REPORTER OHNE GRENZEN
FÜR INFORMATIONSFREIHEIT

Stellungnahme zur

Einführung der Quellen-TKÜ und Online-Durchsuchung

auf Grundlage der Formulierungshilfe zum Gesetzesentwurf DS 18/11272 („Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze“) vom 15. Mai 2017

31. Mai 2017

Eingereicht von:

Reporter ohne Grenzen e.V.
Friedrichstraße 231
10969 Berlin

Ansprechpartner:

Daniel Moßbrucker (Referent für Internetfreiheit)
030 – 6098 9533 - 23
dm@reporter-ohne-grenzen.de (PGP: F09F78A3)

Gegenstand der Stellungnahme:

Diese Stellungnahme bezieht sich auf die Pläne der Bundesregierung, mittels der Formulierungshilfe der Ausschuss-Drucksache 18(6)334 den Einsatz von Staatstrojanern in Ermittlungsverfahren zur Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und Online-Durchsuchung zu legalisieren. Reporter ohne Grenzen konzentriert sich im Folgenden ausschließlich auf Schutzrechte für Journalisten und Informanten vor solchen Maßnahmen. Sind andere Regelungen in dieser Stellungnahme nicht ausdrücklich erwähnt, so ist dies keineswegs dahingehend zu verstehen, dass sie als unbedenklich anzusehen wären.

Ergebnis der Stellungnahme

Die Stellungnahme zeigt, dass die geplante Einführung der Quellen-Telekommunikationsüberwachung den engen Grenzen des Bundesverfassungsgerichtes in mehreren Punkten widerspricht. Die Koppelung der Quellen-TKÜ an § 160a StPO ist abzulehnen, weil die Quellen-TKÜ in der Ausprägung des § 100a Abs. 1 S. 1 und 2 StPO-nF über eine klassische Telekommunikationsüberwachung hinausgeht, weil auch auf „gespeicherte Inhalte“ zugegriffen werden soll. Die Maßnahme ist demzufolge auch am Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme zu messen und damit gegenüber Journalisten unzulässig. Eine Quellen-TKÜ muss damit unter § 100d Abs. 5 StPO-nF aufgeführt werden. Folgerichtig ist, dass Journalisten und Redaktionen von einer Online-Durchsuchung ausgenommen werden sollen. Hier erweist sich die Regelung des § 100d Abs. 5 StPO-nF jedoch als unscharf formuliert und bedarf der sprachlichen Überarbeitung. Wünschenswert wäre zudem, Journalisten generell von verdeckten Ermittlungsmaßnahmen auszunehmen und den § 160a StPO so zu überarbeiten, wie es die SPD in ihrem 2012 eingebrachten „Gesetz zur Stärkung der Pressefreiheit“ (DS 17/9144) selbst gefordert und begründet hat.

1 Quellen-TKÜ

Gemäß § 100a Abs. 1 S. 2 und 3 StPO-nF sollen Ermittler zukünftig Trojaner („technische Mittel“) auf die Endgeräte von Verdächtigen aufspielen können, um Kommunikation abzufangen, bevor sie verschlüsselt wird. Dies gilt sowohl für laufende Kommunikation wie auch für „gespeicherte Inhalte und Umstände der Kommunikation“, wenn diese „während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können“.

1.1 Problem

Die Formulierungshilfe führt in § 100d Abs. 5 StPO-nF einen Schutz für Journalisten ein, der sich allerdings nur auf Maßnahmen des § 100b StPO-nF (Online-Durchsuchung) sowie § 100c StPO-nF (Akustische Wohnraumüberwachung) bezieht. Der Schutz von Journalisten vor einer Quellen-TKÜ richtet sich wie bei einer „normalen“ Telekommunikationsüberwachung gem. § 100a Abs. 1 S. 1 StPO nach § 160a StPO, das den Schutz von Berufsgeheimnisträgern bei verdeckten Ermittlungsmaßnahmen regelt.

In der analogen Welt genießen Journalisten gem. § 53 Abs. 1 S. 1 Nr. 5 StPO ein Zeugnisverweigerungsrecht, das von einem Durchsuchungs- und Beschlagnahmeverbot gem. § 97 Abs. 5 StPO flankiert wird. Diese Rechte können als *absolute* Schutzrechte betrachtet werden, da die in § 53 Abs. 2 S. 2 StPO genannte Schranke in § 53 Abs. 2 S. 3 StPO durch eine Schranken-Schranke aufgehoben wird, sofern eine Zeugenaussage

> „zur Offenbarung der Person des Verfassers oder Einsenders von Beiträgen und Unterlagen oder des sonstigen Informanten oder der ihm im Hinblick auf seine Tätigkeit nach Absatz 1 Satz 1 Nr. 5 gemachten Mitteilungen oder deren Inhalts führen würde“.

Diese Regelung setzt die ständige Rechtsprechung des Bundesverfassungsgerichts um, das eine besondere Stellung von Journalisten im Ermittlungsverfahren mit der konstituierenden Bedeutung einer freien Presse für die Demokratie begründet.

> „Deshalb gehört zur Pressefreiheit auch ein gewisser Schutz des Vertrauensverhältnisses zwischen Presse und privaten Informanten. Er ist unentbehrlich, da die Presse auf private Mitteilungen nicht verzichten kann, diese Informationsquelle aber nur dann ergiebig fließt, wenn sich der Informant grundsätzlich darauf verlassen kann, daß das "Redaktionsgeheimnis" gewahrt bleibt.“ (BVerfG 20, 162)

Entscheidend ist ein „grundsätzliches“ Vertrauen in die Medien. Zweifel an den Schutzmöglichkeiten von Journalisten für ihre Informanten können dazu führen, dass eine Kontaktaufnahme unterbleibt, obwohl die Preisgabe von Informationen im öffentlichen Interesse gewesen wäre.

Dieses „grundsätzliche“ Vertrauen setzt § 160a StPO, der den Schutz von Journalisten vor einer Quellen-TKÜ sichern soll, gerade nicht um. Stattdessen werden Journalisten – im Gegensatz übrigens zu anderen Berufsgeheimnisträgern wie Geistlichen – bei verdeckten (und damit heute vor allem digitalen) Ermittlungsmaßnahmen *relativ* geschützt. § 160a Abs. 2 verlangt eine Einzelfallprüfung, ob im konkreten Fall das Strafverfolgungsinteresse des Staates die Schwere des Eingriffes in die Pressefreiheit überwiegt. Dies erzeugt bereits heute eine Unsicherheit sowohl bei

Journalisten wie auch ihren Informanten, ob Kommunikation vor verdeckten Ermittlungsmaßnahmen wie einer Handyüberwachung sicher ist. An diese Verhältnismäßigkeitsprüfung soll nun auch eine Quellen-TKÜ i.S.d. § 100a Abs. 1 S. 2 und 3 StPO-nF gekoppelt werden. Dies überschreitet klar die Grenzen, die das Bundesverfassungsgericht in ständiger Rechtsprechung zur Weite des Informantenschutzes und dem Einsatz von Staatstrojanern gesetzt.

Es soll möglich werden, Trojaner auf die Endgeräte von Journalisten zu spielen, um verschlüsselte Kommunikation abzufangen. Verschlüsselung ist in der digitalen Welt zum zentralen Mittel geworden, um sich vor Überwachung zu schützen. Reporter ohne Grenzen registriert in seiner Zusammenarbeit mit Journalisten aus Deutschland und anderen Teilen der Welt, dass mittlerweile eine Angst vor einer allumfassenden Überwachung entstanden ist – ausgelöst durch Berichte über weltweite NSA-BND-Spähaktivitäten oder die gezielte Überwachung von Journalisten durch deutsche Geheimdienste [1] . Verschlüsselung ist hier die technische Möglichkeit, verloren gegangenes „grundsätzliches" Vertrauen in Schutzmöglichkeiten von Journalisten wiederherzustellen. 2015 veröffentlichte der UN-Sonderberichterstatter für das Recht auf Meinungsfreiheit, David Kaye, einen Bericht[2], wonach Verschlüsselung in der digitalen Welt dem Individuum erst ermöglicht, sein Menschenrecht auf Kommunikationsfreiheit wahrzunehmen und daher besonders geschützt werden muss.

Journalisten waren stets vorsichtig und haben sich und ihre Informanten bestmöglich vor Überwachung geschützt, etwa indem möglichst viele Gespräche persönlich geführt werden. Gleichwohl implementieren Redaktionen mittlerweile anonyme und stark verschlüsselte „digitale Briefkästen" für Informanten und bieten verschlüsselte Email-Konten an, um Informanten einen bestmöglichen Schutz zu gewährleisten. Trojaner konterkarieren diese Bemühungen im Kern. Anders formuliert: Wenn Journalisten mittels Trojanern in einer Quellen-TKÜ überwacht werden können, gibt es keinen einzigen Kommunikationskanal mehr, in dem Journalisten und Informanten mit letzter rechtlicher Sicherheit vertraut kommunizieren können. Heute bietet zumindest Verschlüsselung die technische Möglichkeit, das rechtliche Defizit des § 160a StPO auszugleichen und sich einen sicheren Kanal zu eröffnen. Es ist in vielen Fällen nicht möglich, auf nicht-digitale Kommunikation zu wechseln und insofern unverständlich, warum mit einem Staatstrojaner zum Beispiel Informationen abgegriffen werden können, über die ein Journalist vor Gericht kein Zeugnis ablegen müsste.

Diese verfassungsrechtlichen Bedenken werden verstärkt, weil die Pläne der Bundesregierung zentrale Vorgaben des Bundesverfassungsgerichtes zum Einsatz von Staatstrojanern nicht umsetzen. Die Koppelung von § 100a Abs. 1 S. 2 und 3 StPO-nF an §160a StPO suggeriert, dass eine Quellen-TKÜ letztlich dieselbe grundrechtliche Eingriffsintensität wie eine „traditionelle" Maßnahme gem. Abs. 1 S. 1 StPO darstellt. Diese Auffassung steht im klaren Widerspruch zur

---

[1] vgl. Der Spiegel v. 25.02.2017, Vorabmeldung online unter: http://www.spiegel.de/politik/deutschland/bnd-bespitzelte-offenbar-auslaendische-journalisten-a-1136134.html, zuletzt aufgerufen am 31.05.2017.

[2] vgl. A/HR/C/29/32, online unter: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc, zuletzt aufgerufen am 31.05.2017.

Rechtsprechung des Bundesverfassungsgerichtes. Während eine Telekommunikationsüberwachung gem. § 100a Abs. 1 S. 1 StPO „nur“ am Grundrecht des Fernmeldegeheimnisses nach Art. 10 GG zu messen ist, kommt bei einer Quellen-TKÜ zusätzlich eine Abwägung mit dem Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme hinzu. Dieses leitete das Bundesverfassungsgericht 2008 in seinem Urteil[3] zum Einsatz von Staatstrojanern im nordrhein-westfälischen Verfassungsgesetz aus Art. 1 Abs. 1 GG i. V. m. Art. 2 Abs. 1 GG ab. Dieses „Computer-Grundrecht“ ist nur dann nicht maßgeblich für eine Quellen-TKÜ, wenn ausschließlich „laufende Kommunikation“ erfasst wird. Darüber setzt sich die Formulierungshilfe jedoch hinweg, da eine Quellen-TKÜ auch „gespeicherte Inhalte und Umstände der Kommunikation“ erfassen können soll. Hier ist die Grenze zur Online-Durchsuchung eindeutig überschritten.

Erschwerend kommt hinzu, dass der gesamte Entwurf keine technischen Vorgaben und rechtlichen Verfahren benennt, um die Maßnahme rechtsstaatlich abzusichern. Es ist also den Staatsanwaltschaften, Gerichten und polizeilichen Ermittlern selbst überlassen, welche Technologie sie einsetzen. Auch hier ignoriert die Bundesregierung damit die strengen Vorgaben aus Karlsruhe, das gefordert hatte, dass „technische Vorkehrungen und rechtliche Vorgaben“[4] die Beschränkung auf „laufende Kommunikation“ sicherzustellen haben.

In der Konsequenz erweisen sich die geplanten Schutzrechte von Journalisten vor einer Quellen-TKÜ als unzureichend und bedürfen der dringenden Überarbeitung. § 160a StPO stellt schon heute keinen zufriedenstellenden Schutz vor Überwachungsmaßnahmen dar, doch die geplanten grundrechtlichen Eingriffe sind weitergehender als eine Telekommunikationsüberwachung gem. § 100a Abs. 1 S. 1 StPO und gehen über den Anwendungsbereich des § 160a StPO noch hinaus.

1.2 Lösung

Es bieten sich demzufolge zwei Möglichkeiten, diese Schwachstelle der Formulierungshilfe zu beseitigen:

1. Medienangehörige werden dem absoluten Schutz vor verdeckten Ermittlungsmaßnahmen des § 160a Abs. 1 StPO unterstellt. Verwiesen sei hierzu auf den Gesetzesentwurf der SPD-Fraktion vom 27. März 2012 (DS 17/0144), in der diese Anpassung vorgesehen war. Darin heißt es: „Die durch [das relative Beweiserhebungs- und Beschlagnahmeverbot] verursachte Verunsicherung über den Schutz der vertraulichen Kommunikation hemmt den Informationsfluss, der gerade für den investigativen Journalismus von großer Bedeutung ist. Aus diesem Grund sollen Journalisten den absoluten Schutz des § 160a StPO genießen, soweit das Zeugnisverweigerungsrecht reicht.“ Diese Anpassung wäre wünschenswert, da Journalisten dadurch auch vor einer Telekommunikationsüberwachung gem. § 100a Abs. 1 S. 1 StPO und der Vorratsdatenspeicherung geschützt wären.

[3] vgl. BVerfGE 120, 274.

[4] vgl. BVerfGE 120, 274, Rn. 190.

2. Maßnahmen des §100a Abs. 1 S. 2 und 3 StPO-nF (Quellen-TKÜ) werden in § 100d Abs. 5 StPO-nF aufgenommen, sodass eine Quellen-TKÜ bei Journalisten, sofern sie sich auf § 53 Abs. 1 S. 1 Nr. 5 StPO beziehen, unzulässig ist.

1.3 Änderungsvorschlag

1. § 160a StPO wird wie folgt geändert:
   a) In Absatz 1 Satz 1 werden die Wörter „oder Nummer“ durch ein Komma ersetzt und werden nach der Angabe „4“ die Wörter „oder Nummer 5“ eingefügt.
   b) In Absatz 2 Satz 1 wird die Angabe „oder Nr. 5“ gestrichen.

oder

2. § 100d Abs. 5 StPO-nF wird wie folgt neu gefasst: „Gegenüber den in § 53 Abs. 1 Satz 1 genannten Personen sind Maßnahmen nach den §§ 100a Abs. 1 S. 1, 100b und 100c unzulässig; ergibt sich während oder nach Durchführung der Maßnahme, dass eine solche Person von der Maßnahme betroffen ist, gilt Absatz 2 entsprechend.“

2 Online-Durchsuchung

Gemäß § 100b StPO-nF soll mittels eines Trojaners („technische Mittel“) auch ohne Wissen des Betroffenen in sein informationstechnisches System eingegriffen werden können, um Daten daraus zu erheben.

2.1 Problem

Die Bundesregierung beabsichtigt, Journalisten und andere Berufsgeheimnisträger von einer Online-Durchsuchung prinzipiell auszunehmen. Maßgebend soll dazu § 100d Abs. 5 StPO-nF sein, wonach „in den Fällen des § 53“ Maßnahmen nach §§ 100b und 100c StPO-nF unzulässig sein sollen. In der Gesetzesbegründung heißt es dazu:

> „Absatz 5 enthält die bisher in § 100c Absatz 6 StPO g.F. enthaltene Regelung zum Schutz von Zeugnisverweigerungsberechtigten, insbesondere Berufsgeheimnisträgern. Diese wird auf Maßnahmen der Online-Durchsuchung erstreckt.“

Dieses Ziel ist wünschenswert. Jedoch ist die Regelung rechtstechnisch verfehlt, da § 53 StPO keine Fälle, sondern Personengruppen benennt. Es ist also unklar, ob Journalisten umfassend vor einer Online-Durchsuchung geschützt sind oder nur in den Fällen, in denen sie sich tatsächlich auf eine Zeugnisverweigerung gemäß § 53 StPO berufen können. Die Verhältnismäßigkeitsprüfung des § 53 Abs. 2 S. 2 StPO eröffnet hier eine gefährliche Schutzlücke, weil Endgeräte zunächst einmal mit einem Trojaner infiltriert werden könnten, um festzustellen, ob die hier gespeicherten Informationen unter den Schutzbereich des § 53 Abs. 1 S. 1 Nr. 5 StPO fallen oder nicht. Damit

wäre ein Eingriff wieder möglich, den § 100d Abs. 5 StPO-nF aber eigentlich prinzipiell ausschließen will.

Ferner offenbart die Regelung, dass ein umfassender Schutz für das Vertrauensverhältnis von Journalisten und Informanten nur dann möglich ist, wenn auch Informanten eigene Schutzrechte genießen und nicht nur auf die Schutzmöglichkeiten der Journalisten angewiesen sind. Mittels einer Online-Durchsuchung auf dem Endgerät des Informanten kann schließlich gespeicherte Kommunikation ausgelesen werden, an welcher der Journalist beteiligt gewesen ist.

2.2 Lösung

Es bieten sich demzufolge zwei Möglichkeiten, diese Schwachstelle der Formulierungshilfe zu beseitigen:

1. Der § 100d Abs. 5 StPO-nF muss dahingehend angepasst werden, dass er nicht auf „Fälle des § 53“ StPO abzielt, sondern auf betroffene Personen, die sich auf § 53 StPO berufen können. Hier muss entgegen § 53 Abs. 2 S. 2 StPO ein absolutes Beweiserhebungsverbot gelten.
2. Die Bundesregierung sollte Whistleblower vor Strafverfolgung schützen mit einem Whistleblower-Schutzgesetz. Erinnert sei an den Koalitionsvertrag von Union und SPD, in der für die aktuelle Legislaturperiode ein solches Gesetz vorgesehen war.

2.3 Änderungsvorschlag

1. § 100d Abs. 5 StPO-nF wird wie folgt neu gefasst: „Gegenüber den in § 53 Abs. 1 Satz 1 genannten Personen sind Maßnahmen nach den §§ 100a Abs. 1 S. 1, 100b und 100c unzulässig; ergibt sich während oder nach Durchführung der Maßnahme, dass eine solche Person von der Maßnahme betroffen ist, gilt Absatz 2 entsprechend.“