Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 22.01.2020

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Innenausschusses zum Thema

Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken

am 27. Januar 2020

Husarenstraße 30
53117 Bonn
Fon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de

Verschlüsselung ist Grundrechtsschutz!

Seit Jahrzehnten wird kontrovers über die Auswirkungen der Nutzung kryptographischer Verfahren diskutiert. Die Eckpunkte der deutschen Kryptopolitik stammen bereits aus dem Jahr 1999, gelten inhaltlich gleichwohl fort. Die Kernfrage ist geblieben: Wie kann es gelingen, Kryptographie und Sicherheitsinteressen auszubalancieren? Sicherheit *durch* Verschlüsselung bei gleichzeitiger Sicherheit *trotz* Verschlüsselung?

Dies vorausgeschickt, unternimmt die vorliegende Stellungnahme nicht den Versuch einer Kommentierung der gesamten Kryptodebatte, sondern versteht sich als pointierte Positionierung in dieser fortwährenden Diskussion.

Die Haltung des Datenschutzes

Verschlüsselung ist die Basis für den Schutz der Privatsphäre eines jeden Einzelnen und fast jeder wirtschaftlichen Betätigung in der digitalen Welt. Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist es erforderlich, Daten wirkungsvoll vor Zugriffen Unberechtigter schützen zu können. Der Einsatz von Kryptographie ist hierbei ein ganz elementares Instrument.

Unsere Aufgabe muss es daher sein, die Nutzung der Verschlüsselung bestmöglich zu fördern. Wir brauchen einfache und sichere Lösungen für den Einsatz moderner kryptographischer Verfahren. Einfach zu bedienende Verschlüsselungsverfahren müssen ohne Einschränkungen für jedermann nutzbar sein. Die Bundesregierung selbst fordert im Koalitionsvertrag, eine „Ende-zu-Ende-Verschlüsselung für jedermann verfügbar“ zu machen, s. Zeilen 1979 ff. des Koalitionsvertrags der 19. Legislaturperiode des Bundestages.

Datenschutz und IT-Sicherheit sind wichtige Einflussfaktoren für eine kluge Industriepolitik. Eine verantwortungsbewusste und sinnvolle technologische Weiterentwicklung ist ohne Datenschutz und IT-Sicherheit undenkbar. Wir sind deshalb gut beraten, in Deutschland und Europa den Einsatz von Verschlüsselungstechnologien zu forcieren und ihre (Weiter-)Entwicklung zu unterstützen. Eine generelle Herabsenkung des Kryptoniveaus unterwandert das Vertrauen in die digitale Welt. Sie ist deshalb zwingend zu verhindern.

Die Forderung nach einer rechtlichen Verankerung eines Rechts auf Verschlüsselung ist vor diesem Hintergrund zu begrüßen.

1. Recht auf Verschlüsselung – Verschlüsselung ist als technisch-organisatorische Maßnahme bereits rechtlich verankert

Gemäß Artikel 5 Abs. 1 lit. f) Datenschutzgrundverordnung (DSGVO) sind personenbezogene Daten in einer Weise zu verarbeiten, die eine angemessene Sicherheit dieser Daten ge-

währleistet. Dies schließt auch den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen mit ein („Integrität und Vertraulichkeit“).

Wie in Art. 34 Abs. 3 lit. a) DSGVO erläuternd dargestellt wird, zielt Verschlüsselung darauf ab, Daten für Unbefugte unzugänglich zu machen. Damit erfüllt sie eine unmittelbar grundrechtsdienende Funktion, die bereits vom Bundesverfassungsgericht in seiner Entscheidung zum „Volkszählungsurteil“ statuiert wurde: Sie schafft einen Freiraum für die freie persönliche Entscheidungen eines jeden Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Mit Art. 32 Abs. 1 DSGVO wird den Verantwortlichen und Auftragsverarbeitern die Pflicht auferlegt, geeignete technische und organisatorische Maßnahmen zur Sicherung personenbezogener Daten zu treffen. Die DSGVO nennt explizit die Verschlüsselung als Maßnahme, um Datenschutzrisiken zu reduzieren und ein angemessenes Schutzniveau zu gewährleisten, vgl. Art. 32 Abs.1 lit. a).

Risikobezogen ist die Verschlüsselung stets unter Berücksichtigung der Umstände der konkret bezweckten Verarbeitung mit in Betracht zu ziehen. Verschlüsselung ist damit mehr als eine unverbindliche Empfehlung. Denn immer dann, wenn hohe Risiken für die Rechte und Freiheiten natürlicher Personen bestehen und es zu Schutzverletzungen kommt, werden Verantwortliche die kritische Frage beantworten müssen, warum auf eine erforderliche Verschlüsselung verzichtet wurde.

Geeignete technische und organisatorische Maßnahmen sind nach Art. 25 DSGVO auch erforderlich, um den Grundsätzen und Anforderungen des „Datenschutzes durch Technikgestaltung“ zu genügen. Zwar lässt der Gesetzgeber weitgehend offen, welche konkreten Schutzmaßnahmen dies umfasst, zumindest aber die Verschlüsselung ist hierzu zu zählen.

Dabei müssen die eingesetzten Sicherheitsverfahren selbstverständlich stets dem Stand der Technik entsprechen und auch tatsächlich zu einem geeigneten Schutzniveau führen. Um diese Schutzwirkung nicht zu konterkarieren, dürfen keine Hintertüren in die Verschlüsselungssysteme eingebaut werden, die ansonsten einen unbefugten Informationszugang ermöglichen könnten. Dies gilt für eine potentielle Nutzung eingebauter Schwachstellen durch berechtigte Stellen ebenso wie für eine Nutzung durch (kriminelle) Dritte.

2. Recht auf Verschlüsselung

Die Vertraulichkeit der Kommunikation ist ein verfassungsrechtlich verbrieftes Grundrecht. Es wird in das Grundrecht des Art. 10 Grundgesetz (GG) eingriffen, wenn gesetzliche Rege-

lungen hinsichtlich der geschützten Kommunikationsformen die Möglichkeit zur Verschlüsselung von Kommunikationsinhalten einschränken (BeckOK Grundgesetz/Ogorek GG Art. 10 Rn. 53). Es muss den Kommunikationsteilnehmern anheimgestellt bleiben, wie sie die Vertraulichkeit des Informationsaustausches gewährleisten wollen und wer von dem Inhalt Kenntnis erlangen soll (BeckOK Grundgesetz/Ogorek GG Art. 10 Rn. 53 m.w.N.).

Aber auch nach Abschluss der laufenden Kommunikation – also, wenn der Schutzbereich des Art. 10 GG endet – sind Betroffene nicht schutzlos. So stellte das Bundesverfassungsgericht unmissverständlich klar, dass das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst (BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07). Eine heimliche Infiltration eines informationstechnischen Systems, mit der die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist daher verfassungsrechtlich nur in engen Grenzen zulässig (sog. Online-Durchsuchung). Hierfür müssen im Einzelfall tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen.

Diesem erheblichen grundrechtlichen Schutzbedürfnis würde es nicht entsprechen, wenn Selbstschutzmöglichkeiten – wie die Verschlüsselung – durch staatliche Aktivitäten konterkariert würden. Der Staat muss vielmehr eine möglichst ungehinderte Persönlichkeitsentfaltung ermöglichen, indem er diese Schutzmöglichkeiten bestmöglich ausbaut, etwa durch eine positivrechtliche Statuierung eines Rechts auf Verschlüsselung.

Kontraproduktiv ist es, wenn Gesetzesinitiativen den gegenteiligen Weg beschreiten, indem sie versuchen, das Sicherheitsniveau des Art. 32 DSGVO abzusenken. Beispielsweise sollen mit einer aktuellen Anpassung der Abgabenordnung auch sensible Daten der Bürgerinnen und Bürger auf Basis einer Einwilligung mit einer unverschlüsselten E-Mail von den Finanzbehörden übermittelt werden können. Die sichere Verarbeitung personenbezogener Daten ist aber gerade nicht disponibel. Sie kann deshalb auch nicht durch eine Einwilligung eingeschränkt werden.

Ebenso kritisch ist die – leider regelmäßig auch in Deutschland diskutierte – Bestrebung, für Nutzer Herausgabepflichten für verwendete Schlüssel oder Passwörter einer Verschlüsselung vorzusehen. Ein entsprechendes Vorgehen verstößt gegen den Grundsatz der Selbstbelastungsfreiheit (nemo-tenetur-Grundsatz). Dieser Grundsatz wird in der Rechtsprechung als selbstverständlicher Ausdruck einer rechtsstaatlichen Grundhaltung bezeichnet, der auf dem Leitgedanken der Achtung vor der Menschenwürde beruht (BVerfG NJW 1981, 1431).

Auch ist es abzulehnen, Diensteanbieter zur Herausgabe von Schlüsseln, Passwörtern etc. zu verpflichten. Dies würde in der Eingriffsintensität einer Online-Durchsuchung gleichkommen, ohne jedoch gleichzeitig die dort notwendigen technischen und organisatori-

schen Maßgaben einhalten zu können, mit der diese Maßnahme kontrollierbar gestaltet werden kann. Zu den technischen und organisatorischen Maßnahmen, die Anbieter nach Art. 32 DSGVO zur Datensicherheit zu treffen haben, gehört auch die sicher verschlüsselte Speicherung und Übermittlung von Passwörtern. Technisch gesehen werden gesetzeskonform arbeitende Anbieter die Passwörter folglich ohnehin als Hash speichern. Sie könnten die gewünschten Informationen daher gar nicht herausgeben. Eine Pflicht zur Speicherung der Zugangsdaten in einer durch Dritte leicht aufhebbaren Verschlüsselung oder gar im Klartext würde die Datensicherheit und den Datenschutz massiv konterkarieren.

3. Ende-zu-Ende-Verschlüsselung von Kommunikationsdiensten

Die fehlende Vertraulichkeit einer unverschlüsselten E-Mail-Kommunikation ist allseits bekannt. Unverschlüsselte E-Mails entsprechen im Hinblick auf den Schutz der Vertraulichkeit dem Versand per Postkarte. Wenn Informationen also im Falle eines Postversands nicht per Postkarte, sondern nur in einem verschlossenen Umschlag verschickt werden würden, dann sollten sie auch beim elektronischen Versand in einer verschlüsselten E-Mail übermittelt werden.

Zwar muss nicht zwangsläufig jedwede Übermittlung personenbezogener Daten auf elektronischem Wege per Ende-zu-Ende Verschlüsselung erfolgen. Die Ende-zu-Ende-Verschlüsselung stellt aber eine mögliche, bei Datenübermittlungen wichtige Maßnahme dar, ein angemessenes Schutzniveau zu gewährleisten. Grundsätzlich sollte daher beispielsweise bei der Übermittlung von E-Mails immer eine Ende-zu-Ende-Verschlüsselung angestrebt werden und somit den Standardanwendungsfall darstellen. Dies gilt insbesondere für E-Mails mit besonders sensiblen Inhalten (s.o.). Nutzer und Anbieter sollten deshalb die notwendigen technischen Voraussetzungen schaffen, um eine verschlüsselte Ende-zu-Ende-Kommunikation durchführen zu können. Mit einer zunehmenden Zahl von Nutzern, wird sich der verschlüsselte Versand dann auch zwischen Privatpersonen zügig verbreiten.

Da es in der Praxis aber in absehbarer Zeit noch immer nicht durchgängig möglich sein wird, eine Ende-zu-Ende-Verschlüsselung durchzusetzen, sollte wenigstens eine Transportverschlüsselung implementiert werden. Diese kann mittel- und langfristig eine Ende-zu-Ende-Verschlüsselung nicht ersetzen, aber kurzfristig einige Risiken bei der Nutzung von E-Mails reduzieren.

Eine proaktive, sichere und damit vertrauenswürdige Technikgestaltung setzt auch voraus, sich bereits bei Standardisierungsprozessen aktiv um ein Höchstmaß an Sicherheit zu bemühen (privacy by design). Hierzu zählt unter anderem der nachdrückliche Einsatz für eine standardmäßige Ende-zu-Ende-Verschlüsselung in neuen Telekommunikationstechnologien, wie dies z.B. bei der Spezifikation von 5G-Netzen versäumt wurde.

4. Plädoyer für eine standardisierte Informationsweitergabe von IT-Sicherheitslücken

Die Digitalisierung durchdringt alle Lebensbereiche. Der Cyber- und Informationssicherheit kommt hierbei eine herausragende Bedeutung zu. Die Sammlung von Informationen über IT-Sicherheitslücken, aber auch Schadprogrammen und IT-Sicherheitsvorfällen ist für ein Gesamtlagebild von enormer Bedeutung. Es ist gut, wenn das Bundesamt für Sicherheit in der Informationstechnik (BSI) weiter zu einer Informationsdrehscheibe für IT-Sicherheit in Deutschland ausgebaut wird. Insbesondere staatliche Behörden sollten daher verpflichtet sein, IT-Sicherheitslücken unverzüglich an das BSI zu melden.

Zu berücksichtigen ist aber auch, dass IT-Sicherheit und Datenschutz unmittelbar miteinander verzahnt sind. IT-Sicherheit soll den Missbrauch, unberechtigten Zugang und die unberechtigte Nutzung personenbezogener Daten ausschließen. IT-Sicherheitsrisiken sind damit regelmäßig auch Datenschutzrisiken. Insoweit ist die Domäne der datenschutzrechtlichen Aufsichtsbehörden betroffen. Es ist daher wichtig, dass das BSI derartige Informationen unmittelbar an alle relevanten Behörden weiterleitet.

5. IT-Sicherheit und Datenschutz als Standortfaktor ausbauen

Datenschutz und IT-Sicherheit sind wichtige Differenzierungsmerkmale in einer digitalisierten Welt. Der Einsatz von Verschlüsselungstechnologien spielt hierbei eine herausragende Rolle. Sie ist auch und gerade wichtig, um einen effektiven Schutz vor Spionage, (Cyber-)Sabotage und Datendiebstahl zu gewährleisten. Es ist deshalb richtig, wenn im Koalitionsvertrag gefordert wird, dass „sicherheitsrelevante Schlüsseltechnologien […] besser vor einem Ausverkauf oder einer Übernahme geschützt werden [sollen], vgl. s. Zeilen 1979 ff. des Koalitionsvertrags der 19. Legislaturperiode des Bundestages.

Jegliche gesetzliche Beschränkungen oder Verbote kryptographischer Sicherheitssysteme sind kontraproduktiv und fahrlässig.

Eine besondere Bedeutung hat die Nutzung von frei verfügbaren, offenen und einfach handhabbaren Protokollen und Verschlüsselungsstandards. Mit ihrer Transparenz tragen sie dazu bei, ihre Überprüfbarkeit zu sichern und ihre Kontrolle zu erleichtern. Offene Standards sind zudem geeignet, unerwünschte Lock-in-Effekte zu vermeiden.

6. Keine grundsätzliche Schwächung des Kryptoniveaus

Sicherheits- oder Strafverfolgungsbehörden tragen seit Jahren vor, aufgrund eines zunehmenden „Going Dark-Effektes“ ihre Aufgaben nicht mehr effektiv wahrnehmen zu kön-

nen. Paradoxerweise steigen zwar die Datenmengen der berechtigen Stellen, gleichzeitig können die Informationen aber wegen der Verschlüsselung nicht im Klartext ausgewertet werden. Es wird schwieriger, Inhalte und Strukturen in den Daten zu erkennen und relevantes von nicht relevantem zu unterscheiden.

Dennoch lassen sich auch aus verschlüsselten Kommunikationsinhalten werthaltige Ermittlungsansätze generieren, etwa mit Blick auf Verbindungsdaten, die Beziehungsgeflechte offenbaren. Auch solche Auswertungen stellen bereits erhebliche Eingriffe in die Privatsphäre der betroffenen Menschen dar.

Soweit Sicherheits- und Strafverfolgungsbehörden heimlich in Datenbestände eingreifen, ist die Rechtsprechung des Bundesverfassungsgerichts zur sog. Online-Durchsuchung zu beachten. Eingriffe sind nur unter den dort dargestellten Voraussetzungen zur Abwehr konkreter Gefahren für überragend wichtige Rechtsgüter zulässig. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Bereits in der Vergangenheit hat es diverse Ansätze gegeben, auf dem Weg der Regulierung bzw. des Verbotes den kryptographischen Schutz von Kommunikation zu schwächen. Ein Beispiel dafür sind die US-Exportbeschränkungen für (damals) „starke“ Kryptographie, die in den Anfangstagen des World Wide Web dazu geführt haben, dass fast alle Internetnutzerinnen und -nutzer mit einem ungenügenden Schutz ihrer Kommunikation leben mussten. Letztlich führen alle diese Ansätze dazu, dass die Sicherheit *aller* Nutzerinnen und Nutzer geopfert wird, um auf die Kommunikation *einiger weniger* Akteure zugreifen zu können.

Bei der Frage, ob Ansätze wie ein Verbot sicherer Verschlüsselung oder das Einbauen von Hintertüren bzw. Schwachstellen in Kommunikationsinfrastruktur dem Gebot der Verhältnismäßigkeit genügen, wird somit die Antwort nicht nur aus grundsätzlichen, sondern auch aus praktischen Gesichtspunkten in der Regel ein klares „Nein“ sein.

7. Digitale Verwaltung – der Staat als Vorbild

Der Staat muss seiner Vorbildfunktion nachkommen. Richtigerweise wird daher auch in dem aktuellen Koalitionsvertrags gefordert, dass Bürgerinnen und Bürgern es ermöglicht werden soll, mit der Verwaltung über gängige Standards verschlüsselt zu kommunizieren (PGP/SMIME), s. Zeilen 1980 ff. des Koalitionsvertrags der 19. Legislaturperiode des Bundestages. Dies wäre ein erster wichtiger Schritt.

Die Sensibilisierung für den Einsatz von Verschlüsselungstechnologien ist eine weitere wichtige Aufgabe, bei der staatliche Stellen Mehrwerte schaffen können. Zusätzlich ist hier

aber ein gesamtgesellschaftliches Engagement von Politik, Wirtschaft und Gesellschaft insgesamt erforderlich. Ziel muss es sein, eine Kultur der *grundsätzlichen* Verschlüsselung zu verankern. Auch vor diesem Hintergrund wäre eine positivrechtliche Festschreibung eines Rechts auf Verschlüsselung sinnvoll.

Der Bundesregierung kommt nach alledem die herausragende Rolle zu, die richtigen Rahmenbedingungen für eine positive Entwicklung eines sicheren und vertrauenswürdigen digitalen Raums zu schaffen. Und Verschlüsselung ist hierfür nach meiner festen Überzeugung ein wesentlicher Erfolgsfaktor.