SSOAR

Open Access Repository
www.ssoar.info

Digitalisierungsinduzierte Interessenkonflikte als Herausforderung für Staat und Gesellschaft: Ein Problemaufriss am Beispiel der Anforderungen von Datenschützern, Sicherheitsbehörden und Datenwirtschaft an den Einsatz elektronischer Kryptographie

Winkel, Olaf

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Verlag Barbara Budrich

Empfohlene Zitierung / Suggested Citation:
Winkel, O. (2022). Digitalisierungsinduzierte Interessenkonflikte als Herausforderung für Staat und Gesellschaft: Ein Problemaufriss am Beispiel der Anforderungen von Datenschützern, Sicherheitsbehörden und Datenwirtschaft an den Einsatz elektronischer Kryptographie. *der moderne staat - dms: Zeitschrift für Public Policy, Recht und Management*, *15*(1), 233-252. https://doi.org/10.3224/dms.v15i1.02

Nutzungsbedingungen:
Dieser Text wird unter einer CC BY Lizenz (Namensnennung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:
https://creativecommons.org/licenses/by/4.0/deed.de

Terms of use:
This document is made available under a CC BY Licence (Attribution). For more Information see:
https://creativecommons.org/licenses/by/4.0

gesis Leibniz-Institut für Sozialwissenschaften

Mitglied der Leibniz-Gemeinschaft

Diese Version ist zitierbar unter / This version is citable under:
https://nbn-resolving.org/urn:nbn:de:0168-ssoar-97294-4

Essay

Olaf Winkel

Digitalisierungsinduzierte Interessenkonflikte als Herausforderung für Staat und Gesellschaft

Ein Problemaufriss am Beispiel der Anforderungen von Datenschützern, Sicherheitsbehörden und Datenwirtschaft an den Einsatz elektronischer Kryptographie

Zusammenfassung
Im Mittelpunkt des Beitrags stehen die Anforderungen, die Datenschützer, Sicherheitspolitiker und Vertreter der Datenwirtschaft an den Einsatz von elektronischer Kryptographie richten. Elektronische Kryptographie kann digitales Signieren, den Schutz vertraulicher Inhalte und anonyme Kommunikation im Internet gleichermaßen unterstützen. Die Aufarbeitung und Kontextualisierung dieser Anforderungen deckt nicht nur erhebliche Interessenkollisionen auf, sondern liefert auch Hinweise auf Ausgleichsmöglichkeiten der divergierenden Positionen. Vieles spricht dafür, eine unabhängige neue Behörde zu schaffen, die für die Bearbeitung der im Kontext von informationstechnischen Innovationen auftretenden Sicherheitsprobleme zuständig ist und in der die Bearbeitung der Sicherheitsprobleme weniger als ingenieurtechnische denn als sozialtechnische Herausforderung verstanden wird. Dabei resultiert die Relevanz des Beitrags nicht allein daraus, dass darin ein zunehmend bedeutsames und dennoch bislang weitgehend unterbelichtetes Handlungsfeld ausgeleuchtet wird. Hinzu kommt, dass die darin aufgeworfenen Fragen auf das Metaproblem eines digitalisierungsinduzierten Anwachsens schwer handhabbarer Interessenkonflikte verweisen, die sich ohne Innovationen zur Erhöhung der gesellschaftlichen Problembearbeitungsfähigkeit kaum adäquat bearbeiten lassen.

Schlagworte: Digitalisierung; Interessenkonflikte; Elektronische Kryptographie; Problembearbeitungskapazität; Governance

Abstract
The requirements for the use of electronic cryptography made by data protectionists, security authorities, and the data industry as an example for digitization-induced conflicts of interest as a challenge for state and society
This article focuses on the requirements that privacy advocates, security politicians, and representatives of the data industry place on the use of electronic cryptography, which can support digital signing, the protection of confidential content and anonymous communication on the Internet. The compilation and contextualization of these requirements not only reveal considerable conflicts of interest, but also provide indications of ways to improve the reconciliation of divergent positions. There are good reasons for the creation of a new and independent agency, that is responsible for processing security problems arising in the context of information technology innovations, and where the handling of security problems is seen less as an engineering challenge than as a socio-technical challenge. This article is not only relevant because it sheds light on an increasingly important field of action, which remains underexplored to date. In addition, the questions raised point to the metaproblem of a digitization-induced increase in conflicts of interest which are difficult to manage and can hardly be adequately addressed without innovations to increase the societal problem-solving ability.

Keywords: Digitization; Conflicts of interest; Electronic cryptography; Problem-solving capacity; Governance

1 Einführung

Im Mittelpunkt der vorliegenden Untersuchung stehen die Anforderungen, die unter Aspekten von Privatheit, öffentlicher Sicherheit und wirtschaftlichem Profitstreben an den Einsatz von elektronischer Kryptographie gerichtet werden. Dabei handelt es sich um eine Basistechnologie der digitalen Informationsgesellschaft, die elektronisches Signieren, den Schutz vertraulicher Inhalte und anonyme Kommunikation im Internet gleichermaßen unterstützen kann. Die Untersuchung gliedert sich in unterschiedliche Arbeitsschritte, die unmittelbar aufeinander aufbauen. Zuerst werden einige konfliktträchtige Entwicklungen thematisiert, die mit der zunehmenden Verlagerung sozialer Funktionen in elektronische Netzwerke einhergehen. Dann werden zentrale Belange von Privatheit, öffentlicher Sicherheit und wirtschaftlichem Profitstreben ausgeleuchtet, die jeweils für sich selbst als durchaus legitime Interessen angesehen werden können. Daran schließt sich eine Auseinandersetzung mit den wesentlichen Merkmalen und Funktionalitäten der elektronischen Kryptographie an, wobei die Software und die für deren Entwicklung und Bereitstellung erforderliche Infrastruktur gleichermaßen Beachtung finden. In weiteren Schritten werden die Anforderungen herausgearbeitet, die von Protagonisten von Privatheit, öffentlicher Sicherheit und wirtschaftlichem Profitstreben an die gesellschaftliche Nutzung von Kryptographie gerichtet werden, und Überlegungen dazu angestellt, was die Folgen wären, wenn eines der konkurrierenden Lager die Möglichkeit erhielte, die eigene Position umfassend und kompromisslos durchzusetzen. Weil die dabei aufscheinenden Extremszenarien Strukturelemente aufweisen, die denen des Darknet, des chinesischen Netzes und des zunehmend von US-amerikanischen Konzernen dominierten Internet der westlichen Welt ähneln, werden deren Konturen ebenfalls umrissen. An die Aufdeckung der zentralen Probleme schließen sich Überlegungen zu der Frage an, wie einem verbesserten Ausgleich der kryptologiebezogenen Interessen von Privatheit, öffentlicher Sicherheit und wirtschaftlichem Profitstreben über institutionelle und kulturelle Innovationen Vorschub geleistet werden könnte. Dies geschieht unter der Prämisse, dass die dabei gewonnenen Einblicke nicht nur hinsichtlich des hier in den Fokus gerückten Politikfelds von Bedeutung sind, sondern auf ein digitalisierungsinduziertes Metaproblem und einen entsprechenden gesellschaftlichen und politischen Handlungsbedarf verweisen, die bislang noch zu wenig Beachtung gefunden haben.

2 Interessenkonflikte in der digitalen Informationsgesellschaft

Aus einer technischen Perspektive steht Digitalisierung für die Umwandlung von analogen Daten in ein von der binären Logik bestimmtes elektronisches Format, das einer maschinellen Bearbeitung besser zugänglich ist (siehe Mattelart, 2003, S. 9 f.; VDE, 2018, S. 5). Aus einer soziologischen Perspektive verweist dieser Begriff auf die Verlagerung überkommener Interaktionen in elektronische Netzwerke, die gravierende soziale Konsequenzen mit sich bringt, weil die Merkmale des virtuellen Raums damit sukzessive zu Merkmalen der Gesellschaft selbst werden (siehe Bridle, 2020, S. 27 ff.; Hirsch-Kreinsen, 2016, S. 10; Mau, 2018, S. 40 ff.).

Eine bislang noch wissenschaftlich unterbelichtete, aber dennoch in ihren Auswirkungen kaum zu überschätzende Folge dieser Entwicklung besteht darin, dass im Über-

gang zur digitalen Informationsgesellschaft vermehrt Interessenkonflikte auftreten und dass es immer schwerer fällt, diese aufzulösen oder zumindest einzuhegen.[1]

Die Zunahme von Interessenkonflikten ist vor allem darauf zurückzuführen, dass die Verlagerung überkommener Interaktionsbeziehungen in elektronische Netzwerke sozialer Ausdifferenzierung Vorschub leistet, weil grenzüberschreitend angelegte virtuelle Räume Gleichgesinnten bislang nie gekannte Möglichkeiten bieten, zueinander zu finden, sich auszutauschen und auch eine über die Netzwelt hinausreichende Anschlusskommunikation zu organisieren (siehe Winkel, 2018, S. 117; Winkel, 2020, S. 72 ff.). Die digitaltechnisch induzierte Ausbildung von Subkulturen und das damit verbundene Auseinanderfallen von ehemals geteilten Werthaltungen, Einstellungen und Problemwahrnehmungen lässt wiederum den Vorrat an gemeinsamen Interessen abnehmen bzw. leistet der Herausbildung von Sonderinteressen Vorschub.

Dass es im Übergang vom Analogen zum Digitalen immer schwerer fällt, soziale Konflikte aufzulösen oder zumindest einzuhegen, hat seine Ursache darin, dass die Funktionalitäten elektronischer Netzwerke zunehmend von der Software bestimmt werden, die anders als die Hardware keiner fixen technischen, sondern einer disponiblen sozialen Logik folgt. Da ein konventioneller Softwarealgorithmus nichts anderes ist als eine von Programmierern[2] entworfene „Anleitung zur Lösung einer Aufgabenstellung“ (Pomberger & Dobler, 2008, S. 29), die „vollständige, präzise und endliche Handlungsanweisungen“ (Etscheid, 2018, S. 140) zu deren schrittweiser Bearbeitung enthält[3], wachsen im Übergang zur digitalen Informationsgesellschaft die Möglichkeiten, politische Ziele, Organisationsstrukturen, Organisationsverfahren, Geschäftsmodelle und vieles andere nach dem Prinzip von „Code is Law“ (Lessig, 2001) sozusagen in Software zu gießen und damit sozial verbindlich zu machen (siehe auch Katzenbach, 2018, S. 315 ff.; Lehner, 2018, S. 17 ff.).

So ist der Umstand, dass Nutzer der Google-Suchmaschine die Vorteile einer durch Algorithmen gestützten Recherche mit der Preisgabe aller damit verbundenen persönlichen Daten bezahlen müssen, nicht auf einen technischen Sachzwang, sondern auf eine menschliche Entscheidung zurückzuführen. Natürlich kann eine Suchmaschine prinzipiell auch so konzipiert werden, dass die Kommunikationsakte und Kommunikationsinhalte der Nutzer vertraulich bleiben.

Zu beachten ist dabei, dass sich gesellschaftliche Verhältnisse über die Gestaltung von Software und der zu ihrer Bereitstellung erforderlichen Infrastruktur weitaus effektiver beeinflussen lassen als mit analog basierten Verfahren von Regelsetzung, Überprüfung der Regeltreue und Sanktionierung abweichenden Verhaltens, wie man sie aus überkommenen Formen des bürokratischen Zentralismus kennt. Denn anders als Algorithmen, die Prozesse in Echtzeit steuern und kontrollieren, können Hierarchien, in denen Menschen Weisungen geben und eine nachgelagerte Kontrolle ausüben, in vielfältiger Weise umgangen, getäuscht oder außer Kraft gesetzt werden.

Wenn aber ein Ziel, das zu einem anderen in Konkurrenz steht, quasi in die Software hineingeschrieben und damit weitaus effektiver als in der Vergangenheit verfolgt werden kann, bedeutet dies natürlich auch, dass im Hinblick auf das konkurrierende Ziel erhebliche Rückschritte hinzunehmen sind (siehe Winkel, 2004, S. 10 f.; Winkel, 2018, S. 125 ff.; Winkel, 2020, S. 73 ff.). Auch hier kann ein Verweis auf Google der Veranschaulichung dienen: In dem Maße, wie jeder Suchvorgang zur Erreichung des Ziels beiträgt, den Unternehmensgewinn zu maximieren, wird das konkurrierende Ziel verfehlt, die informationelle Selbstbestimmung der Suchenden aufrechtzuerhalten. Auf diese Wei-

se ersetzt das Entweder-oder im Übergang vom Analogen zum Digitalen sukzessive das Sowohl-als-auch als Strukturprinzip liberaler Gesellschaften. Die Folge davon ist nicht nur, dass es wegen der großen Durchschlagskraft „algorithmischer Macht" (Katzenbach, 2018, S. 319) immer schwieriger wird, Konflikte durch Kompromisse zu entschärfen, sondern auch, dass gegenläufige Interessen von den Gesellschaftsmitgliedern zunehmend als existentielle Bedrohung wahrgenommen werden, was es ihnen immer schwerer macht, Verständnis für abweichende Wahrnehmungen und Werthaltungen aufzubringen.

3 Privatheit, öffentliche Sicherheit und Profitstreben in der digitalen Informationsgesellschaft

Datenschutz zielt auf die Sicherung der Privatsphäre ab. Als Privatsphäre wird ein nichtöffentlicher Bereich bezeichnet, in dem Menschen unbehelligt von äußeren Einflüssen und Kontrollen ihre Persönlichkeit frei entfalten können (siehe Glaeßner, 2016, S. 88 ff.; Kutscha, 2010, S. 112 ff.; Lewinski, 2012, S. 23 ff.). Der Anspruch auf Privatheit gilt als Menschenrecht und seine Gewährleistung unter anderem auch als Voraussetzung für das Funktionieren der demokratischen Willensbildung (siehe Becker & Seubert, 2019, S. 232 ff.). Aus der Verlagerung zentraler sozialer Funktionen in elektronische Netzwerke erwachsen aber gravierende Bedrohungen für die Privatsphäre. Die Digitalisierung eröffnet Außenstehenden immense neue Möglichkeiten, Kommunikationsverläufe nachzuvollziehen und vertrauliche Informationen auszuspähen. Hinzu kommt, dass die zunehmende Nutzung mobiler Endgeräte dazu führt, dass Kommunikationsprofile um Daten aus Bewegungsprofilen angereichert werden können. Neue technische Instrumente, wie man sie mit Begriffen wie Künstliche Intelligenz und Big Data verbindet, ermöglichen die Auswertung der auf diese Weise gewonnenen Informationen und ihre Verdichtung zu Persönlichkeitsprofilen in einem bislang nie gekannten Ausmaß.

Die Gewährleistung öffentlicher Sicherheit umfasst den Schutz der verfassungsmäßigen Ordnung, des Staates und seiner Einrichtungen und der materiellen und immateriellen Rechtsgüter der Gesellschaftsmitglieder (siehe Eichhorn, 2002, S. 753). Unter den veränderten Vorzeichen einer digitalen Informationsgesellschaft erfordert die Aufrechterhaltung öffentlicher Sicherheit auch den Schutz kritischer Infrastrukturen und die Bekämpfung neuer Kriminalitätsformen.

Kritisch erscheinen Infrastrukturen wie das Energiewesen, das Verkehrswesen oder das Gesundheitswesen gleich in doppelter Weise; nämlich einerseits, weil sie Lebensadern darstellen, ohne die moderne Gesellschaften nicht existieren können, und andererseits, weil sie selbst ohne eine verlässliche Digitaltechnik nicht funktionsfähig sind (siehe BMI, 2009; BSI, 2015, S. 40 ff.; Schulze, 2006).

Internetkriminalität umfasst eine breite Palette von Straftaten einschließlich Datendiebstahl, Identitätsdiebstahl, Urheberrechtsverletzung, Beleidigung, Volksverhetzung, Betrug, Erpressung, Anbahnung des Handels mit Waffen oder Drogen und Verbreitung von Kinderpornographie (siehe Rieckmann & Kraus, 2015, S. 295 ff.; Walter, 2008, S. 12 ff.; Wernert, 2017). Zu den Maßnahmen, die sich zur Sicherung kritischer Infrastrukturen und zum Kampf gegen Internetkriminalität eignen, zählen auch die Beobachtung möglicher Gefahrenquellen und die Zusammenführung und Auswertung der dabei gewonnenen Daten.

Mit der Digitalisierung geht eine wirtschaftliche Globalisierung einher, die ökonomische Handlungsimperative zu einer zentralen Triebkraft der gesellschaftlichen Entwicklung macht. Dabei etabliert sich Wissen über die Gesellschaftsmitglieder als neue „Schlüsselressource", die Unternehmen enorme Profite und Volkswirtschaften „ein schier unglaubliches Wachstum" in Aussicht stellt (ISST, 2019, S. 5). Als besonders ertragreiches Geschäftsfeld der inzwischen allgegenwärtigen Datenwirtschaft gilt die personalisierte Werbung. Dabei sind Internetgiganten wie Alphabet, Amazon und Facebook lediglich Vorreiter einer fast alle Wirtschaftsbereiche umfassenden Bewegung. Inzwischen setzen „Unternehmen aus allen Branchen" auf „datengetriebene Geschäftsmodelle" (Akzan, Iggena, Korte & Spiekermann, 2019, S. 5; siehe auch Goecke, Lichtblau, Schleiermacher & Schützdeller, 2018, S. 14 ff.; Hoffmann & Schröder, 2019, S. 277 ff.). Die Profite der Datenwirtschaft fallen umso größer aus, desto weniger sie daran gehindert wird, Einblick in die Lebensweisen und Lebensperspektiven der Gesellschaftsmitglieder zu nehmen.

Dass der Übergang zur digitalen Informationsgesellschaft geeignet ist, auch Interessenkonflikte zwischen den für sich selbst legitimen Interessen der Wahrung von Privatheit, der Aufrechterhaltung von öffentlicher Sicherheit und der freien wirtschaftlichen Betätigung anzuheizen, steht außer Frage. So ist offensichtlich, dass Maßnahmen zum Schutz der Privatsphäre nicht nur Belangen der öffentlichen Sicherheit, sondern auch Belangen der Datenwirtschaft zuwiderlaufen können, und dass Maßnahmen zur Gewährleistung öffentlicher Sicherheit nicht nur Belange des Datenschutzes, sondern auch Belange der Datenwirtschaft beeinträchtigen können. Wie tiefgreifend und komplex die in diesen Feldern auftretenden Konflikte sind und wie schwer es fällt, sie über Kompromisse oder Kompensationen zu entschärfen, zeigt eine nähere Betrachtung der Anforderungen, die von den unterschiedlichen Seiten an den Einsatz von elektronischer Kryptographie gerichtet werden.

4 Elektronische Kryptographie – Software und Infrastruktur

Kryptographie steht für die Verschlüsselung und Entschlüsselung von Nachrichten (siehe Beutelspacher, 2015, S. 2 f.; Küsters & Wilke, 2011, S. 7). Verschlüsselung nennt man einen Vorgang, bei dem für Menschen oder Maschinen lesbare Informationen, der sogenannte Klartext, in unlesbare Zeichenfolgen umgewandelt werden, den sogenannten Geheimtext oder Schlüsseltext. Den umgekehrten Prozess, also die Transformation von Geheimtext zurück in Klartext, nennt man Entschlüsselung.

Schon im Altertum wurden vertrauliche Informationen verschlüsselt, um sie vor der unerwünschten Kenntnisnahme Dritter zu schützen (siehe Beutelspacher, 2017, S. 35 ff.; Singh, 2017, S. 15 ff.). Bis zum Beginn des zwanzigsten Jahrhunderts geschah dies mittels Stift und Papier oder mechanischer Scheiben. Später wurden dazu spezielle Maschinen eingesetzt, von denen die von der deutschen Marine im Zweiten Weltkrieg genutzte Enigma die bekannteste ist. Anfang der siebziger Jahre mussten die Verschlüsselungsmaschinen Computern weichen, die im Laufe der Zeit immer leistungsfähiger wurden.

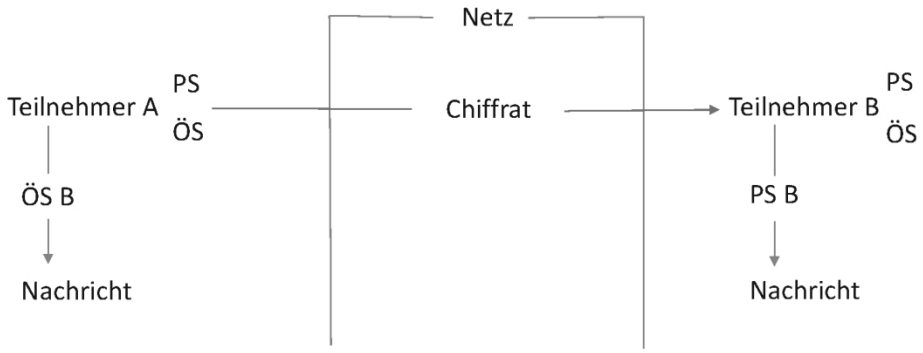
Kryptographiesoftware arbeitet mit hochkomplexen mathematischen Operationen, die vom Anwender unbeobachtet ablaufen (siehe Federrath & Pfitzmann, 2006, S. 279 ff.; Singh, 2017, S. 295 ff.). Weil der unautorisierte Zugriff auf verschlüsselte Informationen mit zunehmender Schlüssellänge, die sich an der Bitzahl ablesen lässt, immer schwie-

riger und letztlich nahezu unmöglich wird, werden in der elektronischen Kryptographie Berechnungen angestellt, die Zahlen mit mehreren hundert Dezimalstellen verwenden.

Elektronische Verschlüsselung und Entschlüsselung kann sowohl in der symmetrischen als auch in der asymmetrischen Variante eingesetzt werden.[4] Während symmetrische Schlüsselsysteme auf den Schutz vertraulicher Informationen beschränkt sind, kann mittels asymmetrischer Systeme darüber hinaus eine verbindliche und integre Kommunikation sichergestellt werden (siehe Spitz, Pramateftakis & Swoboda, 2011, S. 14 ff.). Verbindlich sind kommunizierte Inhalte, wenn sie sich den Kommunikationspartnern verlässlich bzw. nachweisbar zuordnen lassen. Integrität steht für die unverfälschte Übertragung von Nachrichten zwischen berechtigten Partnern.

Bei der Anwendung symmetrischer Schlüsselverfahren (siehe Federrath & Pfitzmann, 2006, S. 279; Küsters & Wilke, 2011, S. 13 ff.) verfügen die Kommunikationsteilnehmer über identische Schlüssel, mit denen sie jeweils die füreinander bestimmten Nachrichten verschlüsseln oder entschlüsseln können. Der gravierende Nachteil dieser ansonsten effektiven und effizienten vertraulichkeitsschützenden Verfahren liegt darin, dass sie einen netzexternen Schlüsseltausch vor Aufnahme der Kommunikation voraussetzen.

Abbildung 1: Grundprinzip symmetrische Verschlüsselung zum Vertraulichkeitsschutz



Legende: PS = Privater Schlüssel, ÖS = Öffentlicher Schlüssel

Weil A zur Verschlüsselung der Nachricht den öffentlichen Schlüssel von B benutzt, der nur mit dem privaten Schlüssel von B entschlüsselt werden kann, den allein B besitzt, kann die Nachricht im Netz wohl abgefangen, aber nicht gelesen werden, so dass A bereits bei der Absendung der chiffrierten Nachricht sicher sein kann, dass ihre Vertraulichkeit gewahrt bleibt.

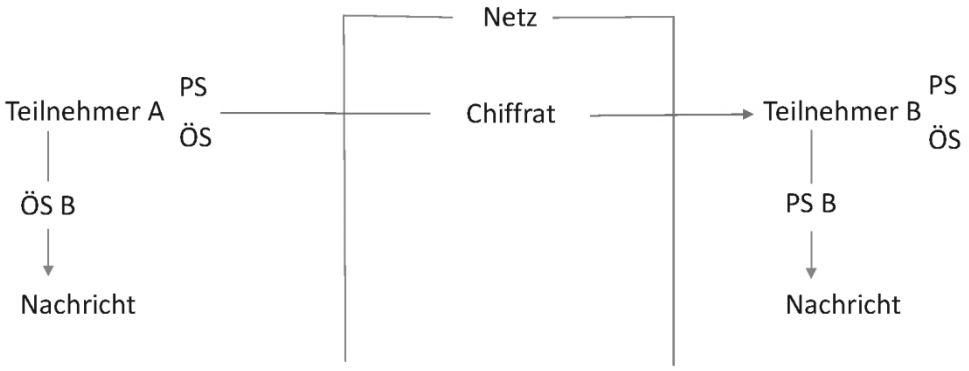
Quelle: Eigene Darstellung.

Bei asymmetrischen Schlüsselverfahren, die nicht mit identischen, sondern mit komplementären Schlüsselpaaren arbeiten[5], fällt diese Einschränkung weg (siehe Federrath & Pfitzmann, 2006, S. 279 f.; Küsters & Wilke, 2011, S. 137 ff.). Durch ihre Entwicklung sind daher die technischen Voraussetzungen für den flächendeckenden Einsatz von leistungsfähigen Schlüsselsystemen in offenen Netzwerken wie dem Internet geschaffen worden.

Das den asymmetrischen Schlüsselverfahren zugrundeliegende Prinzip ist ebenso einfach wie wirkungsvoll: Ein Telekommunikationsteilnehmer erhält jeweils einen geheimen privaten Schlüssel und einen öffentlichen Schlüssel. Der private Schlüssel bleibt exklusiv beim Teilnehmer, der öffentliche Schlüssel wird anderen Teilnehmern zugänglich gemacht. Dies geschieht nicht durch die Anwender selbst, sondern über die Zwischenschaltung einer speziellen Infrastruktur. Mit dem öffentlichen Schlüssel verschlüsselte Nachrichten können nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden, und mit dem privaten Schlüssel chiffrierte Nachrichten lassen sich nur mit dem komplementären öffentlichen Schlüssel dechiffrieren.

Um eine Nachricht vertraulich im Netz zu übermitteln, verschlüsselt sie der Absender mit dem öffentlichen Schlüssel des Empfängers, bevor sie auf den Weg geht. Nach Erhalt der Nachricht entschlüsselt sie der Empfänger mit seinem privaten Schlüssel. Weil allein der Empfänger den komplementären privaten Schlüssel besitzt, mit dem sich die übertragene Nachricht dechiffrieren lässt, kann der Absender sicher sein, dass die Vertraulichkeit im Übertragungsprozess gewahrt bleibt.

Abbildung 2: Grundprinzip asymmetrische Verschlüsselung zum Vertraulichkeitsschutz



Legende: PS = Privater Schlüssel, ÖS = Öffentlicher Schlüssel

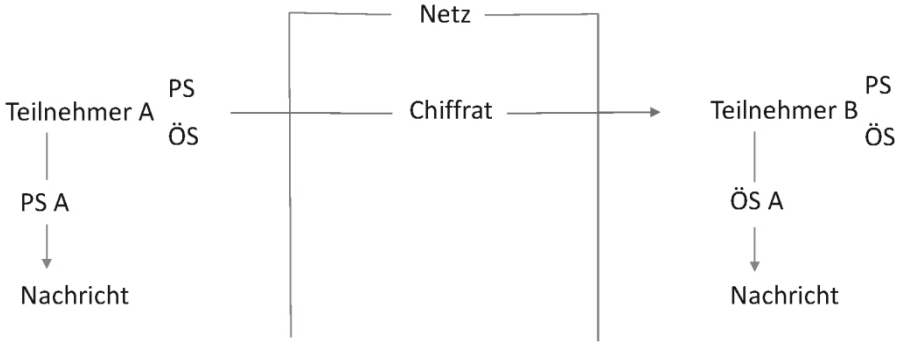
Weil A zur Verschlüsselung der Nachricht den öffentlichen Schlüssel von B benutzt, der nur mit dem privaten Schlüssel von B entschlüsselt werden kann, den allein B besitzt, kann die Nachricht im Netz wohl abgefangen, aber nicht gelesen werden, so dass A bereits bei der Absendung der chiffrierten Nachricht sicher sein kann, dass ihre Vertraulichkeit gewahrt bleibt.

Quelle: Eigene Darstellung.

Die Umkehrung des Verfahrens ermöglicht eine digitale Signatur, mit deren Hilfe rechtsverbindliche Willenserklärungen ausgetauscht werden können. Um eine Nachricht verbindlich im Netz zu übermitteln, verschlüsselt sie der Absender vor der Übertragung mit seinem privaten Schlüssel.[6] Nach Erhalt der Nachricht entschlüsselt sie der Empfänger mit dem öffentlichen Schlüssel des Absenders. Weil eine Nachricht, die der Empfänger mit dem öffentlichen Schlüssel des Absenders entschlüsseln kann, notwendigerweise zuvor mit dem privaten Schlüssel des Absenders verschlüsselt worden sein

muss, über den nur dieser verfügt, kann der Empfänger sicher sein und gegebenenfalls auch gegenüber einem Gericht nachweisen, dass die empfangene Nachricht tatsächlich vom Absender stammt. Während symmetrische Schlüsselsysteme keinen Schutz vor der Manipulation von Nachrichten durch legitime Schlüsselinhaber bieten, bieten asymmetrische Schlüsselsysteme diesen Schutz sehr wohl, weil ein berechtigter Empfänger eine Nachricht lediglich lesen, nicht aber verändern kann.

Abbildung 3: Grundprinzip asymmetrische Verschlüsselung zur verbindlichen Übermittlung



Kurzfassung/Faltung plus Kennung als „Siegel“

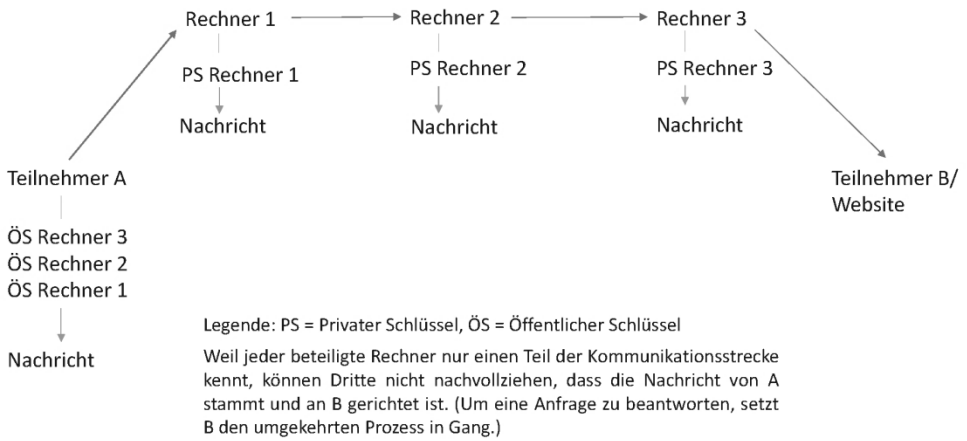
Legende: PS = Privater Schlüssel, ÖS = Öffentlicher Schlüssel

Da eine Nachricht, die B mit dem öffentlichen Schlüssel von A entschlüsseln kann, notwendigerweise zuvor mit dem privaten Schlüssel von A verschlüsselt worden sein muss, und einzig A über diesen Schlüssel verfügt, kann B sicher sein und gegebenenfalls auch nachweisen, dass die empfangene Nachricht von A stammt.

Quelle: Eigene Darstellung.

Dabei setzt die elektronische Kryptographie in der Variante der asymmetrischen Verschlüsselung allerdings eine differenzierte Infrastruktur voraus (siehe Schmeh, 2009, S. 561 ff.). Benötigt werden Einrichtungen, die nicht nur öffentliche Schlüssel allgemein zugänglich machen, sondern auch sichere Schlüsselpaare erzeugen, die Zuordnung von Schlüsselpaaren und Personen garantieren und den Teilnehmern die privaten Schlüssel zur Verfügung stellen.

Abbildung 4: Grundprinzip anonyme Kommunikation mit Tor



Quelle: Eigene Darstellung.

Bei der anonymen Kommunikation mittels Tor-Browser, der Teilnehmern die Möglichkeit bietet, sich in elektronischen Netzwerken zu bewegen, ohne dass die dabei entstehenden Spuren von anderen nachvollzogen und aufgezeichnet werden können, spielt Kryptographiesoftware ebenfalls eine zentrale Rolle. Das Grundprinzip dieser Variante der anonymen Kommunikation lautet folgendermaßen (siehe Krause, 2003, S. 158 ff.; Loshin, 2015, S. 21 ff.; Mey, 2017, S. 4 ff.): Über den Tor-Browser erhalten die Teilnehmer Zugang zu einem Netzwerk aus mehreren tausend Rechnern, denen jeweils komplementäre Schlüsselpaare zugeordnet sind. Eine Nachricht, die unbeobachtbar übermittelt werden soll, wird auf dem Rechner des Absenders mit den öffentlichen Schlüsseln von drei nach dem Zufallsprinzip ausgewählten Rechnern aus dem Tor-Netzwerk verschlüsselt und diesen Rechnern der Reihe nach zugeleitet. Der erste Rechner löst mittels seines privaten Schlüssels die erste Verschlüsselungsschicht auf und leitet das Ergebnis an den zweiten Rechner weiter, welcher mit Hilfe seines privaten Schlüssels die zweite Verschlüsselungsschicht auflöst und das Ergebnis an den dritten Rechner weitergibt, der schließlich mittels seines privaten Schlüssels die dritte Verschlüsselungsschicht auflöst und die Nachricht im Klartext an den Empfänger weiterleitet. Die Anonymität des Absenders bleibt gewahrt, weil die beteiligten Rechner jeweils nur an einem Teil des Kommunikationsprozesses mitwirken. Der erste kann lediglich erkennen, von wem die Nachricht stammt, und der dritte lediglich, an wen sie gerichtet ist.

5 Divergierende Anforderungen an die Nutzung von Kryptographie

Die Verbreitung von Instrumenten für eine verbindliche und integre Kommunikation ist unter Datenschützern, Sicherheitspolitikern und Wirtschaftsvertretern weitaus weniger umstritten als die Verbreitung von Instrumenten, die der Gewährleistung einer vertraulichen Kommunikation dienen. Dass digitale Willenserklärungen etwa mittels De-

Mail (siehe BSI, 2016, S. 8 ff.; BMI, 2016, S. 6 ff.) rechtssicher übermittelt werden können, liegt nicht nur im Interesse derer, die das Internet als Handelsplattform nutzen und ausbauen wollen. Die Einführung und Verbreitung digitaler Signaturen stellt zudem eine wichtige Voraussetzung für die Modernisierung von Staat und Verwaltung dar, was einem Mindestmaß an Akzeptanz auf allen Seiten Vorschub leistet.

Die Anforderungen, die Vertreter der unterschiedlichen Seiten an den Einsatz von vertraulichkeitsschützender Verschlüsselung stellen, stehen dagegen partiell sogar in diametralem Gegensatz zueinander. Umstritten ist dabei nicht nur die Ausgestaltung der Software, sondern auch die Ausgestaltung der zu ihrer Bereitstellung erforderlichen Infrastruktur.

Verteidiger der Privatheit fordern starke vertraulichkeitsschützende Verschlüsselung und Anonymisierungsdienste in den Händen der Teilnehmer. Sie sehen darin den besten Weg, um Bürger vor der Ausspähung von Inhalten, der Aufzeichnung von Kommunikationsakten, der Nachverfolgung von Bewegungen und der Verkettung der in den genannten Bereichen generierten Informationen zur Anfertigung detaillierter Persönlichkeitsprofile zu bewahren (siehe etwa BfDI, 2020; Hohmann, 2016; Johannes & Rossnagel, 2016, S. 29 ff.; Petersen & Pohlmann, 2014, S. 72 ff.).

Das wohl bekannteste Instrument, das Teilnehmer zum Schutz vertraulicher Inhalte in eigener Regie nutzen können, ist das aus dem zivilgesellschaftlichen Raum stammende Programm Pretty Good Privacy, welches später zu OpenPGP weiterentwickelt wurde (siehe Gerling, 2000, S. 11 ff.; Schwenk, 2010, S. 29 ff.). Ebenfalls frei verfügbar und zudem einfacher zu installieren und zu bedienen ist die sogenannte Volksverschlüsselung, einsetzbar in Windows-basierten E-Mail-Programmen wie Outlook und Thunderbird, zu der man sich mittels der eID-Funktion im elektronischen Personalausweis anmelden kann (siehe Asendorpf, 2020, S. 34; Herfert, Selzer & Waldmann, 2016, S. 290 ff.). Bereitgestellt wird die Volksverschlüsselung vom Fraunhofer Institut für sichere Informationstechnologie.

Protagonisten der öffentlichen Sicherheit warnen dagegen vor der Verbreitung von starker vertraulichkeitsschützender Verschlüsselung (siehe etwa Hostettler, 2017, S. 10 ff.; Neuhaus, 2017, S. 192 f.; Schallbruch, 2018, S. 229 f.; Schulze, 2017, S. 25). In Kombination mit Anonymisierungsdiensten würde diese den Sicherheitsbehörden die Möglichkeit nehmen, sicherheitsrelevante Vorgänge in den elektronischen Netzwerken zu beobachten und sich Zugang zu Inhalten zu verschaffen, die von potentiellen Straftätern und Terroristen übermittelt werden. Dies laufe einer effektiven Kriminalitätsbekämpfung und einem zuverlässigen Schutz kritischer Infrastrukturen gleichermaßen zuwider.

Zur Entschärfung des aus ihrer Sicht bedrohlichen Potentials der vertraulichkeitsschützenden Verschlüsselung haben Sicherheitspolitiker bislang die unterschiedlichsten Maßnahmen empfohlen (siehe Brunst, 2012, S. 333 ff.; Schallbruch, 2018, S. 85 ff.; Schulze, 2017, S. 24). Dazu zählen ein Kryptographieverbot, die exklusive Freigabe schwacher bzw. in der Schlüssellänge beschränkter Kryptographiesoftware, die Hinterlegung von Schlüsseln bei unabhängigen Dritten, welche diese gegebenenfalls zu Strafverfolgungszwecken herausgeben sollen, der Einbau „staatlich mandatierter Schwachstellen“ (Schulze, 2017, S. 25) in die Verschlüsselungssoftware, die Ausnutzung von Sicherheitslücken in den Softwareumgebungen der Schlüsselsysteme und als besonders aggressive Variante die Einschleusung von Schadprogrammen in Softwareumgebungen.

Für letzteres eignet sich etwa die Software Pegasus, die von einem israelischen Unternehmen weltweit vertrieben wird und die unter anderem Handydaten, Kontaktlisten, Bankdaten und den Inhalt von Whatsapp-Nachrichten ausspionieren kann, bevor sie auf dem absendenden Rechner verschlüsselt werden (siehe Biermann, 2020, S. 22; Tanriverdi, 2017, S. 10). Der sogenannte Staatstrojaner – hier handelt es sich um eine Software namens FinFisher, die von einem deutsch-britischen Unternehmen vermarktetet wird – fällt ebenfalls in diese Kategorie (siehe Lobe, 2017, S. 40). Die in jüngster Zeit auf der Ebene der Europäischen Union zu beobachtenden Bemühungen zur Regulierung der vertraulichkeitsschützenden Verschlüsselung zielen dagegen auf eine Hinterlegungslösung ab. Dabei ist anschaulich von einem Generalschlüssel die Rede, den die Betreiber von Messengerdiensten unter bestimmten Bedingungen an Sicherheitsbehörden ausliefern sollen (siehe Beisel & Muth, 2020, S. 9).

Dass Vertreter der Datenwirtschaft in der Verbreitung von Anonymisierungsdiensten ein gravierendes „Geschäftshindernis“ (Reppesgaard, 2012, S. 412) sehen, liegt auf der Hand angesichts der Tatsache, dass diese ihnen die Erstellung von Kommunikationsprofilen und Bewegungsprofilen und deren Verdichtung zu Persönlichkeitsprofilen unmöglich machen können. Gegen den Einsatz starker Verschlüsselung, die staatliche Maßnahmen zur Ausspähung übertragener Inhalte ins Leere laufen lässt, haben sie dagegen keine Einwände. Im Gegenteil: Davon ausgehend, dass ein Mindestmaß an Vertrauen in die Vertraulichkeit übermittelter Inhalte auf Seiten der Teilnehmer eine unverzichtbare Voraussetzung für eine umfassende Erschließung der ökonomischen Potentiale der elektronischen Netzwerke darstellt, und dass die Bereitstellung einer starken vertraulichkeitsschützenden Verschlüsselung vertrauensbildend wirkt, bieten Internetkonzerne ihren Kunden selbst entsprechende Funktionen an. Dies geschieht bei einigen Messengerdiensten wie Signal, Threema und Whatsapp obligatorisch, bei anderen wie Facebook Messenger, Google Allo und Telegram optional (siehe Nezik, 2021, S. 21; Schulze, 2017, S. 23). Der Nachteil von vertraulichkeitsschützender Verschlüsselung, die sich nicht in den Händen der Teilnehmer, sondern der Serviceprovider und Internetfirmen befindet: Die Bürgerinnen und Bürger können den Beteuerungen der Konzerne glauben, dass sie nicht mitlesen, dies aber nicht überprüfen.

6 Darknet, chinesisches Netz und Clearnet

Wenn man der Frage nachgeht, wo sich welche der geschilderten Anforderungen an den Einsatz von elektronischer Kryptographie in der Praxis bislang am stärksten durchgesetzt haben, ergibt sich folgendes Bild: Den Anforderungen des Privatheitsschutzes trägt das Darknet am besten Rechnung, den Anforderungen der öffentlichen Sicherheit die „Big Data Diktatur“ (Assheuer, 2017, S. 47) der chinesischen Staatsführung und den Anforderungen der Datenwirtschaft das sogenannte „Clearnet“ oder „Surface Web“ (Mey, 2017, S. 4), also das klassische Internet der westlichen Welt.

Zugang zum Darknet eröffnet der Tor-Browser, gegebenenfalls auch in Kombination mit starker vertraulichkeitsschützender Verschlüsselung. Mit Hilfe dieses Browsers können sich Teilnehmer nicht nur anonym im überkommenen World Wide Web bewegen, sondern zudem anonym betriebene Websites aufsuchen und solche auch selbst aufbauen (siehe Mey, 2017, S. 4 ff.; Schallbruch, 2018, S. 88 ff.). Dabei gilt dieses Netz einerseits als „digitales Kaufhaus der Kriminellen“ (Vogt, 2017, S. 4) und als

Tummelplatz von Terroristen, anderseits aber auch als „Netz der Dissidenten“ (Moßbrucker 2017, S. 16), in dem sich kritische Journalisten, Menschenrechtler und Politiker, die mit autoritären Regimen in Konflikt geraten sind, noch weitgehend frei und ohne Furcht vor Sanktionen bewegen können.

In China finden sich von nationalen Anbietern wie Baidu, Tencent und Alibaba betriebene Suchmaschinen und Plattformen, die einer direkten staatlichen Kontrolle unterliegen oder zumindest einem massiven Kooperationsdruck ausgesetzt sind (siehe Conrad & Wübbeke, 2018, S. 16 f.; Heuser & Knuth, 2020, S. 17). Die dort über die Gesellschaftsmitglieder anfallenden Daten werden von staatlichen Stellen abgeschöpft und um weitere ergänzt. Hinzu kommen insbesondere Daten, die Arbeitgeber über ihre Mitarbeiterinnen und Mitarbeiter sammeln, und Daten, die im Rahmen einer umfassenden Kameraüberwachung öffentlicher Plätze anfallen. Nicht nur die Nutzung von vertraulichkeitsschützender Verschlüsselung und Anonymisierungsverfahren, auch der alternative Zugriff auf die Dienste ausländischer Internetkonzerne wird in China sanktioniert.

Die chinesische Datenwirtschaft dient als Datenlieferant für ein derzeit im Aufbau befindliches *Social Scoring*, das eine unmittelbar verhaltensregulierende Funktion haben soll (siehe Assheuer, 2017, S. 47; Langer, 2020, S. 305 ff.). Den Bürgern werden Punktekonten zugeordnet. Bei einem hohen Punktestand winken Belohnungen, bei einem niedrigen drohen Sanktionen. Zu den für das Scoring relevanten Verhaltensweisen zählen die Zahlungsmoral im Geschäftsverkehr, das Verhalten an öffentlichen Orten und die Bereitschaft zu sozialer Solidarität. Die Belohnungen und Sanktionen, die ein hoher oder niedriger Punktestand auslösen kann, betreffen Faktoren wie den Zugang zur Bildung, Aufstiegschancen im Beruf, die Bewilligung von Krediten, die Vergabe von Wohnungen und die Möglichkeit, zu reisen.

Das Clearnet ist durch die konsequente Umsetzung datengetriebener Geschäftsmodelle geprägt. In dem Maße, wie sich die Daten über die Lebensweisen und Lebensperspektiven der Gesellschaftsmitglieder in Produktionsfaktoren verwandeln, entwickeln sich diese im Internet der westlichen Welt zu „gläsernen Kunden“ (Dietrich, Jörg, Rammig & Helmchen, 2015). Damit wird die „Überwachungsgesellschaft“ zur „Kehrseite der Informationsgesellschaft“, wenn nicht gar zu ihrer „konsequenten Weiterentwicklung“ (Zurawski, 2014, S. 16).

Während die Aushöhlung der Privatheit in den Vereinigten Staaten lediglich auf einen eher geringen Widerstand stößt (siehe Hoffmann, 2016; Weichert, 2012, S. 419 ff.), sind im europäischen Raum immerhin ernsthafte, wenn auch bislang wenig erfolgreiche Bemühungen zur Eindämmung und Entschärfung dieser Entwicklung zu beobachten (siehe Blume & Nezik, 2020, S. 26; Hamann, 2018, S. 21 f.; Hijmans & Langfeld, 2012, S. 403 ff.). Davon zeugt etwa die Datenschutzgrundverordnung, die darauf abzielt, die Regelungen zur Verarbeitung personenbezogener Daten durch Unternehmen und Behörden europaweit zu vereinheitlichen.

7 Handlungsbedarf und Perspektiven

Nicht nur das Darknet und das chinesische System, auch das Clearnet eignet sich nicht, um als Modell für einen sozialverträglichen Einsatz von elektronischer Kryptographie herangezogen zu werden. Denn alle drei Varianten weisen gravierende Mängel auf, die

daraus resultieren, dass sie speziellen Interessen prominent Rechnung tragen und andere vernachlässigen oder gar verleugnen. Zumindest in modernen Demokratien, die sich den Menschenrechten verpflichtet sehen und gleichzeitig den Bedingungen der kapitalistischen Marktwirtschaft unterworfen sind, ist ein Einsatz von elektronischer Kryptographie erstrebenswert, der den wesentlichen Belangen von Datenschutz, öffentlicher Sicherheit und freier wirtschaftlicher Betätigung gleichermaßen Rechnung trägt.

Dabei ist allerdings anzunehmen, dass die Entwicklung mehrseitig akzeptabler Konzepte ohne institutionelle und kulturelle Innovationen zur Erweiterung der gesellschaftlichen Problembearbeitungskapazitäten kaum gelingen kann. Erwecken doch insbesondere die Auseinandersetzungen zwischen den Verteidigern der Privatheit und den Hütern der öffentlichen Sicherheit bislang weniger den Eindruck einer rational gesteuerten Suche nach praxistauglichen Kompromissen als den eines in eingefahrenen Gleisen verlaufenden Rituals, in dem altbekannte Akteure altbekannte Argumente austauschen.

Was die institutionelle Ebene angeht, deutet sich ein erweiterter Bedarf an Einrichtungen an, die den unterschiedlichen Seiten die Möglichkeit eröffnen, Wahrnehmungen und Interessen effektiver als bisher abzugleichen und konsequenter als zuvor auf mehrseitig akzeptable Lösungen hinzuarbeiten. Um diesem Bedarf Rechnung zu tragen, könnten nicht nur neue Arenen, Foren oder Gremien geschaffen, sondern auch überkommene Einrichtungen reformiert und mit zusätzlichen Funktionen betraut werden. So stellt sich etwa die Frage, ob man wissenschaftlichen Institutionen, deren Rolle sich derzeit noch weitgehend auf die Gewinnung und Verbreitung entscheidungsrelevanten Wissens beschränkt, darüber hinaus die Aufgabe zuweisen sollte, sich am Aufbau geeigneter Verhandlungsnetzwerke zu beteiligen und darin als Moderatoren, Makler und Mediatoren mitzuwirken.

Kulturelle Innovationen, ohne die institutionelle Innovationen ins Leere laufen würden, sollten darauf abzielen, die Vertreter von Datenschutz, öffentlicher Sicherheit und Wirtschaft für übergeordnete Zusammenhänge zu sensibilisieren und sie zu befähigen, neben Trennendem auch Verbindendes erkennen und daran in Aushandlungsprozessen anknüpfen zu können. Dies wird allerdings dadurch erschwert, dass die jeweiligen Akteure zumeist durch ein Bildungssystem geprägt sind, das der Vermittlung von Spezialistenwissen gegenüber der Vermittlung von Generalistenwissen und Sozialkompetenz den Vorzug gibt.

Verbindendes zwischen den Belangen von Privatheit, öffentlicher Sicherheit und freier wirtschaftlicher Betätigung, das unter verbesserten institutionellen und kulturellen Bedingungen Anknüpfungspunkte für eine gemeinsame Suche nach Kompromissen und Kompensationslösungen bieten könnte, existiert in höherem Maße als man es angesichts der verbittert geführten Kontroversen vermuten sollte. So liegt es letztlich auch im Interesse der informationellen Selbstbestimmung, wenn Belange der öffentlichen Sicherheit gewahrt bleiben, und im Interesse der Sicherheitsbehörden, wenn es nicht zum „Ende der Privatheit“ (Whitaker, 1999) kommt, legitimieren sich doch beide Seiten über den Anspruch, Demokratie und Rechtsstaatlichkeit schützen zu wollen und sind doch sowohl Demokratie als auch Rechtsstaatlichkeit ohne garantierte individuelle Freiräume ebenso wenig denkbar wie ohne ein System von Regeln und Sanktionsmechanismen, das dem Missbrauch dieser Räume entgegenwirkt (siehe Fraenkel, 1968, S. 165 ff.). Gelänge es einer Partei, ihren Interessen im Übergang zur digitalen Informationsgesellschaft absolute Geltung zu verschaffen, wäre nicht nur das Projekt der anderen Seite, sondern auch das eigene gescheitert.

Gleichzeitig gibt es aber auch für Vertreter der Datenwirtschaft gute Gründe, sich gegenüber den Einwänden von Datenschützern und Sicherheitspolitikern offener und kooperationsbereiter zu zeigen. Denn der dauerhafte Erfolg ihrer Geschäftsmodelle hängt maßgeblich von deren gesellschaftlicher Akzeptanz ab, die ins Wanken gerät, wenn allgemein ersichtlich wird, dass sie bürgerschaftliche Freiräume in Frage stellen und Staatszielen zuwiderlaufen.

Dies zeigt auch der Skandal um die Firma Cambridge Analytica, die im Vorfeld der 2016 durchgeführten US-Präsidentenwahl Facebook-Daten zu Zwecken des politischen *Microtargeting* missbrauchte. Dieser Skandal hat nicht nur Zweifel an der Rechtmäßigkeit der Wahl aufgeworfen (siehe Brost et al., 2016, S. 3; Nezik, 2020, S. 28; Stark, 2018, S. 27), sondern auch zur Auflösung von Cambridge Analytica geführt und Facebook einen enormen Imageschaden beschert. Inzwischen sind sogar massive Bestrebungen zur Zerschlagung Facebooks zu beobachten, dies allerdings weniger aus demokratiepolitischen als aus marktpolitischen Beweggründen (siehe Blume, 2020, S. 30).

Andererseits liegt aber auch eine Blockade der ökonomischen Innovationen, die im Übergang zur digitalen Informationsgesellschaft möglich werden, nicht im Interesse von Staat und Gesellschaft, da die Aufrechterhaltung von Demokratie, Rechtsstaatlichkeit und individuellen Freiräumen ein Mindestmaß an Prosperität voraussetzt (siehe Lipset, 1962).

Unter verbesserten institutionellen und kulturellen Voraussetzungen könnte man etwa die Einführung einer speziellen Software ansteuern, die darauf zugeschnitten ist, die Belange aller an einer digitalen Transaktion Beteiligten so weit wie möglich auf einen gemeinsamen Nenner zu bringen, oder versuchen, sich auf unterschiedliche Systeme für unterschiedliche Lebensbereiche zu verständigen (siehe etwa Pfitzmann, Schil, Westerfeld & Wolf, 2000; Witt, 2006, S. 63 ff.). Ein anderer Ansatz zielt auf die Schaffung eines „zentralen Datenportals“ zur Gewährleistung „individueller Datensouveränität“ (Joost, 2017, S. 27) ab. Ein solches Portal soll Bürgern als „Schnittstelle zu sämtlichen gespeicherten bzw. personalisierbaren Daten“ (SVRV, 2017, S. 8.) dienen, sie kontinuierlich darüber informieren, wer welche Daten über sie besitzt und nutzt, und ihnen zudem die Möglichkeit geben, Daten und Zugriffsrechte gegebenenfalls zu löschen, zu verändern und sogar zu veräußern. Die Sicherheitsbehörden könnten unter der Voraussetzung einer richterlichen Anordnung Zugriff auf Datenkonten erhalten, deren Besitzer einer Straftat verdächtigt werden.

Die Auseinandersetzung mit den Anforderungen, die unter Aspekten von Privatheit, öffentlicher Sicherheit und freier wirtschaftlicher Betätigung an den Einsatz von elektronischer Kryptographie zu richten sind, und die Suche nach Wegen, diese besser als bisher auf einen gemeinsamen Nenner zu bringen, ist nicht nur wegen der besonderen gesellschaftlichen Bedeutung dieser Frage relevant. Sie erscheint auch beachtenswert, weil auf diesem Feld ein Metaproblem zutage tritt, das sich im Übergang vom Analogen zum Digitalen in vielen anderen Bereichen ebenfalls mit zunehmender Dringlichkeit stellt. So würde eine nähere Betrachtung der Spannungen zwischen Belangen von Open Data und Urheberrechtsschutz[7] oder der Konflikte zwischen den Belangen der demokratischen Willensbildung und des Schutzes von Wirtschaftsgeheimnissen[8] höchstwahrscheinlich nicht nur Hinweise auf vergleichbare Problemstrukturen, sondern auch auf einen vergleichbaren Bedarf an institutionellen und kulturellen Innovationen zur Erweiterung der gesellschaftlichen Problembearbeitungskapazität liefern.

Dass Innovationen zur Verbesserung der Fähigkeit moderner Gesellschaften, auf Herausforderungen wie die Bewältigung der Kryptographiefrage angemessen zu reagieren, grenzüberschreitend angelegte Governancelösungen anstreben oder zumindest den Weg zu ihnen offenhalten sollten, liegt angesichts der Vielschichtigkeit und globalen Qualität der zu bearbeitenden Probleme auf der Hand. Weiterführende Überlegungen könnten bei Ideen und Konzepten aus der Diskussion um Wege zur Bewältigung von Wicked Problems und aus dem Diskurs über die Voraussetzungen, Formen und Chancen von Internet Governance anknüpfen.

Als Wicked Problems gelten besonders komplexe Herausforderungen wie etwa der Klimawandel, die sich herkömmlichen Bearbeitungsstrategien von Politik und Verwaltung entziehen und daher neue Formen der gesellschaftlichen Problembearbeitung erforderlich machen (siehe etwa Fuhr, 2019, S. 191 ff.; Rittel & Webber, 2013, S. 20 ff.; Winkel, 2020, S. 70 ff.). Zur Bewältigung von Wicked Problems, die sich niemals dauerhaft lösen, sondern lediglich temporär entschärfen lassen, werden sowohl Anpassungsmaßnahmen im Rahmen überkommener Strukturen und Prozesse als auch die Neuordnung von Strukturen und Prozessen in Betracht gezogen.

Internet Governance steht für Bestrebungen, sachgerechte und möglichst weitgehend akzeptable Normen, Regeln und Programme zur Nutzung und Weiterentwicklung des Internet zu entwickeln und dabei alle Akteure gleichberechtigt einzubeziehen, die im Hinblick auf ein relevantes Handlungsfeld ein berechtigtes Interesse geltend machen können (siehe etwa Betz & Kübler, 2013; Esch, 2018, S. 35 ff.; Schünemann, 2019, S. 32 ff.). Dabei werden nicht nur technische Fragen wie die Vergabe von Internetadressen und Domainnamen adressiert, sondern auch darüberhinausgehende Themen wie die Gewährleistung von Netzneutralität oder die Förderung eines ethisch fundierten Umgangs mit Künstlicher Intelligenz.

Um hierzulande einen Beitrag zur Förderung eines mehrseitig akzeptablen Einsatzes von elektronischer Kryptographie zu leisten, könnte eine von anderen staatlichen Stellen unabhängige neue Behörde geschaffen werden, die speziell für die Bearbeitung von im Kontext von informationstechnischen Innovationen auftretenden Sicherheitsproblemen zuständig ist. Vorrausetzung wäre die Bereitschaft der politischen Entscheidungsträger, Aufgaben aus dem Bereich des Bundesamts für Sicherheit in der Informationstechnik (BSI) (siehe BSI, 2012, S. 4 f.; Deutscher Bundestag, 2019, S. 4 ff.) herauszulösen und dieser Behörde zu übertragen.[9] Anders als das genannte Bundesamt, das dem Bundesministerium des Innern und für Bauen und Heimat nachgeordnet ist, könnte eine solche Einrichtung gegenüber den Verfechtern divergierender Interessen als unparteiischer Makler auftreten und aus dieser Position heraus der Entwicklung mehrseitig akzeptabler Lösungen weitaus effektiver Vorschub leisten als Institutionen und Akteure, die in der öffentlichen Wahrnehmung einem der konkurrierenden Lager zugeordnet werden.

Von entscheidender Bedeutung für den Erfolg der neuen Behörde wäre eine Personalpolitik, die sicherstellt, dass die dort tätigen Menschen die Bearbeitung solcher Sicherheitsprobleme weniger als ingenieurtechnische denn als sozialtechnische Herausforderung begreifen. Mit Fragen des digitaltechnisch induzierten Wandels vertraute Sozialwissenschaftler müssten dort eine mindestens ebenso wichtige Rolle spielen wie Ingenieure, Informatiker und Juristen.

Dabei spräche vieles dafür, die Aktivitäten der neuen Behörde anfangs primär auf den Abbau der Spannungen im Verhältnis von Privatheit und öffentlicher Sicherheit

auszurichten. Weil eine emotionale Aufheizung der Debatte dazu geführt hat, dass sich die Gewichte in jüngster Zeit deutlich zu Lasten des Datenschutzes verschoben haben, erscheint eine Rationalisierung der Auseinandersetzung hier besonders dringlich. Auslöser dieser Emotionalisierung, welche die Entwicklung mehrseitig akzeptabler Lösungen immer weiter in die Ferne rücken lässt, waren Ereignisse wie die Vorbereitung und Koordination terroristischer Aktionen mittels Social Media und Mobilkommunikation oder die systematische Störung demokratischer Prozesse durch informationstechnisch hochgerüstete ausländische Mächte, die einer offenen Gesellschaft feindlich gegenüberstehen. Hinzu kam die Aufdeckung der schockierenden Ausmaße, die der Austausch von kinderpornographischen Darstellungen und die Anbahnung von Kindesmissbrauch im Internet angenommen haben.

Wenn sich beim Abbau der Spannungen im Verhältnis von Privatheit und öffentlicher Sicherheit erste Erfolge einstellen, könnte man den Aktionsradius der Behörde sukzessive ausweiten und datenwirtschaftliche Belange verstärkt in die Aushandlungsprozesse einbeziehen. Und schließlich könnten die Aktivitäten in diesem Handlungsfeld, die quasi wie ein Nukleus ein immer größeres Problemspektrum adressieren, in ihren Voraussetzungen und Folgen ausgewertet und die so gewonnenen Erkenntnisse für Fortschritte in anderen Bereichen und auf anderen Ebenen produktiv gemacht werden.

8 Schluss

Die Untersuchung der Anforderungen, die Datenschützer, Sicherheitspolitiker und Vertreter der Datenwirtschaft an den Einsatz von elektronischer Kryptographie richten, lässt gravierende Interessenkonflikte deutlich werden, deren Bewältigung institutionelle und kulturelle Innovationen erforderlich macht. Vieles spricht dafür, eine von anderen staatlichen Einrichtungen unabhängige neue Behörde zu schaffen, die speziell für die Bearbeitung der im Kontext von informationstechnischen Innovationen auftretenden Sicherheitsprobleme zuständig ist. Diese könnte gegenüber den Verfechtern divergierender Interessen als unparteiischer Makler auftreten und aus dieser Position heraus der Entwicklung mehrseitig akzeptabler Lösungen Vorschub leisten. Voraussetzung für den Erfolg einer solchen Behörde wäre eine Personalpolitik, die gewährleistet, dass die Mitarbeiter die Bearbeitung der Sicherheitsprobleme weniger als ingenieurtechnische denn als sozialtechnische Herausforderung begreifen. Die Aufarbeitung der Anforderungen an den Einsatz von elektronischer Kryptographie und die Suche nach Möglichkeiten, auf die entsprechenden Konflikte durch die Erweiterung gesellschaftlicher Problemkapazität zu reagieren, sind nicht nur hinsichtlich dieses Politikfelds von Belang, sondern verweisen auf ein digitalisierungsinduziertes Metaproblem, das bislang noch zu wenig Beachtung gefunden hat.

Anmerkungen

1 In der Fachdiskussion werden entsprechende Phänomene häufig unter besonderer Berücksichtigung der Rolle von Populisten, Demagogen und Verschwörungstheoretikern betrachtet, die sich im Internet breitgemacht haben, oder werden mit Aktivitäten technisch hochgerüsteter autoritärer Staaten wie Russland oder China in Verbindung gebracht, welche auf die Manipulation politischer Diskurse in pluralistischen Gesellschaften abzielen. Mit dem digitaltechnischen Wandel einhergehende systemische

Entwicklungen, die solchen Kräften erst die Möglichkeit eröffnen, ihr destruktives und aggressives Potential in bislang nie gekannter Weise zu entfalten, finden dagegen noch keine adäquate Beachtung.

2 Aus Gründen der besseren Lesbarkeit wird im Folgenden ausschließlich die männliche Sprachform verwendet. Selbstverständlich sind alle Geschlechter gleichermaßen gemeint.

3 Anderes gilt allerdings für Algorithmen, die im Rahmen von Deep Learning auf der Basis von künstlichen neuronalen Netzen eingesetzt werden. Hier bestimmt nicht lineare Programmierung, sondern die Auswertung von Trainingsdaten die Ausgestaltung von Lösungswegen, wobei sich die Rolle der Programmierer darauf beschränkt, die Kriterien für die Auswertung in groben Zügen vorzugeben.

4 In der Praxis werden beide Verfahren häufig kombiniert genutzt, um die funktionalen Vorteile der asymmetrischen Verschlüsselung mit den Kostenvorteilen der symmetrischen Verschlüsselung zu verbinden.

5 Dazu lässt sich etwa der Umstand nutzbar machen, dass sich eine vielstellige Zahl aus zwei großen Primfaktoren zusammensetzen kann. Basiert der öffentliche Schlüssel auf dieser Zahl, enthält der zugehörige private Schlüssel die Primfaktoren.

6 Allerdings wird im konkreten Anwendungsfall nicht die Nachricht selbst verschlüsselt, sondern eine nach einem bestimmten Verfahren berechnete Kurzfassung. Die Kurzfassung bildet zusammen mit anderen Informationen wie die Absenderkennung die elektronische Signatur.

7 Die Spannungen zwischen Belangen von Open Data und Urheberrechtsschutz erwachsen daraus, dass wirtschaftliche Innovationen durch einen möglichst freien Zugang zu Informationen begünstigt werden, weil Neues zumeist aus der Kombination von Bekanntem entsteht, während sie gleichzeitig aber auch an wirtschaftliche Anreize gebunden sind, die umso geringer ausfallen, desto weniger Unternehmen und Investoren von den Innovationserträgen exklusiv profitieren können.

8 Die Konflikte zwischen Belangen von Demokratie und dem Schutz von Wirtschaftsgeheimnissen sind dem Umstand geschuldet, dass demokratische Willensbildung die Transparenz von Machstrukturen und Machtprozessen voraussetzt, während ein Schutz von Wirtschaftsgeheimnissen, der sich auch auf massiv in die Gestaltung von Lebenswelten eingreifende Software bezieht, dem Transparenzgebot zuwiderläuft. In dem Maße, wie die Regulierung sozialer Beziehungen durch proprietäre Software im Übergang zur digitalen Informationsgesellschaft voranschreitet, nimmt die Gefahr zu, dass demokratische Politik an Steuerungsfähigkeit und Durchschlagskraft verliert.

9 Das dem Bundesamt für Sicherheit in der Informationstechnik zugeordnete Aufgabenspektrum umfasst die Bereiche Schutz der elektronischen Netzwerke des Bundes, Prüfung, Zertifizierung und Akkreditierung digitaltechnischer Produkte und Dienstleistungen sowie öffentliche Aufklärung in Fragen von Informationstechniksicherheit einschließlich der Warnung vor Schadprogrammen und Sicherheitslücken.

Literatur

Akzan, Can, Iggena, Lennart, Korte, Tobias & Spiekermann, Markus (2019). *Datenwirtschaft in Deutschland*. Dortmund: Verlag des ISST.

Asendorpf, Dirk (2020). Sichere E-Mails für alle. *Die Zeit*, Nr. 26 vom 16.06., 34.

Assheuer, Thomas (2017). Die Big Data Diktatur. *Die Zeit*, Nr. 49 vom 30.11., 47.

Becker, Carlos & Seubert, Sandra (2019). Die Stärkung europäischer Grundrechte im digitalen Zeitalter. Demokratiepolitische Potentiale am Beispiel des Privatheitsschutzes. In Jeanette Hofmann, Norbert Kersting, Claudia Ritzi & Wolf Schünemann (Hrsg.), *Politik in der digitalen Gesellschaft* (S. 225-245). Bielefeld: Transcript.

Beisel, Karoline & Muth, Max (2020). EU-Staaten wollen bei Whatsapp und Signal mitlesen. *Süddeutsche Zeitung*, Nr. 69 vom 09.11., 9.

Betz, Joachim & Kübler, Hans-Dieter (2013). *Internet Governance. Wer regiert wie das Internet*? Wiesbaden: Springer.

Beutelspacher, Albrecht (2015). *Kryptologie*. Wiesbaden: Springer.

Beutelspacher, Albrecht (2017). Eine kurze Geschichte der Kryptographie. *Aus Politik und Zeitgeschichte, 46-47*, 35-40.

Biermann, Kai (2020). Die Absauger. *Die Zeit*, Nr. 27 vom 25.06., 22.

Blume, Georg (2020). Das schmeckt nach mehr. *Die Zeit*, Nr. 53 vom 17.12., 30.

Blume, Georg & Nezik, Ann-Kathrin (2020). Google, Amazon, Facebook und Apple beherrschen das Internet. Kann ein EU-Beamter sie zähmen? *Die Zeit*, Nr. 50 vom 03.12., 26.

Bridle, James (2020). *New Dark Age. Der Sieg der Technologie und das Ende der Zukunft*. Bonn: Verlag der Bundeszentrale für politische Bildung.

Brost, Marc et al. (2016). Finstere Attacken. *Die Zeit*, Nr. 52 vom 15.12., 3.

Brunst, Phillip (2012). Staatliche (Anti)Kryptostrategien. *Datenschutz und Datensicherheit*, 5, 333-228.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2012). *Leitfaden Informationssicherheit*. Bonn: Verlag des BSI.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2015). *Die Lage der IT-Sicherheit in Deutschland*. Bonn: Verlag des BSI.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2016). *De-Mail. Sicherer elektronischer Nachrichtenverkehr – einfach, nachweisbar und vertraulich*. Bonn: Verlag des BSI.

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) (2020). *Stellungsnahme des BfDI zur öffentlichen Anhörung des Innenausschusses zum Thema Recht auf Verschlüsselung*. Bonn: Verlag des BfDI.

Bundesministerium des Innern (BMI) (2009). *Nationale Strategie zum Schutz kritischer Infrastrukturen*. Berlin: Verlag des BMI.

Bundesministerium des Innern (BMI) (2016). *De-Mail-Leitfaden für Behörden*. Berlin: Verlag des BMI.

Conrad, Björn & Wübbeke, Jost (2018). *Wird China zur Hightechsupermacht?* Bad Homburg: Verlag des FERI Cognitive Finance Institute.

Deutscher Bundestag (2019). *Zu den Aufgaben des Bundesamts für Sicherheit in der Informationstechnik*. Sachstandsbericht der wissenschaftlichen Dienste. Berlin: Verlag des Deutschen Bundestags.

Dietrich, Matthias, Jörg, Andreas, Rammig, Frank & Helmchen, Moritz (2015). *Web Tracking – der gläserne Kunde*. Kempten: Verlag der Hochschule Kempten.

Eichhorn, Peter (2002). *Verwaltungslexikon*. Baden-Baden: Nomos.

Esch, Johanna (2018). Internationale Internet Governance. *Aus Politik und Zeitgeschichte, 40-41*, 35-40.

Etscheid, Jan (2018). Automatisierungspotentiale in der Verwaltung. In Resa Mohabbat-Kar, Basanta Thapa & Peter Parycek (Hrsg.), *(Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft* (S. 126-158). Berlin: Verlag des Kompetenzzentrums Öffentliche IT.

Federrath, Hannes & Pfitzmann, Andreas (2006). IT-Sicherheit. In Martin Wind & Detlef Kröger (Hrsg.), *Handbuch IT in der Verwaltung* (S. 273-292), Heidelberg: Springer.

Fraenkel, Ernst (1968). Der Pluralismus als Strukturelement der freiheitlich-rechtsstaatlichen Demokratie. In Ernst Fraenkel (Hrsg.), *Deutschland und die westlichen Demokratien* (S. 165-189). Stuttgart: Kohlhammer.

Fraunhofer Institut für Software und Systemtechnik (ISST) (2019). *Datenwirtschaft in Deutschland*. Dortmund: Verlag des ISST.

Fuhr, Harald (2019). Verwaltung und Wicked Problems. In Sylvia Veit, Sylvia, Christoph Reichard & Göttrik Wewer (Hrsg.), *Handbuch zur Verwaltungsreform* (S. 191-200). Wiesbaden: Springer.

Gerling, Rainer (2000). Pretty Good Privacy. *IT-Sicherheit*, 1, 11-16.

Glaeßner, Gert-Joachim (2016). *Freiheit und Sicherheit*. Bonn: Verlag der Bundeszentrale für politische Bildung.

Goecke, Henry, Lichtblau, Karl, Schleiermacher, Thomas & Schützdeller, Peter (2018). *Digitalisierung der KMU in Deutschland*. Köln: Verlag der IW Consult.

Hamann, Götz (2018). Gib mir meine Daten zurück. *Die Zeit*, Nr. 21 vom 17.05., 21-22.

Herfert, Michael, Selzer, Annika & Waldmann, Ulrich (2016). Laientaugliche Schlüsselgenerierung für Ende-zu-Ende-Verschlüsselung. *Datenschutz und Datensicherheit, 5*, 290-294.

Heuser, Uwe & Knuth, Hannah (2020). Die letzten Tage der Unschuld. *Die Zeit*, Nr. 33 vom 06.08., 17.

Hijmans, Hielke & Langfeld, Owe (2012). Datenschutz in der Europäischen Union. In Jan-Hinrik Schmidt & Thilo Weichert (Hrsg.), *Datenschutz. Grundlagen, Entwicklungen und Kontroversen* (S. 403-411). Bonn: Verlag der Bundeszentrale für politische Bildung.

Hirsch-Kreinsen, Hartmut (2016). Zum Verhältnis von Arbeit und Technik bei Industrie 4.0. *Aus Politik und Zeitgeschichte, 18-19*, 10-17.

Hoffmann, Anja (2016). *Privacy Shield – kein ausreichender Datenschutz im unsicheren Hafen USA*. Freiburg: Verlag des Centrums für Europäische Politik.

Hoffmann, Marina & Schröder, Christian (2019). Datenbasierte Geschäftsmodelle – Chancen und Herausforderungen für KMU. *Wirtschaftspolitische Blätter, 3*, 277-287.

Hohmann, Mirko (2016). *Verschlüsselung als Grundvoraussetzung für die Digitalisierung unserer Gesellschaft.* Berlin: Verlag des Zentrums für digitalen Fortschritt.

Hostettler, Otto (2017). Hilflose Ermittler. *Aus Politik und Zeitgeschichte, 46-47*, 10-15.

Johannes, Paul & Rossnagel, Alexander (2016). *Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der digitalen Welt*. Kassel: Kassel University Press.

Joost, Gesche (2017). Kontrolle über meine Daten. *Die Zeit*, Nr. 27 vom 29.06., 27.

Katzenbach, Christian (2018). Die Ordnung der Algorithmen. In Reda Mohabbat-Kar, Basanta Thapa & Peter Parycek (Hrsg.), *(Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft* (S. 315-338). Berlin: Verlag des Kompetenzzentrums Öffentliche IT.

Krause, Christian (2003). Tools für Anonymität. In Helmut Bäumler & Albert von Mutius (Hrsg.), *Anonymität im Internet* (S. 158-171), Wiesbaden: Springer.

Küsters, Ralf & Wilke, Thomas (2011). *Moderne Kryptographie*. Wiesbaden: Springer.

Kutscha, Martin (2010). Mehr Datenschutz – aber wie? *Zeitschrift für Rechtspolitik, 4*, 112-114.

Langer, Paul (2020). Digitale Profile, Reputation Scoring und Social Credits am Beispiel von Chinas National Credit Management System. In Michael Oswald & Isabelle Borucki (Hrsg.), *Demokratietheorie im Zeitalter der Frühdigitalisierung* (S. 305-322), Wiesbaden: Springer.

Lehner, Nikolaus (2018). Etappen algorithmischer Gouvernementalität. In Lorina Buhr, Stefanie Hammer & Hagen Schölzel (Hrsg.), *Staat, Internet und digitale Gouvernementalität* (S. 17-42). Wiesbaden: Springer.

Lessig, Lawrence (2001). *Code und andere Gesetze des Cyberspace*. Berlin: Berlin Verlag.

Lewinski, Kai von (2012). Zur Geschichte von Privatheit und Datenschutz. In Jan-Hinrik Schmidt & Thilo Weichert (Hrsg.), *Datenschutz. Grundlagen, Entwicklungen und Kontroversen* (S. 23-33). Bonn: Verlag der Bundeszentrale für politische Bildung.

Lipset, Seymour (1962). *Soziologie der Demokratie*. Neuwied: Luchterhand.

Lobe, Adrian (2017). Die Gesellschaft wird zum Computer. *Die Zeit*, Nr. 30 vom 12.07., 40.

Loshin, Peter (2015). *Anonym im Internet mit Tor und Tails*. München: Franzis.

Mattelart, Aramand (2003). *Kleine Geschichte der Informationsgesellschaft*. Berlin: Avinus.

Mau, Steffen (2018). *Das metrische Wir. Über die Quantifizierung des Sozialen*. Bonn: Verlag der Bundeszentrale für politische Bildung.

Mey, Stefan (2017). Tor in eine andere Welt. *Aus Politik und Zeitgeschichte, 46-47*, 4-9.

Moßbrucker, Daniel (2017). Netz der Dissidenten. *Aus Politik und Zeitgeschichte, 46-47*, 16-22.

Neuhaus, Heike (2017). Strafverfolger brauchen Zugriff auf verschlüsselte Kommunikation. *Deutsche Richterzeitung, 6*, 192-193.

Nezik, Ann-Kathrin (2020). Halbe Heldin. Brittany Kaiser arbeitete für die fragwürdige Firma Cambridge Analytica. *Die Zeit*, Nr. 5 vom 23.01., 28.

Nezik, Ann-Kathrin (2021). Die Verschlüsselungskünstler. *Die Zeit*, Nr. 5 vom 28.01., 21.

Petersen, Dominique & Pohlmann, Norbert (2014). *Selbstverteidigung. Verschlüsselung als Mittel gegen die Überwachung.* Hannover: Heise.

Pfitzmann, Andreas, Schill, Alexander, Westerfeld, Andreas & Wolf, Gritta (2000). *Mehrseitige Sicherheit in offenen Netzen*. Wiesbaden: Springer.

Pomberger, Gustav & Dobler, Heinz (2008). *Algorithmen und Datenstrukturen*. München: Pearson.

Reppesgaard, Lars (2012). Global Players. Die großen Internetunternehmen betrachten den Datenschutz eher als Geschäftshindernis. In Jan-Hinrik Schmidt & Thilo Weichert (Hrsg.), *Datenschutz. Grundlagen, Entwicklungen und Kontroversen* (S. 412-418). Bonn: Verlag der Bundeszentrale für politische Bildung.

Rieckmann, Johannes & Kraus Martina (2015). Tatort Internet. *DIW Wochenbericht, 12*, 295-301.

Rittel, Horst & Webber, Melvin (2013). Dilemmas in einer allgemeinen Theorie der Planung. In Wolf Reuter & Wolfgang Jonas (Hrsg.), *Thinking Design* (S. 20-38). Basel: Birkhäuser.

Sachverständigenrat für Verbraucherfragen (SVRV) (2017). *Digitale Souveränität*. Gutachten des SVRV. Berlin: Verlag des SVRV.

Schallbruch, Martin (2018). *Schwacher Staat im Netz*. Wiesbaden: Springer.

Schmeh, Klaus (2009). *Kryptografie – Verfahren, Protokolle, Infrastrukturen*. Heidelberg: D-Punkt.
Schünemann, Wolf (2019). E-Government und Netzpolitik – eine konzeptionelle Einführung. In Wolf Schünemann & Marianne Kneuer (Hrsg.), *E-Government und Netzpolitik im europäischen Vergleich* (S. 17-49). Baden-Baden: Nomos.
Schulze, Matthias (2017). Going dark. Dilemma zwischen sicherer privater Kommunikation und den Sicherheitsinteressen von Staaten. *Aus Politik und Zeitgeschichte, 46-47*, 23-28.
Schulze, Tillmann (2006). *Bedingt abwehrbereit. Schutz kritischer Informationsinfrastrukturen in Deutschland und den USA*. Wiesbaden: Springer.
Schwenk, Jörg (2010). *Sicherheit und Kryptographie im Internet*. Wiesbaden: Springer.
Singh, Simon (2017). *Geheime Botschaften*. München: Hanser.
Spitz, Stephan, Pramateftakis, Michael & Swoboda, Joachim (2011). *Kryptographie und IT-Sicherheit*. Wiesbaden: Vieweg.
Stark, Holger (2018). Achtung Missbrauch. *Die Zeit*, Nr. 26 vom 21.06., 27.
Tanriverdi, Hakan (2017). Pegasus – großer Angriff auf das iPhone. *Süddeutsche Zeitung*, Nr. 10 vom 13.01., 10.
Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) (2018). *Digitalisierung. Eine interdisziplinäre Betrachtung*. Frankfurt am Main: Verlag des VDE.
Vogt, Sabine (2017). Das Darknet – Rauschgift, Waffen, Falschgeld, Ausweise. Das digitale Kaufhaus der Kriminellen? *Die Kriminalpolizei, 2*, 4-7.
Walter, Gregor (2008). *Internetkriminalität. Eine Schattenseite der Globalisierung*. Berlin: Verlag der Stiftung Wissenschaft und Politik.
Weichert, Thilo (2012). Datenschutz und Überwachung in ausgewählten Staaten. In Jan-Hinrik Schmidt & Thilo Weichert (Hrsg.), *Datenschutz. Grundlagen, Entwicklungen und Kontroversen* (S. 419-425). Bonn: Verlag der Bundeszentrale für politische Bildung.
Wernert, Manfred (2017). *Internetkriminalität*. Stuttgart: Boorberg.
Whitaker, Reg (1999). *Das Ende der Privatheit. Überwachung, Macht und soziale Kontrolle im Informationszeitalter*. München: Kunstmann.
Winkel, Olaf (2004). Zukunftsperspektive Electronic Government. *Aus Politik und Zeitgeschichte, 18*, 7-15.
Winkel, Olaf (2018). Entwicklungslinien, Handlungsfelder und widerstreitende Handlungsimperative der Digitalisierung in Staat und Verwaltung. *Verwaltung und Management, 3*, 115-130.
Winkel, Olaf (2020). Wicked Problems und Digitalisierung als Herausforderung für politisch-administratives Handeln. *Verwaltung und Management, 2*, 70-77.
Witt, Bernhard (2006). *IT-Sicherheit kompakt und verständlich*. Wiesbaden: Vieweg.
Zurawski, Nils (2014). Geheimdienste und Konsum der Überwachung. *Aus Politik und Zeitgeschichte, 18-19*, 14-19.

Anschrift des Autors:

Prof. Dr. habil. Olaf Winkel, Hochschule für Wirtschaft und Recht Berlin, Campus Lichtenberg, Fachbereich 3: Allgemeine Verwaltung, Alt-Friedrichsfelde 60, 10315 Berlin, E-Mail: olaf.winkel@hwr-berlin.de.