Vertrauen in digitale Kommunikation: Eine Bestandsaufnahme

von Henning Lahmann und Dr. Till Kreutzer, iRights.Lab

Diskussionspapier im Projekt „Braucht Deutschland einen Digitalen Kodex?“

Juni 2017

Inhaltsverzeichnis

1 Einleitung

Das Teilprojekt „Vertrauen in Kommunikation im digitalen Zeitalter“ im Rahmen des Projekts „Braucht Deutschland einen Digitalen Kodex?“, das das iRights.Lab im Auftrag des DIVSI durchführt, geht von der Grundannahme aus, dass ein Bedürfnis nach geschützter und damit vertrauenswürdiger Kommunikation in bestimmten sensiblen Kommunikationsverhältnissen besteht. Darauf aufbauend wird im Rahmen des Projekts der Frage nachgegangen, wie diese Kommunikationsverhältnisse ausgestaltet sein könnten, damit das Bedürfnis nachhaltig befriedigt wird. Das vorliegende erste Papier zum Thema dient der Bestandsaufnahme und untersucht, wie es gegenwärtig um das Vertrauen in der digitalen Kommunikation bestellt ist. Im Anschluss an diese Problemanalyse wird sich das zweite Themenpapier mit Lösungsmöglichkeiten beschäftigen, die sich auf die technische, auf die rechtliche wie auch auf die organisatorische Ausgestaltung beziehen.

Noch bis vor zweieinhalb Jahrzehnten waren vergleichsweise wenige verschiedene Kommunikationsmittel vorhanden, um mit anderen individuell in Kontakt zu treten – Brief, Telegramm, Telefon, Telefax. Seitdem jedoch hatten die Ausbreitung des Internets und die Entwicklung der anfangs relativ schlichten Mobiltelefone zu internetfähigen Smartphones, bei denen das Telefonieren zu lediglich einer Funktion von vielen geworden ist, geradezu eine Revolution der Kommunikation zur Folge.

Für die meisten ist digitale Kommunikation inzwischen eine Selbstverständlichkeit. Zugleich verliert der klassische, „analoge“ Brief zunehmend an Bedeutung. Nicht nur mit Freunden und Familie, sondern auch mit Unternehmen und staatlichen Einrichtungen findet die Kontaktaufnahme immer häufiger mit digitalen Kommunikationsmitteln statt. Doch obwohl deren Vorteile auf der Hand liegen – sind sie doch schnell, bequem und kostengünstig – so haben die vergangenen Jahre ebenso viele Schattenseiten zutage gefördert: Computerkriminalität wie auch Überwachungs- und Datenschutzskandale haben gezeigt, dass digital gespeicherte und versendete Informationen angreifbar sind.

Wie später noch im Detail erörtert werden wird, haben die bekannt gewordenen Vorfälle das Vertrauen in die digitale Kommunikation beeinträchtigt. Als Konsequenz äußern inzwischen nicht wenige Bürgerinnen und Bürger Vorbehalte, wenn es darum geht, wichtige Informationen auf digitalem Wege zu übermitteln, sei es an Unternehmen oder Behörden.[1] Damit im Einklang gibt es, wie ebenfalls gezeigt werden wird, ein Bedürfnis danach, dass Kommunikation geschützt und damit vertrauenswürdig bleibt.

Die vorliegende Bestandsaufnahme stellt auf der Grundlage entsprechender Befragungen zum Thema beachtliches Misstrauen, das in weiten Teilen der Bevölkerung vorherrscht, fest. Aus pragmatischer Sicht hat Vertrauen in der modernen und sich schnell wandelnden Welt jedoch eine sehr wesentliche Funktion: Vertrauen führt zu Komplexitätsreduktion und in der Folge zur Herstellung oder Sicherstellung von Handlungsfähigkeit.

[1] Vgl. z.B. DIVSI, „Elektronische Dokumentenzustellung“, repräsentative dimap-Umfrage ab 18 Jahren, 1. und 2. März 2017, https://www.divsi.de/wp-content/uploads/2017/03/2017-03-08_Unterlage_DIVSI-dimap-Umfrage_Dokumentenzustellung.pdf.

Nach einer kurzen Übersicht über die Modalitäten von Kommunikation im digitalen Zeitalter wird diese Funktion von Vertrauen im Detail analysiert und seine Bedeutung für Kommunikation erörtert. Die Beschreibung technischer, rechtlicher und organisatorischer Maßnahmen zur Absicherung von Vertrauen bei der Kommunikation führt zu der anschließenden Frage nach möglichen Ursachen für fehlendes Vertrauen und den daraus resultierenden Folgen.

2 Modalitäten der Kommunikation im digitalen Zeitalter

Bis zur Entwicklung der Telegrafie im 19. Jahrhundert beschränkte sich Distanz-Kommunikation im Wesentlichen – von sehr beschränkten Ausnahmen wie Rauch- oder Lichtzeichen oder dem mündlichen Überbringen von Nachrichten durch Boten abgesehen – auf das Versenden von Briefen. Der Telegraf und wenig später das Telefon machten erstmals den („fernmündlichen“) Informationsaustausch in Echtzeit über längere Strecken möglich. Die Erfindung von Telex und Telefax, im Grunde Weiterentwicklungen der Telegrafie, änderten an diesem technologischen Stand bis weit ins 20. Jahrhundert nur wenig.

Erst als sich das in den sechziger Jahren geschaffene Internet zunehmend ausbreitete und spätestens im letzten Jahrzehnt des 20. Jahrhunderts zur selbstverständlich verfügbaren Alltagstechnologie geworden war, änderte sich das Kommunikationsverhalten grundlegend. Nun war es möglich, sich schnell und unkompliziert, und vor allem ohne relevante Kosten, jederzeit schriftlich auszutauschen. Schnell wurde die E-Mail zum allgegenwärtigen Kommunikationsmittel, sei es für private Zwecke oder für den Austausch zwischen Unternehmen und ihren Kunden sowie Behörden und Bürgern. Die Möglichkeit, ab ungefähr Mitte des ersten Jahrzehnts des 21. Jahrhunderts auch per Mobiltelefon zu meist bezahlbaren Tarifen auf das Internet zugreifen zu können, hatte noch einmal ein starkes Wachstum des Kommunikationsaufkommens zur Folge. Recht schnell wurde es zum erwarteten Normalzustand, überall und jederzeit erreichbar zu sein und kommunizieren zu können. Während die Zahl erfolgter Telefongespräche zurückging[2], nahm die schriftliche Kommunikation immer weiter zu.

Digitale Kommunikation gibt es in vielen Ausprägungen, z.B. abhängig von den Kommunikationspartnern („wer mit wem“?), dem Zeitverhalten (synchron oder asynchron) oder bestimmten technischen Details (z.B. Ende-zu-Ende oder vermittelt über eine Plattform). Die einfachste Differenzierung dürfte diejenige nach Absender und Adressat sein, auf die im Folgenden zunächst eingegangen wird.

2.1 Kommunikation zwischen Personen

Heute kann mit jedem durchschnittlichen Smartphone eine Vielzahl von Apps – also Anwendungsprogrammen für mobile Betriebssysteme – verwendet werden, die es insbesondere ermöglichen, mit anderen in Kontakt zu treten. Neben der E-Mail-Funktion sowie

[2] Vgl. https://de.statista.com/statistik/daten/studie/155005/umfrage/volumina-der-in--und-auslandsverbindungen-seit-2005/.

Programmen, die ausschließlich der Kommunikation dienen, wie beispielsweise SMS, iMessage auf Apples iPhone, WhatsApp, Threema, Signal, SIMSme oder Telegram, gibt es eine geradezu unüberschaubare Fülle an Anwendungen, bei denen die Möglichkeit der persönlichen und direkten Kontaktaufnahme mit anderen Nutzerinnen und Nutzern lediglich eine sekundäre Funktion darstellt – so zum Beispiel bei Sozialen Netzwerken wie Twitter, Facebook, LinkedIn oder Instagram. Nicht selten kommt es deshalb vor, dass man sich mit derselben Person wie selbstverständlich auf verschiedenen dieser Kanäle unterhält.

2.2 Kommunikation mit Unternehmen

Auch die Kommunikation zwischen Unternehmen und ihren Konsumenten („business-to-customer“, B2C) wird mehr und mehr auf digitale Kommunikationsmittel verlagert. So würde es heute kaum eine Firma mehr wagen, keine E-Mail-Adresse zum Zweck der Kontaktaufnahme anzugeben. Mehr noch: Nach dem Telemediengesetz ist eine solche Kontaktmöglichkeit sogar rechtlich vorgeschrieben, wenn das Unternehmen eine Webseite unterhält – was heute auf so gut wie jede Firma zutrifft. Immer häufiger ist es zudem möglich, den Kundenservice nicht nur klassisch per Telefon zu erreichen, sondern auf der Webseite des Unternehmens in Echtzeit mit Mitarbeitern zu chatten. Geht es um die Bereitstellung von Informationen, die sensiblere Daten der Kundinnen und Kunden betreffen – wie zum Beispiel Kontoauszüge oder Krankenkassenunterlagen – sind Portallösungen weit verbreitet. Hierbei wird der Kunde zumeist per E-Mail lediglich darüber informiert, dass Informationen für ihn vorliegen. Die eigentlichen Informationen werden in einem individuellen Bereich auf dem Server des Anbieters bereitgestellt. Auf dieses kann der Kunde über einen Login auf seinen Account, seinen persönlichen Zugang, zugreifen, für den er sich zunächst mit einem Benutzernamen oder einer Kundennummer und einem Passwort anmelden muss. Diese einfachste Form der Authentifizierung wurde von einigen Anbietern inzwischen vor dem Hintergrund von Phishing-Angriffen durch die sichereren sogenannten Zwei-Faktor-Verfahren ersetzt.[3]

2.3 Kommunikation mit Behörden

Neben Unternehmen der Privatwirtschaft versuchen inzwischen ebenfalls immer mehr Behörden und andere staatliche Stellen, digitale Kommunikationskanäle mit den Bürgerinnen und Bürgern zu etablieren („government-to-citizen“, G2C). Dass man heute per E-Mail mit der jeweils zuständigen Behörde in Kontakt treten kann, um bestimmte Informationen zu erlangen, versteht sich dabei fast von selbst. Auch Termine mit zum Beispiel Bürgerämtern oder KFZ-Zulassungsstellen können im Normalfall über die entsprechenden Webseiten vereinbart werden. Sogar Verwaltungsentscheidungen mit unmittelbarer rechtlicher Wirkung wie beispielsweise Baugenehmigungen werden mitunter auf elektronischem We-

[3] Phishing: Versuch, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Nutzers zu gelangen und damit Identitätsdiebstahl zu begehen (Quelle: https://de.wikipedia.org/wiki/Phishing).

ge zugestellt.[4] Soweit dies nicht mittels speziell abgesicherter E-Mail-Varianten geschieht (zum Beispiel per PGP-verschlüsselten Mails), besteht auch hier seit Kurzem die Möglichkeit, Online-Postfächer, also Portallösungen, einzusetzen.[5]

2.4 Kommunikationsformen

Das Projekt „Vertrauen in Kommunikation im digitalen Zeitalter" konzentriert sich in erster Linie auf die Kommunikation B2C sowie G2C. Soweit dabei von „digitaler Kommunikation" gesprochen wird, liegt der Fokus auf verschiedenen Varianten der E-Mail sowie auf den genannten Portallösungen. Auch hybride Formen, die sich zugleich analoger und digitaler Techniken bedienen – wie beispielsweise der E-Postbrief der Deutschen Post, Neopost oder Pixelletter – fallen unter diese weiter gefasste Definition digitaler Kommunikation. Weitere digitale Kommunikationsformen wie Messenger-Dienste werden nur genannt, soweit dies für das Verständnis einzelner Punkte notwendig erscheint. Die digitalen Kommunikationsmittel werden insbesondere dem Brief als derjenigen analogen Form der Kommunikation gegenübergestellt, die auch im digitalen Zeitalter insofern weiterhin bedeutsam ist, als viele Behörden noch vorwiegend wie auch zahlreiche Unternehmen auf diese Weise kommunizieren.

2.5 Auswirkungen

Als Folge des Umstands, dass wir heute zunehmend auf digitalem Wege miteinander sowie mit Behörden und Unternehmen kommunizieren, sind mehr und mehr Informationen und persönliche Daten über jede Person im Datenstrom des Internets unterwegs oder auf Servern im Netz gespeichert.[6] Denn bei der digitalen Kommunikation sind neben den eigentlichen Kommunikationsteilnehmerinnen und -teilnehmern zumeist auch Dritte involviert. Diese – insbesondere Kommunikationsdienstleister wie zum Beispiel E-Mail-Provider – transportieren die Kommunikation nicht nur auf digitalem Wege, sondern speichern diese auch auf ihren Servern, zumindest vorübergehend. Dadurch steigt die Gefahr von Missbrauch. Das über das herkömmliche Telefon geführte Gespräch ist flüchtig – jedenfalls solange es niemand mitschneidet, was eine seltene Ausnahme und nicht die Regel ist. Elektronisch übermittelte Daten müssen jedoch gespeichert werden, bevor sie von den Kommunikationsteilnehmerinnen und -teilnehmern abgerufen werden können. Die dadurch entstehenden Kopien der Daten können in einer Weise automatisiert gescannt und analysiert werden, die bei rein analoger Übermittlung von Informationen so nicht oder nur mit

[4] Siehe zum Beispiel für Berlin das Webportal https://www.berlin.de/ebg/, über das das gesamte Baugenehmigungsverfahren elektronisch abgewickelt werden kann.
[5] Rechtliche Grundlage hierfür ist der zum 1. Januar 2017 in Kraft getretene § 41 Abs. 2a des Verwaltungsverfahrensgesetzes, der die Bekanntgabe von Verwaltungsakten über „öffentlich zugängliche Netze" regelt. Die Abwicklung des Verwaltungsverfahrens in dieser Form ist von der vorherigen Einwilligung des Bürgers abhängig. Vgl. dazu im Detail Alexander Schmid und Claudia Heudecker, Der vollständig automatisierte Erlass eines Verwaltungsakts (§ 35a VwVfG) sowie die Bekanntgabe eines Verwaltungsakts über öffentlich zugängliche Netze (§ 41 Abs. 2a VwVfG) (Teil 2), jurisPR-ITR 8/2017, http://bit.ly/2qaOKqG.
[6] Andrea Voßhoff, Vertrauen und Kommunikation in einer digitalisierten Welt aus Sicht der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Vortrag, 17. November 2014, https://www.bfdi.bund.de/DE/Infothek/Reden_Interviews/2014/VertrauenundKommunikation_Muenster171114.html?nn=5217192.

hohem Aufwand möglich ist – Briefe beispielsweise kamen und kommen im Normalfall ungeöffnet und damit ungelesen beim Empfänger an. Zudem gilt, dass jedenfalls für technische Laien oft überhaupt nicht nachzuvollziehen ist, wo diese Speicherung erfolgt – ob im Inland oder Ausland; ob auf Servern des Unternehmens, mit dem in Kontakt getreten wird, oder auf denen eines ansonsten unbeteiligten Dritten. Wer außer dem Versender und dem Adressaten der E-Mail theoretisch noch Zugriff auf ihren Inhalt hat, bleibt für Anwender, die nicht über spezielle EDV-Kenntnisse verfügen, für gewöhnlich im Dunkeln.

Die zunehmende Hinwendung zur Portallösung, die bei immer mehr Unternehmen wie insbesondere Stromanbietern oder Banken zu beobachten und dank der genannten Gesetzesänderung künftig auch bei der Kommunikation mit Behörden zu erwarten ist, bringt zudem einen grundsätzlicheren Wandel des Kommunikationsverhaltens mit sich. Bedeuteten die Nutzung sowohl von analogen Briefen als auch von E-Mails, dass die Unternehmen oder Behörden die Informationen den Kunden bzw. Bürgern überbrachten, wird von diesen bei der Portallösung erwartet, dass sie die Informationen selbst aktiv abrufen. Man könnte sagen, dass sich die Kommunikation zwischen den Akteuren so von einer Bring- zu einer Holschuld wandelt. Der Nutzer ist damit nicht nur in der Verantwortung, sich selbst darum zu kümmern, dass die Informationen zu ihm gelangen;[7] er hat, jedenfalls teilweise, zudem dafür zu sorgen, dass die Informationsübertragung beim Abruf sicher ist.[8] Das kann sich dann als problematisch erweisen, wenn er nur wenig über die technischen Abläufe während des Kommunikationsvorgangs weiß. Diese Verlagerung könnte einen Paradigmenwechsel für solche Kommunikationsverhältnisse auslösen.

3 Vertrauen in Kommunikation

Diese technischen Umstände erfordern beinahe selbstverständlich Vertrauen – Vertrauen der Kommunikationsteilnehmerinnen und -teilnehmer darauf, dass der Inhalt von den in welcher Funktion auch immer am Vorgang Beteiligten (also z. B. auch von den technischen Dienstleistern) sorgfältig und vertraulich behandelt wird. In diesem Zusammenhang ist allerdings zunächst einmal genauer zu erörtern, was für eine gesellschaftliche Funktion Vertrauen überhaupt erfüllt.

3.1 Die gesellschaftliche Funktion von Vertrauen

Der Begriff „Vertrauen“ entzieht sich einer einfachen, für alle denkbaren Situationen angemessenen Definition. In seiner grundlegendsten Form bezeichnet „Vertrauen“ einen psychischen Zustand, der sich auf ein Gegenüber bezieht und Erwartungen an dessen (künftiges) Verhalten formuliert. Wer einer anderen Person vertraut, der verlässt sich darauf, dass sich diese entweder so verhalten wird, wie es vereinbart worden ist, oder wie es den (berechtigten) Erwartungen der vertrauenden Person entspricht. Dies impliziert zu-

[7] Was zumindest bei der Kommunikation mit Behörden noch davon abhängig gemacht wird, dass der Bürger dieser Form der Informationsmitteilung vorher zugestimmt hatte.
[8] Z. B. darf der Nutzer Warnungen nicht ignorieren, dass Zertifikate, die zur Absicherung einer Verbindung genutzt werden, nicht gültig sind.

gleich einen Moment der Unsicherheit. Wäre es gesichert, wie sich die andere Person verhält, so wäre Vertrauen weniger wichtig oder gar unnötig. Deshalb ist es auch immer mit einem gewissen Risiko verbunden, der anderen Person Vertrauen zu schenken: Die Erwartung an deren Verhalten kann trotz Vertrauens stets enttäuscht werden. Auf der anderen Seite setzt Vertrauen ein Mindestmaß an Wissen über die andere Person voraus. Bei völliger Unkenntnis über die Eigenschaften des Gegenübers kann nur auf ein erwünschtes künftiges Verhalten gehofft, jedoch nicht darauf vertraut werden.[9]

In der immer komplexer und unübersichtlicher werdenden modernen Gesellschaft, so der Soziologe Niklas Luhmann, reicht dieses interpersonale Vertrauen allein allerdings nicht mehr aus. Denn täglich kommt es zu Interaktionen mit Personen und anderen Akteuren wie Unternehmen oder Behörden, zu denen keine persönliche Beziehung besteht und über die der Kommunizierende so gut wie nichts wissen kann, denen er aber trotzdem ein gewisses Vertrauen entgegenbringen muss, damit die Interaktion in der jeweils angezeigten Weise erfolgreich sein kann. Interpersonales Vertrauen muss daher durch das sogenannte Systemvertrauen ersetzt bzw. ergänzt werden. Die Erwartungen an das Funktionieren des Systems, dessen Teil der Einzelne ist, wird dadurch stabilisiert, dass darauf vertraut werden kann, dass sich die Mitglieder des Systems den ihnen zugewiesenen Rollen entsprechend verhalten.[10]

Ist dieses Systemvertrauen gegeben, so Luhmann, dann kann Vertrauen seine zentrale gesellschaftliche Funktion erfüllen und als entscheidender Mechanismus dienen, die Komplexität unserer Interaktionen mit anderen innerhalb der modernen Gesellschaft zu reduzieren. Auf diese Weise macht es Vertrauen möglich, mit den Unsicherheiten und Unwägbarkeiten, die der heutigen Gesellschaft inhärent sind, zurechtzukommen. Systemvertrauen macht diese Unsicherheit tolerierbar und versetzt den Einzelnen somit in die Lage, trotz der undurchschaubaren Komplexität, die sichere Voraussagen über die Zukunft verhindert, Entscheidungen zu treffen und so überhaupt handlungsfähig zu bleiben.[11]

3.2 Bezugspunkte des Vertrauens in der digitalen Welt

Die sich hieran anschließende Frage ist, was Vertrauen angesichts seiner Funktion für die Kommunikation in der modernen Gesellschaft bedeutet. So ist einerseits zu fragen, worauf sich Vertrauen in der digitalen Welt bezieht, um dann zu eruieren, ob es seine Funktion insoweit erfüllen kann. Mit anderen Worten: Zu erörtern ist, wann davon gesprochen werden kann, dass digital übermittelte Kommunikation überhaupt vertrauenswürdig ist.

Vertrauen in die Kommunikationsmittel kommt gerade in der digitalen Welt, in einer Informations- und Kommunikationsgesellschaft, eine wichtige Rolle zu. Zwar wurde von einigen

[9] Walter Bamberger, Interpersonal Trust – Attempt of a Definition, 2010, http://www.ldv.ei.tum.de/en/research/fidens/interpersonal-trust/.
[10] Niklas Luhmann, Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität, 3. Aufl., Stuttgart 1989, Kapitel 7.
[11] Bamberger, ebenda.

Anhängern der sogenannten Post-Privacy-Bewegung[12] behauptet, dass es eines solchen Vertrauens nicht mehr bedürfe. Die Teilnehmerinnen und Teilnehmer digitaler Kommunikation sollen hiernach an der Vertraulichkeit von Informationen und Kommunikationsinhalten gar nicht mehr interessiert sein, was – wenn man hiervon tatsächlich ausgehen könnte – Vertrauen in ihren Schutz naturgemäß entbehrlich machen würde. Vor allem aufgrund der Verbreitung von Sozialen Netzwerken wie Facebook, Twitter, Instagram, aber auch Xing oder LinkedIn, ist wiederholt die Behauptung aufgestellt worden, der Begriff von Privatheit und damit auch der Inhalt dessen, was jeder Einzelne als privat oder intim anderen vorenthalten möchte, habe sich in der digitalen Gesellschaft grundlegend gewandelt und sei mittlerweile aufgeweicht. Da es ohnehin unmöglich sei, im Internet volle Kontrolle über die eigenen Daten zu behalten, müsse ein grundlegend anderer Umgang mit persönlichen Informationen gefunden werden. Unter anderem habe der traditionelle Datenschutz in seiner Funktion ausgedient.[13]

Die Vertreter von Post-Privacy repräsentieren aber mit ihren Ansichten weder die Mehrheit der Bevölkerung[14] noch behaupten selbst sie, dass es in der digitalen Welt keinerlei Privatsphäre oder Geheimhaltung/Datenschutz von sensiblen Informationen mehr geben sollte. Vielmehr ist sicherlich unbestritten, dass auch heute noch hochsensible Daten existieren, deren Sicherheit einem objektiven Schutzinteresse unterliegt und die vor dem unkontrollierten Zugriff durch Dritte geschützt werden müssen. Zu denken wäre an sensible Gesundheitsdaten oder auch Kreditkarteninformationen, Kontostände oder sonstige Daten, die die eigene finanzielle Sphäre betreffen.[15] Gelangen solche Daten in falsche Hände, werden kompromittiert oder missbraucht, können den Betroffenen erhebliche Schäden entstehen. Auch die persönliche Reputation kann betroffen sein, was im Einzelfall für Opfer existenzbedrohende Konsequenzen nach sich ziehen kann. Das gilt umso mehr in einer zunehmend digitalisierten Welt, in der Daten die Identität der Menschen prägen und repräsentieren. Die häufigen Fälle von Identitätsdiebstahl zeigen eindrücklich die Bedeutung einer nicht-manipulierten und authentischen Identität im digitalen Raum.

Auch wenn viele Menschen heute über Soziale Netzwerke einer oft nicht bestimmbaren Anzahl von Dritten einen beachtlichen Einblick in ihr Leben gewähren, kann nicht gefolgert werden, dass für sie die Privatheit bestimmter Informationen nachrangig ist. Wer eine E-Mail an eine gute Freundin schreibt, um von den Ergebnissen der letzten Vorsorgeuntersuchung zu berichten, wird darauf vertrauen wollen, dass außer der Freundin niemand mitliest. Wer seine Kontoauszüge auf dem Online-Portal seiner Bank abruft, wird darauf vertrauen, dass bei der Übertragung niemand die Daten abfängt und kopiert – den meisten

[12] Vgl. Christian Heller, Post Privacy: Prima leben ohne Privatsphäre, München 2011; Gary Younge, Social Media and the Post-Privacy Society, Guardian, 2. April 2012, https://www.theguardian.com/commentisfree/cifamerica/2012/apr/02/social-media-and-post-privacy-society; Nova Spivack, The Post-Privacy World, Wired, Juli 2013, https://www.wired.com/insights/2013/07/the-post-privacy-world/.
[13] Jan Rähm, Wissenschaftler plädieren für einen neuen Datenschutz, Deutschlandfunk, 9. Juli 2016, http://www.deutschlandfunk.de/also-doch-post-privacy-wissenschaftler-plaedieren-fuer.684.de.html?dram:article_id=359646.
[14] Siehe hierzu weiter unten, Punkt 3.4.
[15] Stephan Dörner, Die Deutschen sind erschreckend uninformiert, Welt.de, 27. Juli 2015, https://www.welt.de/wirtschaft/webwelt/article144508313/Die-Deutschen-sind-erschreckend-uninformiert.html.

wird klar sein, dass diese Daten sehr leicht zum finanziellen Nachteil des Betroffenen missbraucht werden können, sollten sie in die falschen, also kriminelle Hände geraten. Mehr noch, die Person wird darauf vertrauen, dass sie nach der Eingabe der Webadresse der Bank im Browserfenster auch tatsächlich auf die Seite der Bank geleitet wird und nicht auf die eines Dritten, die nur genauso aussieht. Wer in einer E-Mail, die von der eigenen Bank zu stammen vorgibt, einen Link zum Webportal anklickt, um beispielsweise den aktuellen Kontoauszug herunterzuladen, wird jedenfalls darauf hoffen, dass die Nachricht keine Fälschung ist und der Link in betrügerischer Absicht zur Seite eines Kriminellen führt.[16] Und auch wenn jedem bewusst sein dürfte, dass alle Nutzerinnen und Nutzer ständig Datenspuren im Netz hinterlassen, die für interessierte Stakeholder Rückschlüsse auf unser Verhalten und unsere Vorlieben zulassen, werden die meisten dennoch zumindest darauf vertrauen wollen, dass diese Daten nicht gegen sie, also zu ihrem unmittelbaren Nachteil verwendet werden.

Vertrauen in Kommunikationsvorgänge erfüllt eine ganz wesentliche Funktion. Sie liegt darin, dass die mitteilende Person mit hinreichender Sicherheit vorhersagen kann, was mit den übermittelten Daten und Informationen geschieht und ob und inwieweit sie vor dem Zugriff durch Akteure, die nicht unmittelbar an dem Vorgang beteiligt sind und die nicht legitimiert sind oder die die mitteilende Person nicht legitimiert hat, geschützt sind. Dies gilt für jede, zumindest jede durch Technik vermittelte, Individualkommunikation, unabhängig von den verwendeten Kommunikationsmitteln.

Es lässt sich also festhalten, dass Nutzerinnen und Nutzer von vertrauenswürdiger Kommunikation – ob digital oder analog – erwarten, dass:

- die Daten und Informationen, die sie übermitteln, insoweit geschützt sind, dass sie nicht in die Hände Krimineller oder generell unbefugter Dritter geraten;
- die Daten und Informationen von den Informationsempfängern nicht zum unmittelbaren Nachteil der Nutzerinnen und Nutzer verwendet werden;
- einzelne, sensible Informationen nicht der allgemeinen Öffentlichkeit zugänglich gemacht werden;
- die Person bzw. das Unternehmen oder die staatliche Stelle, mit der kommuniziert wird, auch tatsächlich diejenige ist, für die sie sich ausgibt;
- die Informationen nicht verfälscht worden sind,
- die versandte Nachricht tatsächlich und innerhalb kurzer Zeit den Empfänger erreicht.

[16] Wobei in diesem Zusammenhang darauf hinzuweisen ist, dass das Phänomen des Phishings (siehe unten 3.5.1) inzwischen zu einem so großen Problem geworden ist, dass ein Vertrauen auf die Authentizität eines Links in einer E-Mail nicht mehr empfohlen werden kann.

Vergleichbare Anforderungen kann auch der Empfänger stellen, beispielsweise möchte er in der Regel sicherstellen, dass der Absender auch derjenige ist, als der er sich ausgibt, und er hat auch ein Interesse an unverfälschten Nachrichten. Vertrauenswürdige Kommunikation hat also beidseitig hohe Ansprüche an Privatheit und Integrität der Inhalte, Authentizität von Sender und Empfänger und an Effektivität und Verlässlichkeit der Zustellung.

3.3 Maßnahmen zur Herstellung von Systemvertrauen

Erörtert wurde bislang, was für eine Funktion Vertrauen, v. a. Systemvertrauen, erfüllt und worauf sich dieses bei Kommunikationsvorgängen, insbesondere in der digitalen Welt, bezieht. Da Vertrauen hier aufgrund der Komplexität praktisch nur als Systemvertrauen aufgebaut und aufrechterhalten werden kann, ist deshalb weiter zu fragen, wie dieses hergestellt, bestärkt und gewährleistet werden kann. In Betracht kommen in erster Linie technische, rechtliche und organisatorische Vorkehrungen.

3.3.1 Technische Absicherung

Technische Absicherung von Vertrauen in analoge Kommunikation

Wer einen Brief verschickt, zumal wenn dieser sensible Informationen enthält, muss zunächst einmal vertrauen, dass der mit der Versendung beauftragte Dienst den Brief wie vereinbart zum Adressaten liefert. Hierfür sind das Vertrauen in die Rolle des Dienstes und seiner Mitarbeiter sowie die Erwartungshaltung aufgrund vertrauensbildenden vergangenen Verhaltens ausreichend. Sollte sich herausstellen, dass Briefe regelmäßig auf dem Weg verloren gehen und nie ankommen, dürfte der Dienst alsbald seine Kundinnen und Kunden verlieren.

Schon seit Jahrhunderten aber ist dieses Vertrauen in die Integrität des Kuriers als nicht hinreichend erachtet worden – selbst wenn er den ihm übergebenen Brief stets verlässlich bei der richtigen Person abgeliefert hat. Dieser Umstand genügte jedoch nicht, um ein solides Vertrauen dahingehend zu erzeugen, dass der Brief auch ungeöffnet und damit ungelesen beim Empfänger ankam. Die räumliche Distanz zwischen Versender und Empfänger machten Briefe in besonderem Maße gefährdet für Zugriffe durch Dritte und damit die Verletzung der Privatheit des Inhalts. Schon frühzeitig wurde das Vertrauen in das System der Briefzustellung deshalb durch technische Methoden abgesichert. Mit Hilfe von Siegeln wurden Briefe so verschlossen, dass niemand den Brief öffnen konnte, ohne das Siegel zu zerstören und somit die Handlung zu offenbaren. Noch heute werden Briefumschläge so verschlossen, dass ihr Inhalt im Normalfall nicht unbemerkt von jemand anderem als dem bezweckten Adressaten gesichtet werden kann. Zugespitzt könnte man sagen, dass der Briefverkehr viele Merkmale einer digitalen Ende-zu-Ende-Verschlüsselung aufweist: Der Versender verschließt die Nachricht oder versiegelt sie gar und erst der vorgesehene Empfänger öffnet den Umschlag und erhält somit Zugriff auf den Inhalt.

Technische Unterstützung von Systemvertrauen in Kommunikation in der digitalen Welt

Wie bereits ausgeführt, erschweren spezifische Eigenschaften der digitalen Sphäre das Entstehen von Vertrauen bei den Nutzerinnen und Nutzern von Online-Kommunikationsdiensten. Einige der Faktoren, die eine zentrale Rolle spielen, wenn sich Vertrauen zwischen Kommunikationsteilnehmerinnen und -teilnehmern herausbilden soll, lassen sich nur schwer oder sogar gar nicht im Cyberspace abbilden. Aspekte wie erleichterte Anonymität, flexible Identitäten, Entkörperlichung oder nur schwer durchschaubare Kontexte, vor deren Hintergrund Kommunikation stattfindet, unterminieren interpersonales Vertrauen.[17] Hinzu kommt, dass viele vormals sichtbare Vorgänge, die im Zusammenhang mit Kommunikation nun digital erfolgen, im Verborgenen stattfinden und jedenfalls für den technisch durchschnittlich informierten Bürger kaum nachvollziehbar sind, was es zusätzlich erschwert, den Prozess als vertrauenswürdig zu empfinden.

Da interpersonales Vertrauen aus diesen Gründen insofern noch schwerer zu realisieren ist als bei Kommunikation, die auf analogen Wegen erfolgt, liegt es nahe, bei digitaler Übermittlung von Informationen das Vertrauen in das System noch stärker durch technische Maßnahmen abzusichern bzw. zu unterstützen. Hierbei geht es neben dem Schutz des Inhalts der Kommunikation auch um die Authentizität; also darum, dass die Identität des Absenders verifiziert werden kann und sichergestellt ist, dass die Nachricht tatsächlich von dem Absender stammt, von dem sie zu stammen scheint. Obwohl es selbstverständlich schon im analogen Zeitalter möglich war, Schriftstücke zu fälschen, ist dies durch digitale Hilfsmittel um ein Vielfaches einfacher geworden.

Anders als beim herkömmlichen Briefverkehr ist die Ende-zu-Ende-Verschlüsselung von versendeten Nachrichten allerdings beim E-Mail-Verkehr nicht der Normalfall. Ganz im Gegenteil ist die gewöhnliche E-Mail, die als digitale Kommunikationsform bislang dominiert, weniger mit dem geschützten Brief, sondern eher mit der ungeschützten Postkarte vergleichbar. Nicht selten wird bei der Kommunikation via E-Mail überhaupt keine Verschlüsselung eingesetzt, die Nachricht also offen über das Internet verschickt. Doch selbst wenn eine Transportverschlüsselung wie TLS für den Weg zwischen den E-Mail-Providern des Absenders und des Empfängers verwendet wird und auch die Kommunikation zwischen dem Nutzer und dem Server des Providers verschlüsselt abläuft – bei Einsatz eines E-Mail-Clients über Protokolle wie SMTPS, POP3S oder IMAPS, bei Nutzung eines Webmailers mittels verschlüsselter HTTPS-Verbindung – ist die Vertraulichkeit des Inhalts der Nachricht noch immer nicht gewährleistet. Denn die E-Mails werden im Regelfall auf den Servern der Provider unverschlüsselt gespeichert und sind dort wie Postkarten für jeden lesbar, der Zugriff hat oder sich verschafft.[18] Das können kriminelle Hacker sein, aber ebenso staatliche Geheimdienste oder auch der Anbieter des E-Mail-Services selbst, der

[17] Helen Nissenbaum, Will Security Enhance Trust Online, or Supplant It?, in: R. Kramer und K. Cook (Hg.), Trust and Distrust Within Organizations: Emerging Perspectives, Enduring Questions, New York 2004, S. 155, 161 f.
[18] Vgl. Wikipedia, E-Mail, https://de.wikipedia.org/wiki/E-Mail.

beispielsweise die Inhalte der gespeicherten E-Mails auf Schlüsselworte hin durchsuchen kann, um darauf basierend gezielt Werbung zu schalten.[19]

Erst die wirkliche Ende-zu-Ende-Verschlüsselung, bei der die E-Mail von der versendenden Person vor der Übergabe an den Provider verschlüsselt und von der empfangenden Person erst auf dem eigenen Rechner wieder entschlüsselt wird, rechtfertigt die Analogie zum Brief.[20] Dafür bieten sich verschiedene, mehr oder weniger komfortable Lösungen an, auf die im zweiten Themenpapier näher eingegangen wird.[21]

Sind solche Technologien bei der Kommunikation via E-Mail heute noch eher die Ausnahme, so kommt Ende-zu-Ende-Verschlüsselung inzwischen standardmäßig bei vielen der bekannten Instant-Messaging-Dienste wie Threema, Signal, SIMSme, iMessage oder WhatsApp zum Einsatz. Auch Portallösungen, bei denen sich der Nutzer auf der Webseite des Unternehmens oder der Behörde per Passwort und gegebenenfalls zusätzlich mittels eines TAN-Verfahrens anmelden muss,[22] um direkt von dort Dokumente oder Informationen herunterzuladen, bieten einen deutlich höheren Schutzstandard als gewöhnliche E-Mails. Hier wird die Sicherheit zum einen dadurch hergestellt, dass die Verbindung zwischen dem Computer des Nutzers und dem Server mittels HTTPS verschlüsselt abläuft. Darüber hinaus werden die jeweiligen Dokumente bzw. Informationen in dem Online-Postfach häufig zusätzlich verschlüsselt gespeichert.[23]

3.3.2 Rechtliche Absicherung

Neben den beschriebenen technischen Maßnahmen können auch rechtliche Vorschriften zur Herstellung und Stärkung von Systemvertrauen in Kommunikation dienen. Schützt das Recht nicht davor, die Integrität, Authentizität und Vertraulichkeit von Individualkommunikation zu verletzen, kann sich Vertrauen in das System der Kommunikation nur schwer entwickeln oder leicht nachhaltig beschädigt werden. Als ein Beispiel, in diesem Fall aus der „analogen Zeit“, sei die Praxis der Abteilung „M“ des Ministeriums für Staatssicherheit in der Deutschen Demokratischen Republik genannt, Briefe mittels spezieller technischer Vorrichtungen zu öffnen und wieder zu schließen und dabei kaum sichtbare Spuren am Briefumschlag zu hinterlassen.[24] Solche Maßnahmen schädigen die Privatheit der Kommunikation. Werden sie bekannt (was letztlich bei derlei gravierenden Verletzungen fast immer geschieht), unterminieren sie das Vertrauen in das Kommunikationssystem als solches. Es wird in der Folge nicht mehr für vertrauliche Kommunikation genutzt werden.

---

[19] Siehe als Beispiel Googles Gmail: Florian Rötzer, Bei jeder Mail wird mitgelesen, Telepolis, 2. April 2004, https://www.heise.de/tp/features/Bei-jeder-Mail-wird-mitgelesen-3434025.html.
[20] Lars Meyer, Wann sind E-Mails „sicher“?, Datenschutz Notizen, 8. Januar 2016, https://www.datenschutz-notizen.de/wann-sind-e-mails-sicher-2713442/.
[21] Für einen Überblick vgl. Wikipedia, E-Mail-Verschlüsselung, https://de.wikipedia.org/wiki/E-Mail-Verschl%C3%BCsselung.
[22] Wikipedia, Transaktionsnummer, https://de.wikipedia.org/wiki/Transaktionsnummer.
[23] Siehe als ein Beispiel die Datenschutzbestimmungen der CosmosDirekt, C.1 und C.3: https://www.cosmosdirekt.de/finanzassist-datenschutz/.
[24] Hanna Labrenz-Weiß, Abteilung M, MfS-Handbuch, Berlin 2005, S. 28, http://www.bstu.bund.de/DE/Wissen/Publikationen/Publikationen/handbuch_abt-m_labrenz-weiss.pdf?__blob=publicationFile.

Insofern erklärt es sich, dass die Nachrichtenübermittlung per Brief schon mit Beginn der Neuzeit rechtlich abgesichert wurde, um das Vertrauen der Bürgerinnen und Bürger in das System zu stützen. Die Allgemeine Preußische Postordnung von 1712 sanktionierte Postbeamte mit Entlassung und Bestrafung wegen Meineids. In Frankreich drohte hierfür ab 1742 gar die Todesstrafe.[25]

In Deutschland wird das Brief- und Postgeheimnis seit 1949 durch Artikel 10 des Grundgesetzes sogar als Grundrecht geschützt. In erster Linie adressiert es wie alle Grundrechte den Staat: Es verbietet, dass staatliche Bedienstete selbst Briefe öffnen. Darüber hinaus entfaltet es aber auch eine Drittwirkung insofern, dass es den Staat darüber hinaus verpflichtet, mittels gesetzlicher Regeln dafür Sorge zu tragen, dass auch im Postwesen tätige private Dienstleistungsunternehmen und sonstige Dritte die Vertraulichkeit des Inhalts von Briefen nicht verletzen.[26] Zu diesen gesetzlichen Regeln gehört unter anderem das Strafrecht. Hierdurch wird jede Person strafrechtlich sanktioniert, die das Briefgeheimnis (§ 202 Strafgesetzbuch) oder das Post- oder Fernmeldegeheimnis (§ 206) verletzt.

Auch digitale Kommunikationsvorgänge werden neben den genannten technischen Schutzmaßnahmen durch rechtliche Garantien flankiert, die den Zweck verfolgen, das Vertrauen in das System abzusichern. In erster Linie handelt es sich hierbei wiederum um grundrechtliche Garantien.

So umfasst der Artikel 10 des Grundgesetzes zunächst einmal nicht nur das Brief- und Postgeheimnis, sondern schützt als Fernmeldegeheimnis genauso Inhalte und Umstände individueller Kommunikationsvorgänge, die drahtlos oder drahtgebunden mittels elektromagnetischer Signale erfolgen. Da es auf die konkrete Übermittlungsart hierbei nicht ankommt, erstreckt sich der Schutz auf die Kommunikation via Internet.[27] Auch hier richtet sich das Grundrecht nicht nur an den Staat selbst, um dessen eigene Handlungsmöglichkeiten zu beschränken; er hat im Sinne einer Drittwirkung des Grundrechts auch dafür zu sorgen, dass private Kommunikationsdienstleister das Recht nicht verletzen. Entscheidend ist insoweit allerdings, dass die Nachrichten nur dann und so lange von Artikel 10 geschützt sind, wie sie zwischen Absender und Empfänger unterwegs sind – was ein Speichern auf den Servern des E-Mail-Dienstleisters allerdings mit einschließt, wie das Bundesverfassungsgericht im Jahr 2009 mit Hinweis auf den Schutzzweck des Grundrechts entschied.[28] Befinden sich die Informationen noch auf dem Computer des ersteren oder sind bereits angekommen und beim Empfänger gespeichert, greift der Schutzbereich des Grundrechts nicht mehr.[29]

[25] Vgl. Wikipedia, Briefgeheimnis, https://de.wikipedia.org/wiki/Briefgeheimnis.
[26] Bodo Pieroth und Bernhard Schlink, Grundrechte – Staatsrecht II, 23. Auflage, Heidelberg 2007, S. 191.
[27] Pieroth/Schlink, S. 193.
[28] Bundesverfassungsgericht, Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers nicht verfassungswidrig, Pressemitteilung Nr. 79/2009, 15. Juli 2009, http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-079.html.
[29] Entscheidung des Bundesverfassungsgerichts im Fall „Kommunikationsdaten“, 2. März 2006, http://www.servat.unibe.ch/dfr/bv115166.html.

Daten, die sich auf dem Computer einer Person selbst befinden und Auskunft über diese erteilen können, werden nicht durch das Fernmeldegeheimnis, sondern allgemein durch datenschutzrechtliche Regelungen geschützt. Grundrechtlich unterfüttert werden diese durch das Recht auf informationelle Selbstbestimmung, welches durch das Bundesverfassungsgericht im sogenannten Volkszählungsurteil als Unterfall des allgemeinen Persönlichkeitsrechts herausgebildet worden war.[30] Es definiert die Befugnis jeder Person, im Grundsatz stets selbst darüber bestimmen zu können, ob ihre persönlichen Daten preisgegeben und wie und wofür sie verwendet werden.[31] Weil aber das Recht auf informationelle Selbstbestimmung nach der Konzeption des Bundesverfassungsgerichts notwendig darauf beschränkt ist, vor gezielten und punktuellen Datenerhebungen durch den Staat zu schützen, greift es dann nicht, wenn staatliche Stellen beispielsweise den gesamten Computer eines Bürgers ausspähen oder überwachen. Um diese Schutzlücke zu schließen, entwickelte das Gericht in einer weitreichenden Entscheidung von 2008 das sogenannte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, das verfassungsrechtlichen Schutz vor Online-Durchsuchungen gewährt.[32] Sobald digitale Kommunikationsvorgänge also abgeschlossen und die sensiblen Informationen auf dem Rechner des Empfängers gespeichert sind, wird deren Vertraulichkeit nicht mehr durch das Fernmeldegeheimnis, sondern je nach Kontext durch eines der beiden vorgenannten Rechte geschützt. Auch diese beiden Grundrechte richten sich wiederum in zweierlei Hinsicht an den Staat. So ist er einerseits angehalten, sie nicht durch eigene, nicht gerechtfertigte Maßnahmen zu verletzen.[33] Zum anderen hat er durch gesetzliche Vorgaben – hier insbesondere datenschutzrechtliche Vorschriften wie das Bundesdatenschutzgesetz und die Datenschutzgesetze der Länder – dafür zu sorgen, dass auch private Akteure den Datenschutz achten.

Die beiden genannten Grundrechte sowie die Datenschutzgesetze werden ebenfalls durch strafrechtliche Vorschriften ergänzt. So stellt der § 202a des Strafgesetzbuchs das Ausspähen von Daten unter Strafe, die gespeichert und gegen unberechtigten Zugriff gesichert sind, während es § 202b Strafgesetzbuch sanktioniert, wenn jemand Daten, die nicht für ihn bestimmt sind, während einer nichtöffentlichen Datenübermittlung abfängt. Da der § 206 Strafgesetzbuch zudem ausdrücklich auch Verletzungen des Fernmeldegeheimnisses umfasst, sind damit sämtliche Phasen digitaler Kommunikationsvorgänge gegenüber unberechtigten Dritten strafrechtlich abgesichert. Auch das Bundesdatenschutzgesetz selbst umfasst Vorschriften, die Verstöße entweder mit Bußgeld oder sogar mit Strafe sanktionieren.[34]

[30] Entscheidung des Bundesverfassungsgerichts im Fall „Volkszählung“, 15. Dezember 1983, http://www.servat.unibe.ch/dfr/bv065001.html.
[31] Claudio Franzius, Das Recht auf informationelle Selbstbestimmung, Zeitschrift für das juristische Studium 3/2015, S. 259.
[32] Ebd., S. 262 f.
[33] Nicht gerechtfertigt sind solche Maßnahmen insbesondere dann, wenn sie ohne gesetzliche Grundlage vorgenommen werden und/oder nicht verhältnismäßig sind.
[34] Siehe §§ 43, 44 Bundesdatenschutzgesetz; die Gesetze der Länder enthalten entsprechende Bestimmungen.

Rechtliche Absicherungen sind nur dann in der Lage, Systemvertrauen herzustellen bzw. abzusichern, wenn das Recht auch durchgesetzt wird. Dies ist in der digitalen Welt insbesondere im Hinblick auf die Drittwirkung der genannten Grundrechte und damit auf das Handeln privater Akteure wie beispielsweise E-Mail-Dienstleistern nicht immer unproblematisch. So bemängeln Datenschutzbeauftragte, dass Verstöße gegen datenschutzrechtliche Bestimmungen kaum sanktioniert werden.[35] Dies kann mitunter auch eine Folge des Umstands sein, dass (noch) nicht immer klar ist, wie sich bestimmte rechtliche Konstruktionen auf digitale Kommunikationsvorgänge übertragen lassen. So beharrt Google beispielsweise auf dem Standpunkt, das Fernmeldegeheimnis sei auf die Praxis des Scannens von E-Mails, die auf den Servern des Unternehmens (zwischen-)gespeichert sind, nicht anwendbar, da es sich um automatisierte, also nicht unmittelbar durch Menschen gesteuerte Prozesse handelt.[36]

3.3.3 Organisatorische Absicherung

Neben der technischen und der rechtlichen kann auch eine organisatorische Absicherung zur Stärkung von Vertrauen führen. In Frage kommen Maßnahmen vielfältiger Art. Organisation als Merkmal erfordert als Träger häufig eine Institution, und diese kann beispielsweise durch prozess- oder regelbasiertes Arbeiten, durch die Einführung geeigneter Rollen, durch Selbstverpflichtungen, durch Zertifizierungen oder durch eine lange Tradition verlässlichen Handelns vertrauensstiftend wirken.

Ein Beispiel für prozessbasiertes Arbeiten ist, dass bei technischen Administrationsaufgaben ein Vieraugenprinzip eingesetzt oder bei telefonischen Anfragen von Kunden Wert auf eine eindeutige Identifikation gelegt wird. Ein wirkungsvoller Datenschutzbeauftragter in einer sichtbaren Rolle kann Missbräuche rechtzeitig erkennen oder im Vorfeld verhindern. Eine Selbstverpflichtung hat eine Bindewirkung, die aufgrund eines potenziellen Reputationsschadens bei deren Verletzung mit entsprechenden wirtschaftlichen Folgen wirksam sein kann. Eine Zertifizierung durch bekannte Prüforganisationen signalisiert Transparenz und führt im Rahmen der entsprechenden Vorbereitung zumindest zu einer erhöhten Aufmerksamkeit für die betreffenden Themen. Eine lange Tradition verlässlichen Handelns schließlich ist ein Ausweis einer hohen Professionalität über einen längeren Zeitraum, was beispielsweise auch markenprägend und damit vertrauensfördernd wirken kann.

[35] Christiane Schulzki-Haddouti, Datenschutz-Verstöße werden sehr selten sanktioniert, Der Datenschutz-Blog, 4. April 2016, https://www.datenschutzbeauftragter-online.de/datenschutz-verstoesse-werden-sehr-selten-sanktioniert/9536/.

[36] Bei Einführung von Googles E-Mail-Dienst Gmail im Jahr 2004 hatten Beauftragte für den Datenschutz verschiedener Länder die Ansicht vertreten, die Praxis, E-Mails zu Werbezwecken routinemäßig automatisiert zu scannen, verstoße gegen das Briefgeheimnis und das Recht auf Privatsphäre, vgl. RP Online, Staatsanwalt soll Google-Mail überprüfen, 18. Mai 2004, https://www.datenschutzbeauftragter-online.de/datenschutz-verstoesse-werden-sehr-selten-sanktioniert/9536/; in einem Gerichtsprozess im kalifornischen San Jose im Jahr 2013 führte Google hingegen explizit aus, automatisierte Verarbeitung der E-Mails könne keine Verletzung der Rechte darstellen. Mehr noch: “Just as a sender of a letter to a business colleague cannot be surprised that the recipient’s assistant opens the letter, people who use web-based email today cannot be surprised if their communications are processed by the recipient’s ECS [electronic communications service] provider in the course of delivery.” Dominic Rushe, Google: Don’t Expect Privacy When Sending to Gmail, The Guardian, 15. August 2013, https://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit.

Ein weiterer Grund für die Bedeutung von Organisation ist, dass diese es erst ermöglicht, dass Recht in zielgerichtetes Verhalten, z.B. auch technischer Natur, umgesetzt wird. Sie ist damit ein wichtiger Transmissionsmechanismus, der rechtliche Vorschriften wirksam und technische Maßnahmen umsetzbar macht.

3.4 Mangelndes Vertrauen in der digitalen Welt

Die vorstehenden Ausführungen haben gezeigt, dass Vertrauen in Kommunikation in der digitalen Welt besonderen Herausforderungen ausgesetzt ist. Da systemisches Vertrauen in Kommunikation jedoch nach wie vor wichtig, man könnte sagen: wichtiger denn je, ist, wird es durch technische, rechtliche und organisatorische Maßnahmen gestützt. Fraglich ist, ob diese Maßnahmen ausreichen, um Vertrauen herzustellen bzw. wie es tatsächlich um das Vertrauen in Kommunikation in der digitalen Welt bestellt ist.

Bereits im Juli 2013 wies die damalige Bundesjustizministerin Sabine Leutheusser-Schnarrenberger in einem Interview mit der Süddeutschen Zeitung darauf hin, dass das Vertrauen in die digitale Kommunikation aufgrund von Datenschutz- und Überwachungsskandalen beeinträchtigt ist.[37] Auch die Bundestagsfraktion der Grünen konstatierte in einem Antrag an die Bundesregierung im Sommer 2016, mit dem sie etwas gegen den „Stillstand beim E-Government“[38] in Deutschland unternehmen wollte, dass die geringe Akzeptanz vorhandener Angebote im Netz jedenfalls „auch auf ein mangelndes Vertrauen der Bürgerinnen und Bürger in Datensicherheit und Datenschutz“ zurückzuführen ist.[39]

Aktuelle repräsentative Befragungen stützen die These, dass Misstrauen gegenüber den Kommunikationswegen im digitalen Zeitalter in der Bevölkerung verbreitet ist, und das nicht nur in Bezug auf das Verhältnis zu staatlichen Angeboten. Skepsis kommt auch gegenüber der Kommunikation mit privatwirtschaftlichen Unternehmen zum Ausdruck.

So kam eine Anfang März 2017 im Auftrag von DIVSI durch dimap durchgeführte Umfrage zu dem Ergebnis, dass es die Mehrheit der Bürger (55 Prozent) „eher schlecht“ oder „sehr schlecht“ findet, wenn Unternehmen oder Behörden wichtige Dokumente und Informationen ihren Kunden bzw. Bürgern per E-Mail zustellen oder in einem Online-Postfach zum Abruf hinterlegen.[40] Zwar sind deutliche Unterschiede zwischen den einzelnen Altersgruppen festzustellen. Deutsche unter 35 haben deutlich weniger Berührungsängste in dieser Hinsicht: 58 Prozent der Befragten in dieser Altersgruppe finden die elektronische Zustel-

[37] Wolfgang Janisch und Heribert Prantl, Interview mit Justizministerin Leutheusser-Schnarrenberger, Vertrauen in digitale Kommunikation ist beeinträchtigt, Süddeutsche Zeitung, 6. Juli 2013, http://www.sueddeutsche.de/politik/justizministerin-leutheusser-schnarrenberger-vertrauen-in-digitale-kommunikation-ist-beeintraechtigt-1.1714126.

[38] „E-Government“ wird insoweit ganz allgemein als der digitale Austausch zwischen Bürgern und Unternehmen auf der einen, und staatlichen Einrichtungen auf der anderen Seite verstanden.

[39] Antrag der Fraktion Bündnis 90/Die Grünen, Stillstand beim E-Government beheben – Für einen innovativen Staat und eine moderne Verwaltung, BT-Drucksache 18/9056, 6. Juli 2016, S. 2, http://dip21.bundestag.de/dip21/btd/18/090/1809056.pdf.

[40] DIVSI, „Elektronische Dokumentenzustellung“, repräsentative dimap-Umfrage ab 18 Jahren, 1. und 2. März 2017, https://www.divsi.de/wp-content/uploads/2017/03/2017-03-08_Unterlage_DIVSI-dimap-Umfrage_Dokumentenzustellung.pdf.

lung von Dokumenten und Informationen gut. Die entgegengesetzte Einstellung ist bei den Bürgern über 65 zu beobachten, von ihnen sind zwei Drittel skeptisch.

Noch auffälliger als die Skepsis gegenüber der Übermittlung oder Bereitstellung von Informationen durch Unternehmen oder Behörden auf digitalem Wege ist die in der gleichen Befragung zum Ausdruck gekommene Sorge, dass die persönlichen Daten der Kunden bzw. Bürger auf digitalen Kommunikationskanälen nicht sicher sind. Ganze 64 Prozent, also beinahe zwei Drittel aller Teilnehmerinnen und Teilnehmer, gaben an, in dieser Hinsicht „eher besorgt“ oder „sehr besorgt“ zu sein. Dieser Umstand impliziert einen Mangel an Vertrauen gegenüber digitalen Kommunikationsmitteln, wenn es darum geht, dass Unternehmen oder Behörden sensible Informationen an Kunden bzw. Bürger übermitteln. Nutzer sind sich unsicher, ob an diesem entscheidenden Punkt ein hinreichender Schutz gewährleistet werden kann.

Andererseits belegt die Studie nicht eindeutig, dass es aufgrund mangelnden Vertrauens in die Sicherheit der Daten und Informationen verbreitet abgelehnt wird, wichtige Dokumente auf elektronischem Wege übermittelt zu bekommen.

Andere Befragungen, die sich mit der Einstellung von Bürgern zu E-Government-Angeboten befassen, scheinen eine entsprechende Korrelation ebenfalls nicht unmittelbar zu bestätigen. So ergab eine von der Europäischen Kommission im Jahr 2014 durchgeführte (allerdings europaweite) Studie, dass die Sorge um die Sicherheit der persönlichen Daten nur für insgesamt elf Prozent der Befragten ein Problem darstellt, wenn es um die Nutzung von Angeboten des E-Governments geht.[41] Als viel wesentlicheren Grund für die fehlende Akzeptanz durch die Bürger wurden von 80 Prozent der Befragten die geringe Nutzerfreundlichkeit bzw. eine generelle Präferenz, persönlich mit dem zuständigen Mitarbeiter der Behörde in Kontakt zu treten, angegeben.

Der eGovernment MONITOR, der jährlich vom Institute for Public Information Management gemeinsam mit der Initiative D21 durchgeführt wird, kommt für das Jahr 2016 zu dem Ergebnis, dass die Nutzung von E-Government-Angeboten in Deutschland leicht steigt, allerdings noch immer nicht einmal jeder zweite deutsche Onliner auf diese zurückgreift (45 Prozent).[42] Dieser Studie zufolge gaben im Jahr 2014 noch zwei Drittel der Befragten in Deutschland an, dass Bedenken bezüglich Sicherheit und Schutz sensibler persönlicher Daten sie von der Nutzung der Angebote abhielten. Dieser Wert ist zwar für 2016 auf nur noch etwas mehr als ein Drittel (34 Prozent) gesunken[43], zeigt aber dennoch die Bedeutung dieser Themen für einen signifikanten Teil der Nutzer.

[41] Siehe McKinsey & Company, E-Government in Deutschland – Eine Bürgerperspektive, März 2015, S. 5, https://www.mckinsey.de/files/e-government_in_deutschland_eine_buergerperspektive.pdf.
[42] IPIMA und Initiative D21, eGovernment MONITOR 2016 – Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich, September 2016, S. 6, http://initiatived21.de/app/uploads/2016/12/egovmon2016_web.pdf.
[43] Ebd., S. 7.

Von denjenigen Befragten, die Sorgen bezüglich Sicherheit und Schutz sensibler Daten äußerten, waren für jeweils die Hälfte Angst vor Datendiebstahl sowie ein Mangel an Information darüber, was mit den Daten passiert, die gewichtigsten Gründe für das fehlende Vertrauen. Als weitere Faktoren wurden die Sorge vor mangelnder Sicherheit bei der Datenübertragung (48 Prozent), vor dem möglichen Zusammenführen von Daten in einer zentralen Datenbank („gläserner Bürger“, 48 Prozent) und Bedenken hinsichtlich der Sorgfalt im Umgang mit den Daten vonseiten der Behörden (46 Prozent) genannt.[44]

Obwohl auch diese Zahlen 2016 deutlich niedriger waren als noch zwei Jahre zuvor, geht aus ihnen jedenfalls hervor, dass die Menschen nicht mehrheitlich in einem „Post-Privacy“-Zeitalter leben wollen und ihnen Datenschutz und Vertrauen in sensible Kommunikation wichtig sind. Wer digital kommuniziert, wird zumindest darauf vertrauen wollen, dass sensible Daten ein Mindestmaß an Schutz vor dem Zugriff Dritter genießen.

3.5 Gründe für mangelndes Vertrauen in der digitalen Welt

Der Feststellung, dass ein Misstrauen in Kommunikationswege in der digitalen Welt weit verbreitet ist, schließt sich die Frage nach den Gründen an. Dazu ist zunächst festzuhalten, dass die Entstehung von Vertrauen von einer Reihe von Faktoren abhängig ist. Individuell vertrauen wir anderen Personen, wenn wir ihr künftiges Verhalten zumindest zu einem bestimmten Grad voraussehen können, es also eine gewisse Konsistenz aufweist. Der primäre Gradmesser hierfür ist ihr Verhalten in der Vergangenheit.[45] Wird die so geformte Erwartungshaltung durch eine Handlung, die die Konsistenz durchbricht, enttäuscht, so geht Vertrauen verloren. Daneben spielen andere Aspekte eine Rolle, wenn Vertrauen gebildet werden soll, wie bestimmte als vertrauenswürdig akzeptierte Eigenschaften, zum Beispiel Ehrlichkeit, Loyalität oder Besonnenheit.[46]

Vertrauen in ein System ist ebenfalls davon abhängig, dass es sich als stabil erweist, also in einem Mindestmaß konsistent ist, so dass die Erwartungen des Einzelnen an das Verhalten des Systems nur im Ausnahmefall enttäuscht werden. Stabilität wird insbesondere dann erreicht, wenn sich die Akteure, die an dem System beteiligt sind, ihren (beruflichen oder institutionellen) Rollen entsprechend verhalten.[47] Repräsentanten des Systems Kommunikation sind beispielsweise Briefträger oder E-Mail-Serviceprovider.

3.5.1 Ursachen für systemisches Misstrauen gegenüber Kommunikation in der digitalen Welt

In der digitalen Sphäre wird die Herausbildung von Vertrauen dadurch erschwert, dass an jedem Kommunikationsvorgang neben dem unmittelbaren Kommunikationspartner eine Vielzahl mittelbarer weiterer Teilnehmer beteiligt sind – so zum Beispiel die E-Mail-Dienstleister. Da die kommunizierenden Personen deshalb oft gar nicht wissen können,

[44] Ebd., S. 17.
[45] Nissenbaum, S. 159.
[46] Ebd.
[47] Bamberger, ebenda.

wer alles von den Inhalten des Vorgangs Kenntnis nehmen kann, ist das Vertrauen in den Kommunikationsweg von vornherein erheblich erschwert. Durch diese Komplexität kommt dem Systemvertrauen in der digitalen Welt eine noch einmal erhöhte Bedeutung zu. Es ist für die Kommunikationsteilnehmerinnen und -teilnehmer schwieriger, überhaupt Vertrauen aufzubauen. Zugleich ist es leichter zu enttäuschen und zu unterminieren. Kommt es dadurch abhanden, so kann es seine Funktion nicht mehr erfüllen. In dem Fall steigt das inhärente Risiko für die kommunizierende Person. Dies reduziert ihre Handlungsfähigkeit und führt im Extremfall dazu, dass die Kommunikation ganz abgebrochen oder von vornherein unterlassen wird.

Trotz technischer Maßnahmen zum Schutz digitaler Kommunikationsvorgänge und zusätzlich rechtlicher Absicherung sowohl gegen das Handeln des Staates als auch Privater wie auch organisatorischer Vorkehrungen bekannter Unternehmen hat in den vergangenen Jahren eine Vielzahl unterschiedlicher Vorkommnisse dazu geführt, dass das Systemvertrauen in digitale Kommunikationsmittel erheblich Schaden genommen hat.[48]

So ist beispielsweise Internetkriminalität heute an der Tagesordnung, die ihren Ausgangspunkt zumeist in der Manipulation oder Störung von Kommunikationsvorgängen nimmt. Sogenannte Phishing-Attacken, die den Zweck verfolgen, die Identität des Opfers zu stehlen oder sensible Daten wie Bank- oder Kreditkarteninformationen abzugreifen, gehören zu den häufigsten Formen der Kriminalität im Netz. Die Angriffe werden dabei immer raffinierter und bedienen sich immer häufiger des sogenannten Social Engineering, also der manipulierenden Beeinflussung von Zielpersonen, um sie zu bestimmten, kompromittierenden Handlungen zu verleiten. Durchgeführt werden diese im Regelfall mittels einer E-Mail, die entweder von einer Person zu kommen scheint, der der Empfänger der Nachricht vertraut, oder die sonst einen auf ihn zugeschnittenen, persönlichen und vertrauenserweckenden Inhalt aufweist.[49] Ist man erst einmal Opfer einer solchen Straftat geworden, so wird man der Kommunikation über Online-Kanäle künftig nur noch wenig Vertrauen entgegenbringen. Doch schon die durchaus erschreckenden Statistiken und regelmäßigen Medienberichte über groß angelegte Phishing-Attacken allein können potentiell zu einem Vertrauensverlust in der Bevölkerung beitragen.[50]

Auch staatliche Stellen haben in den vergangenen Jahren ihren Anteil daran gehabt, dass Vertrauen in digitale Kommunikation verloren gegangen ist.[51] Es ist zu einer ganzen Reihe von sich häufig sogar wiederholenden Ereignissen gekommen, die das Vertrauen in die Kommunikation der Bürgerinnen und Bürger mit Behörden und Unternehmen erschüttert haben. Um nur das prominenteste Beispiel zu nennen: Im Jahr 2013 enthüllte der NSA-Whistleblower Edward Snowden, dass die Geheimdienste vor allem der Vereinigten Staa-

[48] Vodafone Institut, Auf dem Weg zum digitalen Staat: Erfolgsbedingungen von E-Government-Strategien am Beispiel Estlands, 2014, S. 5, http://www.vodafone-institut.de/wp-content/uploads/2015/09/VFI_eGovEra_DE.pdf.
[49] Bundeskriminalamt, Internetkriminalität/Cybercrime, https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html.
[50] Vgl. Bitkom, Jeder zweite Internetnutzer Opfer von Cybercrime, 13. Oktober 2016, https://www.bitkom.org/Presse/Presseinformation/Jeder-zweite-Internetnutzer-Opfer-von-Cybercrime.html.
[51] Vgl. Bitkom, Vertrauen in Datensicherheit im Internet schwindet weiter, 9. Dezember 2013, https://www.bitkom.org/Presse/Presseinformation/Vertrauen-in-Datensicherheit-im-Internet-schwindet-weiter.html.

ten und des Vereinigten Königreichs jahrelang massenhaft die digitale Kommunikation von Nutzerinnen und Nutzern weltweit überwacht hatten und bis heute überwachen.[52] In Deutschland wiederum plant die Bundesregierung, eine „Zentralstelle für Informationstechnik im Sicherheitsbereich“ zu errichten, zu deren Aufgaben es unter anderem gehören soll, Methoden zu entwickeln, Verschlüsselungen von Kommunikationsdiensten zu brechen.[53] Auch durch solche Maßnahmen wird die Vertraulichkeit des Inhalts von digitaler Kommunikation jedes Einzelnen potentiell kompromittiert.

3.5.2 Vertrauensverlust trotz Sicherheit

Das Systemvertrauen in digitale Kommunikation wird nicht nur durch unbefugte Eingriffe durch Dritte, durch Sicherheitslücken oder illegale Handlungen erschwert.[54] Vielmehr veranlasst auch im Grunde sichere Kommunikation, bei der sich Unbefugte oder Unbeteiligte (rechtswidrig) Zugang zum Kommunikationsvorgang verschaffen, zunehmend systemisches Misstrauen.

So legen die zitierten Studien nahe, dass das Vertrauen in die Kommunikation in der digitalen Welt nicht nur dadurch untergraben wird, dass die Vorgänge nicht „sicher“ sind bzw. als nicht sicher empfunden werden. „Sicherheit“ impliziert in diesem Zusammenhang eine Abwehr nach außen, also den Schutz der sensiblen Daten und Informationen vor dem Zugriff durch Dritte, die nicht legitimiert wurden, an dem Kommunikationsvorgang teilzunehmen. Das können, wie ausgeführt, Kriminelle oder Geheimdienste sein.

Gerade in der Onlinewelt wird das Vertrauen darüber hinaus häufig bereits durch diejenigen beeinträchtigt, die vom Nutzer im Grunde befugt wurden, Einsicht in den Kommunikationsvorgang zu nehmen bzw. an diesem teilzunehmen. Viele Anwendungen zur digitalen Kommunikation können heute gar nicht mehr gestartet werden, ohne dass sich der Nutzer zuvor über die Zustimmung zu den allgemeinen Vertragsbedingungen – die im Normalfall gar keine oder jedenfalls kaum Beachtung finden – dazu bereit erklärt hat, den Anbieter bis zu einem gewissen Grad „mitlesen“ zu lassen bzw. das Abgreifen von Daten zuzulassen. So warnten Datenschutzexperten bei der Einführung von Googles E-Mail-Dienst Gmail im Jahr 2004 davor, dass das Scannen der Inhalte der E-Mails durch den Anbieter mit dem Zweck, kontextbasierte und damit gezieltere Werbung anzeigen zu können, das implizite systemische Vertrauen der Verbraucher in E-Mail-Dienstleister beeinträchtigen würde.[55] Auch Plattformbetreiber wie Social Media-Unternehmen sammeln zumeist Daten über ihre registrierten Nutzerinnen und Nutzer, gerade auch wenn diese über die Dienste miteinander kommunizieren, und lassen sich dazu über die allgemeinen Vertragsbedin-

[52] Siehe z.B. Oslo University Library, Global Surveillance, An Annotated and Categorized Overview of the Revelations Following the Leaks by the Whistleblower Edward Snowden, http://www.ub.uio.no/fag/informatikk-matematikk/informatikk/faglig/bibliografier/no21984.html.
[53] Georg Mascolo, Neue Behörde soll für Regierung verschlüsselte Kommunikation knacken, sueddeutsche.de, 23. Juni 2016, http://www.sueddeutsche.de/digital/sicherheitspolitik-neue-behoerde-soll-fuer-regierung-verschluesselte-kommunikation-knacken-1.3047884.
[54] Vgl. Nissenbaum, S. 166 ff.
[55] Privacy Rights Clearinghouse, Thirty-One Privacy and Civil Liberties Organizations Urge Google to Suspend Gmail, 6. April 2004, https://www.privacyrights.org/blog/thirty-one-privacy-and-civil-liberties-organizations-urge-google-suspend-gmail.

gungen von den Nutzerinnen und Nutzern die Genehmigung erteilen. Über die Einzelheiten solcher Handlungen und deren Regeln herrscht bei den Nutzerinnen und Nutzern häufig Unsicherheit und Unkenntnis. Gründe hierfür sind, unter anderem, die Komplexität von Nutzungsbedingungen und Rechtsgrundlagen, die Aufdeckung unwahrer Behauptungen der Diensteanbieter und Vieles mehr.

Hinzu kommt das Problem der Spam-Mails, also unerwünschter E-Mails, die zumeist Werbung enthalten. Spam basiert nicht, jedenfalls nicht in erster Linie, auf mangelnder Sicherheit, sondern schlicht auf dem Phänomen, dass der Versand einer E-Mail (anders als bei physischer Post) kaum Kosten verursacht. Spam hat dazu geführt, dass E-Mail als Kommunikationsform erheblich an Vertrauen eingebüßt hat. Bereits im Jahr 2003 kam eine US-amerikanische Studie zu dem Schluss, dass Spam zu Einschränkungen der Nutzung von E-Mails führt. 73 Prozent der damals Befragten gaben an, aufgrund des Phänomens ihre E-Mail-Adresse nicht mehr herauszugeben.[56]

Schließlich ist zu erwägen, ob und inwieweit sich der beschriebene Paradigmenwechsel von der Bring- zur Holschuld negativ auf das Vertrauen der Nutzerinnen und Nutzer in digitale Kommunikation auswirken könnte. Auch hier geht es weniger um das Problem, dass die von Unternehmen oder Behörden bereitgestellten Portallösungen nicht sicher sind – es kann wohl davon ausgegangen werden, dass Kommunikationsverbindungen zu diesen Portalen im Normalfall den gängigen Verschlüsselungsstandards genügen. Ein Faktor, der das Vertrauen mindert, könnte jedoch beispielsweise sein, dass es durch die Verschiebung zur Holschuld zunehmend den Nutzerinnen und Nutzern aufgebürdet wird, die Übersicht darüber zu behalten, bei wie vielen Portalen relevante Dokumente oder Informationen regelmäßig abzurufen sind. Zwar werden Nutzerinnen und Nutzer für gewöhnlich per E-Mail (die zumeist auch einen entsprechenden Link direkt zum jeweiligen Portal enthalten) darüber informiert, dass diese zum Abruf bereitstehen. Dennoch ist mit dieser Art der Kommunikation eine Verantwortungsverlagerung verbunden. Es ist deshalb jedenfalls durchaus denkbar, dass eine solche Unübersichtlichkeit zu einem Gefühl der Unsicherheit im Netz beiträgt.

4 Fazit

Es lässt sich festhalten, dass viele Menschen der digitalen Kommunikation aus verschiedenen Gründen nicht vertrauen. Vertrauen in die Integrität, Authentizität und Vertraulichkeit von Individualkommunikation ist in der digitalen Welt wichtiger denn je. Trotz mangelnden Vertrauens benutzen die meisten Menschen ständig v. a. digitale Kommunikationsmittel für jede Art von Kommunikation, gleich welchen Inhalts (sensibel, wenig sensibel). Ein direkter Zusammenhang zwischen dem weit verbreiteten Misstrauen und dem Kommunikationsverhalten ist insofern nicht ersichtlich. Letztlich hat diese „Ignoranz des Misstrauens“ zwar große Vorteile, denn hielte das Misstrauen von digitaler Kommunikation

[56] Andreas Wilkens, US-Studie: Werbemüll beschädigt das Vertrauen in E-Mails, Heise Online, 23. Oktober 2003, https://www.heise.de/newsticker/meldung/US-Studie-Werbemuell-beschaedigt-das-Vertrauen-in-E-Mails-87321.html.

ab, würde der Fortschritt verweigert und aufgehalten. Dabei sind digitale Kommunikationsmittel nicht nur absolut üblich, sondern sie bieten, offensichtlich, in vielerlei Hinsicht erhebliche Vorzüge und Möglichkeiten. Digitale Kommunikation ist nicht nur schnell und preisgünstig. E-Government-Dienste beispielsweise können die Verwaltung und Bürokratie erheblich vereinfachen und entlasten und somit zu Effizienzgewinnen führen. Hierdurch kann – auch auf Seiten des Bürgers – Zeit und Geld eingespart werden. Gleiches gilt für geschäftliche Interaktionen mit Unternehmen. Für diese ergeben sich unmittelbar geschäftliche Nachteile, wenn ihnen insoweit kein „Vertrauenskapital“ durch ihre Kundinnen und Kunden zugestanden wird.

Die Erkenntnis dieser Untersuchung zeigt einen gravierenden Missstand auf: Kommunikation spielt in der digitalen Welt eine herausragende Rolle für das soziale, berufliche und private Leben der Menschen. Um diesem Bedürfnis nachzukommen, benutzen die Menschen – bewusst oder unbewusst, wohl oder übel – ständig Kommunikationsmittel, die nicht sicher sind und denen sie ganz häufig nicht vertrauen. Das wiederum bereitet vielen offensichtlich Sorgen und führt zu Effizienz- und Systemvertrauensverlusten. Es stellt sich daher die Frage, der im nächsten Themenpapier weiter nachzugehen sein wird, wie man diesem Missstand abhelfen könnte.