Bundesverfassungsgericht weist Verfassungsbeschwerde gegen polizeigesetzliche Quellen-TKÜ in Baden-Württemberg ab

26.07.2021

BVerfG, Beschluss vom 8. Juni 2021, Az. 1 BvR 2771/18. Kommentar und Standpunkt des BDK-Landesvorsitzenden Steffen Mayer.

Über einfache Antworten, Dual Use und die digitale Veränderung

In unserer heutigen, weiterhin zunehmend digitaler werdenden Welt gibt es manchmal (ich meine immer öfter) keine einfachen Antworten. In der Informationstechnik gibt es viele Dinge, die weder „gut“ noch „böse“ sind, sie lassen sich schlicht und ergreifend dual nutzen. Während eine Firma mit in Auftrag gegebenen Penetrationstests das eigene System auf Schwachstellen überprüfen kann und anschließend das System härtet, kann ein Hacker mit den gleichen Tools einen Angriff auf das System durchführen. Die Software kann dabei völlig identisch sein, der Unterschied in der Auswirkung mitunter existentiell. Auch das teilweise mystifizierte Darknet, ein abgeschotteter Teil des Netzes, das nicht einfach über einen normalen Browser zugänglich ist, ist weder per se „böse“ noch „gut“. Es lädt aufgrund seiner Konstruktion aber leider auch sehr herzlich Kriminelle ein und die Vielfalt an kriminellen Angeboten kennt hier in der Tat keine Grenzen.

Das Prinzip der Verschlüsselung ist ebenfalls vergleichbar einzuordnen. Während verschlüsselte Kommunikation beispielsweise für Bankgeschäfte oder die Übermittlung von Gesundheitsdaten an die Krankenkasse zur Abrechnung mehr als nur sinnvoll ist, kann Verschlüsselung auch dazu genutzt werden, um illegale Geschäfte zu verabreden oder abzuwickeln.

Die Strafprozessordnung und einige Polizeigesetze haben traditionell Regelungen getroffen, um Strafverfolgungsbehörden den Zugang zu Kommunikation zu ermöglichen – auch verdeckt. Einige Vorschriften sind sehr alt, denken wir beispielsweise an § 99 StPO, die Postbeschlagnahme, die es bereits in ähnlicher Form in der Strafprozeßordnung von 1877 gab. Demnach dürfen (verkürzt und bezogen auf den heutigen Gesetzestext) *„an den Beschuldigten gerichtete Postsendungen und Telegramme“* beschlagnahmt werden. Ich weiß nicht, wann Sie das letzte Mal ein Telegramm bekommen haben, ich kann mich jedenfalls nicht daran erinnern. Meine Versicherungen und Firmen bei denen ich Kunde bin, stellen nach und nach auf E-Mails um, das vermeidet Kosten und ist im Grunde genommen für Anbieter und Kunde bequemer. Es tut sich etwas in Sachen Kommunikation und das erstreckt sich natürlich auch auf das Privatleben. Auf meinem Smartphone sind mehrere Messengerdienste installiert, in der Familiengruppe werden auf kurzem Wege Nachrichten und Albernheiten ausgetauscht. Vorbei die Zeit, als die SMS Geld kostete.

Das Smartphone ist keine Erfindung der 90er und nicht selten hat man heute mehrere mobile Geräte mit eigenen SIM-Karten, also Anschlüssen in Gebrauch. Das Festnetz hingegen steht schon nicht mehr in jedem Haushalt, warum auch, das Handy ist ja in der Hosentasche oder liegt griffbereit auf dem Couchtisch. Mittels Telekommunikationsüberwachung war und ist es der Polizei erlaubt Kommunikation verdeckt zu überwachen. Im Übrigen benutzt das Bundesverfassungsgericht in seinem Beschluss den Begriff heimlich, der weder in der Strafprozessordnung, noch im Polizeigesetz benutzt wird. Ich lehne diesen Begriff ab. Die Kripo ermittelt in vielen Bereichen verdeckt – oder nutzen wir doch den konkreten Begriff aus § 54 Polizeigesetz Baden-Württemberg, den Paragraphen der im Blickpunkt des Bundesverfassungsgerichts stand: „Der Polizeivollzugsdienst kann *ohne Wissen der betroffenen Person*“ – ich denke das trifft es besser und hat zudem keine negative Konnotation, wie das Wort heimlich. Zudem ist das Wort zu nahe an dem Wort Geheimpolizei anzusiedeln und hiergegen verwehre ich mich entschieden.

Kommunikation verändert sich, genutzte Technik ändert sich, ist es dann nicht konkludent, dass sich auch polizeiliche Eingriffsmaßnahmen weiterentwickeln, also angepasst werden müssen an die Veränderungen unserer Zeit? Ich meine ja, unbedingt! Das ist eine Grundvoraussetzung in einem demokratischen Rechtsstaat. Stillstand ist hier Rückschritt und weit schlimmer noch, die Polizei wird zunehmend blinder und tauber im Bereich der Telekommunikationsüberwachung. Das FBI hat vor einigen Jahren zum Spannungsfeld zwischen notwendigen Eingriffsmaßnahmen der Vollzugsbehörden und der zunehmenden Verschlüsselung von Kommunikation den Begriff „going dark“ geprägt. Er bringt zum Ausdruck, dass Kommunikation, die aus präventivpolizeilichen oder strafprozessualen Gründen überwacht werden muss, zunehmend nicht mehr überwacht werden kann. Das ist ein echtes Praxisproblem. Ich habe übrigens schon bei anderen Gelegenheiten darauf hingewiesen, dass TKÜ-Maßnahmen keine verdeckten Maßnahmen sind, bei denen eine Sonderkommission oder noch schlimmer eine einzelne Ermittlerin der Kripo in ihrem Verfahren juhu schreit, denn sie sind personal- und zeitintensiv. Dies gerade auch mit Blick auf die zunehmenden Anzahl an Geräten, die konsequenterweise alle überwacht werden müssen, wenn man eine TKÜ schaltet, weil die Zielperson eben mehrere SIM-Karten im Einsatz hat.

Die Quellen-TKÜ

Ich denke es ist hilfreich zunächst das Bundeskriminalamt zu zitieren, um alle auf Ballhöhe zu bringen*: „Viele Kommunikationsprogramme nutzen standardmäßig eine Verschlüsselung ihrer Kommunikationsdaten und -inhalte, die ohne aktives Handeln des Nutzers im Hintergrund arbeitet. Diese Inhalte können in vielen Fällen durch die klassische Form der Telekommunikationsüberwachung nicht mehr ausgewertet werden. Dies lässt aber die notwendigen und gesetzlich zulässigen Maßnahmen der Telekommunikationsüberwachung (TKÜ) bei der Verfolgung schwerer Straftaten oder der Abwehr von Gefahren für hochwertige Rechtsgüter ins Leere laufen.*

Die Quellen-TKÜ ist eine besondere Form der TKÜ, die Kommunikation erfasst, bevor diese verschlüsselt wird oder nachdem diese entschlüsselt wurde bzw. die Entschlüsselung ermöglicht. Hierbei wird nur die Kommunikation erlangt, die auch durch eine „konventionelle“ TKÜ erlangt würden.“

Das ist ein guter Punkt, denn durch Technik und Nutzerverhalten sind uns vielfach die Hände gebunden, Verschlüsselung wird hier missbraucht und aus Sicht des BDK Baden-Württemberg muss ein Ausgleich geschaffen werden. Die Quellen-TKÜ ist hier ein Mittel, um im Wettlauf mit den Kriminellen wieder etwas aufschließen zu können. Dabei sind wir uns sehr bewusst, dass eine Quellen-TKÜ deutlich aufwendiger ist, als eine klassische TKÜ-Maßnahme. Und Erfolg kann nicht in jedem Fall garantiert werden, aber damit leben wir bei vielen Ermittlungsmaßnahmen. Auch bei der Wohnungsdurchsuchung geht man manchmal mit leeren Händen nach Hause. Die Quellen-TKÜ gehört dennoch in den polizeilichen Werkzeugkasten des Ermittlers. Eine Argumentation, dass diese bisher kaum oder gar nicht eingesetzt wurde, ist kein stichhaltiges Argument gegen dieses Einsatzmittel. Mit der Schaffung der präventivpolizeilichen Quellen-TKÜ in § 54 Absatz 2 PolG BW hat Baden-Württemberg zusammenfassend den richtigen Schritt getan. Die Quellen-TKÜ schafft im Ergebnis einen möglichen Ausgleich aus dem Dilemma zunehmend blind bzw. taub bei der TKÜ zu sein. Ein Mehr an Daten ist im Übrigen gar nicht die Zielrichtung, das möchte ich an dieser Stelle nochmal bekräftigen.

Wenn es das Telegramm nicht mehr gibt, sondern die verschlüsselte E-Mail die allseits neue Standardkommunikation wäre, ist es dann nicht konsequent, den Strafverfolgungsanspruch des Staates und den Schutz der Bürgerinnen und Bürger durch sinnvolle Rechtsanpassungen weiterhin zu gewährleisten? Ich denke Sie verzeihen mir die rhetorische Frage am Ende dieses Absatzes.

Alternativen zur Quellen-TKÜ

Festzustellen ist, dass in einer Demokratie im Spannungsfeld zwischen Sicherheit und Freiheit über Ermittlungsmaßnahmen fachlich diskutiert werden muss (möglichst nicht am Stammtisch, das bringt selten etwas). Denn auch hier gibt es, wie eingangs betont, keine einfachen Antworten. (Eine gleiche Diskussion muss es zum Thema Mindestdatenspeicherfrist – auch Vorratsdatenspeicherung bezeichnet – geben, aber das würde auch ein paar Seiten füllen.) Ist jetzt also das Ausnutzen von Schwachstellen oder gar sogenannter Zero Day Exploits, also Schwachstellen, die allgemein beim Hersteller noch gar nicht bekannt sind, für die noch keine Patches entwickelt wurden – also gegen die man sich quasi gar nicht wehren kann – in Ordnung? Insbesondere auch mit Blick auf die polizeiliche Nutzung einer solchen Zero Day Sicherheitslücke ohne, dass diese Kenntnis in der Folge eine Hinweispflicht o.ä. gegenüber dem betroffenen Softwareanbieter auslöst? Man könnte auch fragen, heiligt der Zweck die Mittel? Das ist in der Tat eine Frage, die man diskutieren muss. Mit dem Beschuss des Bundesverfassungsgerichts gab es nunmehr einige juristische Hinweise speziell zu dieser Fragestellung. Eng mit der Diskussion verknüpft, muss die Frage nach wirkungsvollen Alternativen gestellt werden.

Was ist also mit echten Alternativen? Grundsätzlich könnte man Softwareanbieter und Hersteller dazu verpflichten, bei verschlüsselter Kommunikation eine Eintrittstüre für Sicherheitsbehörden einzubauen – direkt in die Software oder auf dem Wege der Datenübermittlung, die nach entsprechender rechtlicher Prüfung wie einem richterlichen Beschluss, die Kommunikation der Polizei unverschlüsselt zur Verfügung stellen. Aber hier stoßen wir auf verschiedene Problemstellungen. Erstens sitzen viele der Anbieter in den USA oder zumindest außerhalb von Deutschland. Ein Interesse deutsches Recht bei der Erstellung ihrer Produkte zu beachten ist doch eher untergeordnet zu sehen. Zudem ist das Interesse an der Mitwirkung im deutschen Strafprozess oder bei der Gefahrenabwehr nur bedingt vorhanden. Zweitens hat ein Wettbewerbsvorteil, wer als Firma zusichert, dass er selbst nicht in verschlüsselte Kommunikation Einblick nehmen kann. Drittens würde eine solche Hintertür natürlich auch wieder Anreize schaffen, diese durch Dritte (Randnotiz: jedenfalls nicht den deutschen Staat) missbräuchlich zu verwenden, es zumindest zu versuchen. Viertens hat Deutschland bisher im Gegensatz zu den USA keine diesbezüglichen Vorstöße unternommen und diese sind m. E. derzeit nicht zu erwarten. Sichere Kommunikation und „gute“ Verschlüsselung sind im Gegensatz dazu sogar geförderte Ziele und daran haben wir als BDK BW überhaupt nichts auszusetzen. Zuletzt kann ich mir nicht vorstellen, dass die Akzeptanz der Kritiker bei dieser Vorgehensweise deutlich höher liegen würde, als bei der Quellen-TKÜ.

Eine weitere Alternative bestünde technisch gesehen in dem Versuch die verschlüsselte Kommunikation zu entschlüsseln, man muss aber nicht Kryptographie studiert haben, um diesen Punkt sehr schnell als unrealistisch abzuhaken. Es ist ja auch nicht so, dass man das nicht versucht hätte. Die Verschlüsselung ist in aller Regel viel zu gut und die Aufwände übersteigen die Ressourcen (gerne vertiefen: Brute-Force-Angriffe auf Passwörter und deren Zeitdauer abhängig von der Schlüssellänge). Was allerdings passiert, wenn Quantenrechner praxistauglich werden, wird sich zeigen, im Übrigen bedauerlicherweise auch für die „gute“ Verschlüsselung.

Aktuell sehen wir zusammenfassend keine greifbaren Alternativen zu einer Quellen-TKÜ, wenngleich diese Maßnahmen ebenfalls nicht als befriedigend zu bewerten sind, weil sie einen hohen Aufwand bedeuten und wir diese Maßnahme gar nicht flächendeckend einsetzen können. Wie jede Maßnahme muss sie überlegt und abgewogen und schließlich in Einklang mit Recht und Gesetz umgesetzt werden.

Zur vertiefenden inhaltlichen Auseinandersetzung des Beschlusses verweise ich auf Pressemitteilung und Volltext, Quelle Bundesverfassungsgericht, sowie die Besprechung auf der Seite Rechtslupe (letzter Link in der Übersicht). An dieser Stelle übernehme ich abschließend nur die Leitsätze aus der Entscheidung.

Leitsätze des Beschlusses des Ersten Senats vom 8. Juni 2021:

1 - Art. 10 Abs. 1 GG begründet neben einem Abwehrrecht einen Auftrag an den Staat, vor dem Zugriff privater Dritter auf die dem Fernmeldegeheimnis unterfallende Kommunikation zu schützen (Bestätigung von BVerfGE 106, 28 <37>).

2 - a) Die grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verpflichtet den Staat, zum Schutz der Systeme vor Angriffen durch Dritte beizutragen.

2 - b) Die grundrechtliche Schutzpflicht des Staates verlangt auch eine Regelung zur grundrechtskonformen Auflösung des Zielkonflikts zwischen dem Schutz informationstechnischer Systeme vor Angriffen Dritter mittels unbekannter Sicherheitslücken einerseits und der Offenhaltung solcher Lücken zur Ermöglichung einer der Gefahrenabwehr dienenden Quellen-Telekommunikationsüberwachung andererseits.

3 - Für die Geltendmachung einer gesetzgeberischen Schutzpflichtverletzung bestehen spezifische Darlegungslasten. Eine solche Verfassungsbeschwerde muss den gesetzlichen Regelungszusammenhang insgesamt erfassen. Dazu gehört, dass die einschlägigen Regelungen des beanstandeten Normkomplexes jedenfalls in Grundzügen dargestellt werden und begründet wird, warum diese verfassungsrechtlich unzureichend schützen.

4 - Richtet sich eine Verfassungsbeschwerde unmittelbar gegen ein Gesetz, kann nach dem Grundsatz der Subsidiarität auch die Erhebung einer verwaltungsgerichtlichen Feststellungs- oder Unterlassungsklage zu den zuvor zu ergreifenden Rechtsbehelfen gehören. Das ist nicht erforderlich, wenn die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft und von einer vorausgegangenen fachgerichtlichen Prüfung keine verbesserte Entscheidungsgrundlage zu erwarten wäre (stRspr). Dies gilt auch im Falle der Rüge einer gesetzgeberischen Schutzpflichtverletzung.

Externe Links:

- Polizeigesetz Baden-Württemberg, § 54
- BVerfG, Pressemitteilung № 62/2021 vom 21. Juli 2021: „Unzulässige Verfassungsbeschwerde zum Umgang der Polizeibehörden mit Sicherheitslücken in informationstechnischen Systemen“ und Entscheidung vom 8. Juni 2021, Az. 1 BvR 2771/18
- PM IM BW, 21.07.2021
- Bundeskriminalamt zum Thema Quellen-TKÜ und Onlinedurchsuchung
- Rechtslupe, 22.07.2021: „Zero-Day-Exploits – und der Staatstrojaner“