BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 72/2020
November 2020

zum

Entwurf für einen Beschluss des Rats zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung (Vermerk der Ratspräsidentschaft vom 6. November 2020)

Mitglieder des Ausschusses Datenschutzrecht

RA Klaus Brisch, LL.M.
RA Michael Dreßler
RAin Simone Eckert
RA Prof. Dr. Armin Herb, (Vorsitzender)
RA Dr. Wulf Kamlah
RAin Simone Kolb
RA Jörg Martin Mathis
RA Dr. Hendrik Schöttle
RA Prof. Dr. Ralph Wagner, LL.M.

RA André Haug, Vizepräsident BRAK
Referent Rafael Javier Weiske, BRAK Brüssel
RA Sebastian Aurich, LL.M., BRAK Berlin

Verteiler: **Europa**
Rat der Europäischen Union
Ständige Vertretung der Bundesrepublik Deutschland bei der Europäischen Union
Europäische Kommission
Europäisches Parlament
Europäischer Datenschutzbeauftragter
Vertretungen der Länder
Rat der Europäischen Anwaltschaften (CCBE)

Deutschland
Bundesministerium für Justiz und Verbraucherschutz
Bundesministerium des Innern
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte
Rechtsausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Landesjustizminister/Justizsenatoren der Länder
Rechtsanwaltskammern
Bundesnotarkammer
Bundessteuerberaterkammer
Bundesverband der Freien Berufe
Deutscher Anwaltverein
Deutscher Juristinnenbund
Deutscher Notarverein
Deutscher Richterbund
Neue Richtervereinigung e.V.
Patentanwaltskammer
Deutscher Steuerberaterverband e.V.
Wirtschaftsprüferkammer
Gesellschaft für Datenschutz und Datensicherheit e. V.
Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
Deutsche Vereinigung für Datenschutz e. V.
Bitkom e. V.
davit – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e. V.
eco – Verband der Internetwirtschaft e. V.
VAUNET – Verband Privater Medien e. V.
Stiftung Datenschutz
Datenschutzberater
Computer und Recht
Redaktionen der NJW, ZAP, AnwBl, DRiZ, FamRZ, FAZ, Süddeutsche Zeitung, Die Welt, taz, Handelsblatt, dpa, Spiegel, Focus, Deubner Verlag Online Recht, Beck aktuell, Jurion Expertenbriefing, Juris Nachrichten, LexisNexis Rechtsnews, Otto Schmidt Verlag

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

I. Sachverhalt

Aus Anlass des Terroranschlags vom 2. November 2020 in Wien haben sich die JHA-Ratsmitglieder in ihrer informellen Sitzung vom 3. November 2020 auf den Grundsatz Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung festgelegt. Nach der dort entworfenen Beschlussvorlage für den Rat müsse es den zuständigen Behörden möglich sein,

> *„auf rechtmäßige und zielgerichtete Art und Weise und unter vollumfänglicher Beachtung der Grundrechte und Datenschutzverordnungen auf Daten unter Wahrung der Cybersicherheit zuzugreifen. Technische Lösungen für den Zugriff auf verschlüsselte Daten müssen den Prinzipien Rechtmäßigkeit, Transparenz, Erforderlichkeit und Verhältnismäßigkeit entsprechen."*[1]

Für entsprechende Zugriffsmöglichkeiten solle ein rechtlicher Rahmen geschaffen werden (Ziffer 6 der Beschlussvorlage). Zu dessen konkreter Umsetzung verhält sich der Entwurf nicht. Entsprechende technische und operative Lösungen sollten in Absprache mit den Service Providern/Telekommunikationsanbietern und zuständigen Behörden entwickelt werden. Umfasst wäre ausweislich der Präambel auch Ende-zu-Ende-verschlüsselte Kommunikation. Praktisch werden derartige Lösungen nur in einem Verbot vollständiger Ende-zu-Ende-Verschlüsselung bestehen können. Denn deren Zweck und Haupteigenschaft ist es ja gerade, Zugriffe bzw. Einblicke von dritter Seite zu verhindern. Hierüber kann die betont technikoffene Gestaltung des Entwurfs nicht hinwegtäuschen. Die Grundrechtsrelevanz dieses Vorhabens sprechen die Ratsmitglieder in dem Entwurf selbst an, wenn sie zugleich die Bedeutung der Verschlüsselung für die Grundrechtsverwirklichung hervorheben.

II. Stellungnahme

Die Bundesrechtsanwaltskammer lehnt den Beschlussvorschlag ab und fordert den Ministerrat und die gesetzgebenden Organe der EU auf, von der Formel „Sicherheit trotz Verschlüsselung" jedenfalls insoweit Abstand zu nehmen, als damit auf eine Durchbrechung der Verschlüsselung gezielt wird.

In jedem Fall müsste die Vertraulichkeit anwaltlicher Kommunikation auf allen Kommunikationskanälen gewährleistet bleiben. Dies wäre bei etwaigen Gesetzesvorhaben zu berücksichtigen und sicherzustellen. Voraussetzung dessen wären auch eine bisher nicht erfolgte klare Benennung der mit einem Verschlüsselungsverbot einhergehenden Gefahren für den Rechtsstaat und eine angemessene Beteiligung der Öffentlichkeit und besonders betroffener Kreise.

[1] Ziffer 5 der Beschlussvorlage.

Im Einzelnen:

1. Beeinträchtigte Grundrechte

Das nach dem Resolutionsentwurf zwangsläufig zu verabschiedende Verschlüsselungsverbot wird es Nutzern entsprechender Kommunikationsdienste unmöglich machen, auf die Vertraulichkeit ihrer Kommunikation zu vertrauen.

a) Grundrechtsbeeinträchtigungen

Dies würde zwangsläufig Grundrechtsbeeinträchtigungen in erheblichem Ausmaß bedeuten, die in Ermangelung einer Eignung, Erforderlichkeit und Angemessenheit, nicht zu rechtfertigen sind (siehe dazu unten). Neben den offensichtlicheren Rechten – etwa auf Vertraulichkeit elektronischer Kommunikation bzw. Korrespondenz (Art. 8 Abs. 1 EMRK, Art. 7 Abs. 1 GRCh, Art. 10 Abs. 1 GG), Achtung des Privat- und Familienlebens (Art. 8 EMRK, 7 GRCh), Privatsphäre (Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG), Schutz personenbezogener Daten (Art. 8 Abs. 1 GRCh), Vertraulichkeit und Integrität informationstechnischer Systeme („IT-Grundrecht“ gemäß Urteil v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07) werden das Recht auf Eigentum (Art. 14 GG, Art. 17 GRCh, Art. 1 Zusatzprotokoll zur EMRK), die Freiheit der Berufsausübung (Art. 15 GRCh, Art. 12 GG) und nicht zuletzt die Freiheit der Medien (Art. 11 Abs. 2 GRCh, Art. 5 Abs. 1 GG unter dem Gesichtspunkt des Quellenschutzes) teils erheblich beeinträchtigt.

b) Beeinträchtigung des Mandatsgeheimnisses, des Zugangs zum Recht und des Rechtsstaats im Allgemeinen

Ferner würde ein Verschlüsselungsverbot die Einhaltung verfassungsrechtlich vorgegebener und strafbewährter Vertraulichkeitspflichten – etwa von Ärzten, Steuerberatern und Rechtsanwälten – auf breiter Front unmöglich machen. Der Zugang zu Dienst- und Unterstützungsleistungen, die solchen Vertraulichkeitspflichten unterliegen, würde erschwert. Dabei kann die Lösung keinesfalls darin bestehen, entsprechend verschwiegenheitsverpflichtete Berufsgruppen auf alternative Kommunikationsmittel zu verweisen. Dies gilt in besonderem Maß für die Anwaltschaft, denn anwaltliche Beratung muss in einem Rechtsstaat jederzeit über die von Bürgern und Institutionen genutzten Kommunikationswege zugänglich bleiben. Zudem stünde zu befürchten, dass, der üblichen Dynamik in der Diskussion um Überwachungskompetenzen folgend, in kürzester Zeit auch die der Anwaltschaft unter Umständen verbleibenden Kommunikationsmittel einer Überwachung zugänglich gemacht werden würden. Der Zugang zum Recht und die Vertraulichkeit anwaltlicher Kommunikation müssen aus rechtsstaatlichen Gründen nach deutschem und europäischem Verfassungs- bzw. Primärrecht (Art. 20 Abs. 2 GG, Art. 103 Abs. GG, Art. 47 Abs. 1 Satz 2 GRCh, Art. 6 Abs. 1 Satz 1, Abs. 3 lit. c EMRK) jederzeit gewährleistet sein. Soweit der Ministerrat mit dem Verschlüsselungsverbot eine gegenläufige Lösung anstrebt, würden Mandanten und Rechtsanwälte in ihren verfassungs- und primärrechtlich verbürgten Rechten aus Art. 6 Abs. 1 Satz 1, Abs. 3 lit. c EMRK, Art. 47 Abs. 1, 2 Satz 2 GRCh, Art. 20 Abs. 3, Art. 103 Abs. 1 GG, 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK, Art. 7 GRCh, Art. 12 Abs. 1 GG beeinträchtigt und in Ermangelung einer verfassungsrechtlichen Rechtfertigung hierfür auch in diesen Rechten verletzt.

2. Geeignetheit

Es ist bereits fraglich, ob und gegebenenfalls welche Erwägungen der Ministerrat mit Blick auf die bei der Schaffung einer derart grundrechtsrelevanten Eingriffsmöglichkeit verfassungsrechtlich geforderte Geeignetheit eines solchen Verschlüsselungsverbots angestellt hat. Dem konkreten Anlass des Beschlussvorschlages – dem Terroranschlag in Wien vom 2. November 2020 – lässt sich eine Eignung etwa zur Verhinderung oder Verfolgung terroristischer Straftaten bislang nicht entnehmen. Nach der öffentlichen Berichterstattung und nach ersten Stellungnahmen der zuständigen Behörden hierzu gab

es im Vorfeld des Attentats diverse Ermittlungs- und Überwachungs-Pannen (so etwa der ORF: orf.at/stories/3188343/). Der Attentäter war wegen terroristischer Delikte vorbestraft und wurde vom Verfassungsschutz überwacht. Die österreichischen Behörden hatten vor dem Attentat von der slowakischen Polizei Informationen zu einem versuchten Munitionskauf durch den Attentäter erhalten. Bislang ist nicht ersichtlich, dass neben dem Ministerrat überhaupt irgendjemand das Attentat auf fehlende Möglichkeiten zur Messenger-Überwachung zurückführt.

Damit reiht sich dieser vorgeblich anlassbezogene Regulierungsvorstoß in eine Kette ähnlicher Vorstöße zur Kommunikationsüberwachung ein, bei denen sich die Eignung und Erforderlichkeit weder dem Einzelfall noch der allgemeinen wissenschaftlichen Evidenz entnehmen ließ. Erst in ihrer Stellungnahme 65/2020 hatte die BRAK auf einen solchen Fall hingewiesen.

Gerade in dem als Überwachungsziel genannten Bereich der organisierten Kriminalität und terroristischer Bedrohungen, wird sich ein Verschlüsselungsverbot als wenig geeignet erweisen. Denn in diesen Bereichen wird auf entsprechende staatliche Zugriffsmöglichkeiten sehr zügig und professionell reagiert, im Zweifel durch Nutzung anderer Kommunikationsformen oder eigene Verschlüsselungssoftware. Was bliebe, wäre im Wesentlichen die Möglichkeit der Überwachung in Fällen niedrigschwelliger Kriminalität und vor allem in solchen Fällen, in denen überhaupt kein legitimes Interesse an einer Überwachung besteht, nämlich denen der alltäglichen Messenger-Kommunikation eines jeden Einzelnen.

3. Erforderlichkeit

In begrenztem Umfang mag die Überwachung verschlüsselter Inhalte wirksame Prävention bzw. Strafverfolgung ermöglichen. Zumeist stehen hier aber – wie im Falle des Terroranschlags von Wien – mildere Mittel zur Verfügung, die dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz entsprechend zunächst ausgeschöpft werden müssen. Insoweit bestehen in den Mitgliedstaaten neben der klassischen analogen Überwachung bereits zahlreiche gesetzliche Möglichkeiten der Telekommunikationsüberwachung und des Zugriffs auf IT-Systeme.

4. Angemessenheit

Angesichts der Auswirkungen und Gefahren, die ein Verschlüsselungsverbot mit sich bringen würde, erscheint der im Titel der Beschlussvorlage angedeutete angemessene Ausgleich zwischen sicherer Verschlüsselung und einem Verbot derselben nicht herstellbar. Letzteres müsste, um zu funktionieren, absolut gelten. Damit wäre eine grundsätzlich bestehende Überwachungsmöglichkeit für alle Lebensbereiche und Sektoren geschaffen – vom privaten Austausch über Wirtschaftskorrespondenz bis hin zu berufsgeheimnisgeschützter Kommunikation. Geheimdienste haben bereits unterschiedslos auf Internetdatenströme zugegriffen und ihr Interesse daran bekundet, dies künftig zu tun. Auch abseits der Geheimdienste und innerhalb der EU besteht die Gefahr, dass Ermittler Zugriffsmöglichkeiten überziehen oder missbrauchen. So sind etwa im Rahmen der Vorratsdatenspeicherung Fälle bekannt geworden, in denen z. B. journalistische Kommunikation überwacht wurde. Daneben besteht die Gefahr, dass für staatliche Stellen gedachte Zugriffsmöglichkeiten durch Kriminelle genutzt werden. Auch dies ist in der Vergangenheit bereits geschehen. Nicht zuletzt angesichts der zweifelhaften Eignung und Erforderlichkeit eines Verschlüsselungsverbotes kann das Interesse an einer effektiven Prävention und Strafverfolgung die Inkaufnahme dieser erheblichen Vertraulichkeitsrisiken nicht rechtfertigen.

5. Fehlende Erwägungen zum Schutz des Rechtsstaats und des Mandatsgeheimnisses

Abgesehen davon, dass eine dem Mandatsgeheimnis und damit den vorstehenden Grundrechten genügende Umsetzung des vom Ministerrat erwogenen Beschlusses nicht ersichtlich ist, gibt besonderen Anlass zur Sorge, dass die Auswirkungen des Regulierungsansinnens auf den Rechtsstaat und insbesondere den Schutz des Mandatsgeheimnisses in der Beschlussvorlage noch nicht einmal angesprochen wurden. Ohne entsprechende Erwägungen kann eine ernsthafte, rechtstaatlich orientierte Diskussion derartiger Vorhaben nicht erfolgen. Rechtsstaatsverstöße und Grundrechtsverletzungen sind dann vorprogrammiert.

6. Fehlende Einbeziehung der Öffentlichkeit

Ebenso besorgniserregend ist, dass der Beschluss und dessen anschließende Umsetzung – ausweislich etwa der Qualifizierung als I-Item – offenbar ohne die einer derart rechtsstaats- und grundrechtsrelevanten Gesetzgebung angemessene Öffentlichkeitsbeteiligung erfolgen sollte.

* * *