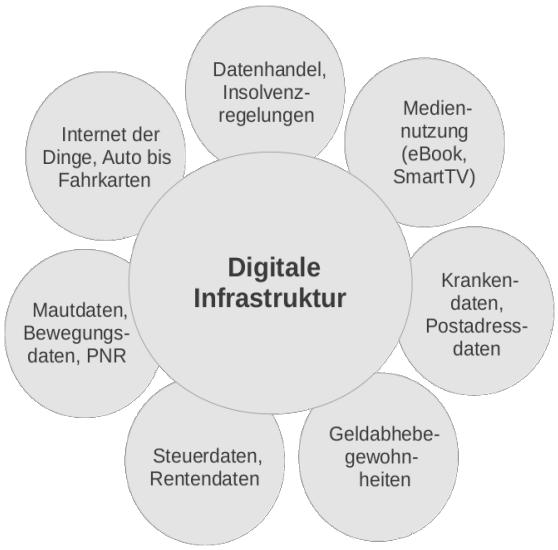

Abb. 2: Informationstechnische Systeme, bei denen keine „Selbstverteidigung“ möglich ist

(Quelle: Autor)

offen kommuniziert; ein Konzept, um Schwarzmärkte für Exploits etc. auszutrocknen, anstatt solche Märkte durch Käufe der eigenen Dienste zu vergrößern oder überhaupt erst zu erzeugen; ein Vorantreiben der Softwarehaftung für proprietäre Software (freie Software kann auditiert werden, proprietäre nicht); das Bundesamt für Sicherheit in der Informationstechnik (BSI) aus seinem Zielkonflikt lösen (Bundesministerium des Innern/Geheimdienste gegen den Schutz der Bürger vor Zugriffen auf ihre ITS); Förderung von freier Software, aber effektive Förderung und nicht mit so halbherzigen Empfehlungen wie im „Kompetenzzentrum OSS", und man kann natürlich staatlich finanzierte Audits von großen,

verbreiteten freien Projekten durchführen, aber vor allem kann man bezüglich dieses Grundrechtes die Zusammenarbeit mit fremden Diensten abstellen und dadurch die selbstverursachte politische Ohnmächtigkeit ablegen, vgl. Abb. 2.

7. Den Blick erweitern, was fehlt noch?

Es bleibt festzustellen, dass die Blickrichtung des Grundrechtes auf Gewährleistung der *Vertraulichkeit* und *Integrität* informationstechnischer Systeme zentral auf das Individuum und dessen Persönlichkeitsentfaltung abstellt, wobei der Kernbereich privater Lebensgestaltung dabei eine wesentliche Rolle spielt. Das ist verständlich, folgt doch das Grundgesetz grundsätzlich einer sehr individualistischen Gesellschaftsdoktrin (bis auf Umweltschutz und Tierrechte). Dennoch oder gerade deswegen muss perspektivisch immer auch auf systemische oder emergente – nennen wir sie einfach gesellschaftliche – Effekte automatisierter Informationsverarbeitung und Entscheidungsproduktion (Pohle 2015, S. 5) hingewiesen werden, denn diese stellen die zweite Seite der Medaille „Datenschutz-Datensicherheit“ dar (vgl. Kühne 2015, S. 64 ff.). Diese zweite Seite kann man nicht durch individuelle Initiative in den Griff bekommen (siehe Abb. 2).

Literatur

Anderson, Ross (2008) *Security Engineering, A Guide to Build Dependable Distributed Systems.* 2. Auflage. Indianapolis: Wiley

BSI (2015) : Bundesamt für Sicherheit in der Informationstechnik *Sicher Unterwegs mit Smartphone & Co.* Broschüre, 09. 02. 2015

BVerfG (2008): Bundesverfassungsgericht *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung.* BVerfG, 1 BvR 370/07, 27. 02. 2008

BVerfG (1993): Bundesverfassungsgericht *Bundesverfassungsgerichtsurteil zum Schwangerschaftsabbruch II.* BVerfGE 88, 203, 28. 05. 1993

BVerfG (1983): Bundesverfassungsgericht *Bundesverfassungsgerichtsurteil zur Volkszählung.* 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1, 15. 12. 1983

dpa (2007): Deutsche Presse Agentur *Geheimdienste spitzeln schon seit Jahren.* Stern.de, 25. 04. 2007

FIfF-Kommunikation (1/2015), Schwerpunkt FIfF-Konferenz 2014, ISSN 0938-3476

Kühne, Christian (2015) *GNUnet und Informationsmacht: Analyse einer P2P-Technologie und ihrer sozialen Wirkung. MV-Wissenschaft, Münster: Monsenstein und Vannerdat, erwartet 2015*

Pfitzmann, Andreas (2007) *Rede vor dem Bundesverfassungsgericht als Sachverständiger zur Online-Durchsuchung.* Karlsruhe, veröffentlichtes Redemanuskript, 10.10.2007

Pohle, Jörg (2015) *Die kategoriale Trennung zwischen »öffentlich« und »privat« ist durch die Digitalisierung aller Lebensbereiche überholt – Über einen bislang ignorierten Paradigmenwechsel in der Datenschutzdebatte.* In »Worüber reden wir eigentlich?« Festgabe für Rosemarie *Will; Hrsg: Plöse, Michael and Lüders, Sven and Fritsche, Thomas and Kuhn, Michael and Zado, Julian, Berlin, erwartet 2015*

Rehak, Rainer (2013) *Angezapft! Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung.* MV-Wissenschaft, Münster: Monsenstein und Vannerdat, 2013