Hacken zur Strafverfolgung? Gefahren und Grenzen der strafprozessualen Online-Durchsuchung

verfassungsblog.de/hacken-zur-strafverfolgung-gefahren-und-grenzen-der-strafprozessualen-online-durchsuchung/

Tobias Singelnstein So 2 Jul 2017

So 2 Jul 2017

Zum Abschluss der Legislaturperiode hat die Große Koalition mit der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und der Online-Durchsuchung zwei äußerst eingriffsintensive heimliche Ermittlungsmaßnahmen zum Zweck der Strafverfolgung eingeführt. Die beiden Regelungen wurden im Eilverfahren und ohne jegliche Debatte in ein bereits laufendes Gesetzgebungsverfahren eingebracht und treten voraussichtlich noch im Juli dieses Jahres in Kraft. Sie gestatten massive Grundrechtseingriffe und bedeuten einen weiteren wesentlichen Schritt hin zur Vergeheimdienstlichung des Strafverfahrens.

Die beiden neuen StPO-Befugnisse basieren auf einer heimlichen Infizierung informationstechnischer Systeme – z.B. Computer, Tablet, Handy – mittels einer Schadsoftware, weshalb sie zusammen auch unter dem Begriff „Staatstrojaner“ firmieren. Der Unterschied zwischen beiden Maßnahmen besteht alleine im Umfang der Daten, auf die zugegriffen wird. Bei der Quellen-TKÜ darf grundsätzlich nur laufende Telekommunikation an dem betroffenen Endgerät ausgeleitet werden – beispielsweise Skype-Telefonate oder Messenger-Nachrichten, bevor diese für die Übertragung verschlüsselt werden. Bei der Online-Durchsuchung hingegen ist im Prinzip ein Zugriff auf alle auf dem jeweiligen System gespeicherten Daten gestattet.

Quellen-TKÜ und Online-Durchsuchung in der StPO

Der Grund für die Differenzierung in zwei Maßnahmen ist ein verfassungsrechtlicher: Das Bundesverfassungsgericht hatte in seiner Entscheidung zur geheimdienstlichen Online-Durchsuchung 2008 aus dem Allgemeinen Persönlichkeitsrecht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entwickelt. Dieses neue Grundrecht soll gerade der zentralen Bedeutung Rechnung tragen, die moderne Informationstechnik heute im Leben vieler Bürger und damit auch für deren Persönlichkeitsrechte spielt. Das Gericht hat die spezifischen Gefahren, die mit einer heimlichen Infiltration solcher Systeme verbunden sind, als besonders schwerwiegend eingeschätzt und dementsprechend hohe Anforderungen an eine Rechtfertigung von Eingriffen in den Schutzbereich errichtet. Zugleich hat es für die Quellen-TKÜ ausdrücklich eine Hintertür offengelassen: Wenn technisch und rechtlich sichergestellt sei, dass eine solche Infiltration ausschließlich laufende Telekommunikation betrifft, so sei die Maßnahme nur am Fernmeldegeheimnis aus Art. 10 GG zu messen, das geringere Anforderungen an eine Rechtfertigung stellt.

Diese Differenzierung hat der Gesetzgeber mit seinem Regelungskonzept aufgegriffen. Die Quellen-TKÜ wurde eingeführt durch eine Ergänzung der bisherigen Regelung zur allgemeinen Telekommunikationsüberwachung in § 100a StPO. Nach § 100a Abs. 1 S. 2, 3 StPO n.F. ist die Überwachung nun auch durch eine heimliche Infiltration zulässig, wenn dies notwendig ist, „um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen.“ Hierfür gelten im Grundsatz die gleichen Anforderungen wie bei der normalen Telekommunikationsüberwachung. Anders als der sicherheitsbehördliche Diskurs dies suggeriert, betrifft die Maßnahme allerdings nicht nur verschlüsselte Messenger wie zum Beispiel WhatsApp oder Telegram. Vielmehr lassen sich auf diesem Weg vielfältige Daten überwachen, die per Internet übertragen werden. Hierzu gehört also auch das Surfen, Chatten und Austauschen von Dateien – wenn man den Telekommunikationsbegriff weit versteht sogar die Speicherung von Daten in Cloud-Speichern.

Die Online-Durchsuchung hat demgegenüber eine eigenständige Regelung im neuen § 100b StPO erfahren. Die Voraussetzungen für den Eingriff sind eng an die des großen Lauschangriffs in § 100c StPO angelehnt. Liegen

diese vor, so darf nach § 100b Abs. 1 StPO n.F. mit „technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden“. Diese Legaldefinition macht – ebenso wie bereits der Name der Maßnahme („Durchsuchung“) – deutlich, dass § 100b StPO n.F. alleine dazu ermächtigt, bereits bestehende, gespeicherte Daten für die Verwendung im Strafverfahren zu sichern. Dies stellt die Befugnis klar, indem sie die Formulierung „daraus erhoben“ verwendet; sie bezieht sich damit nicht auf eine Erhebung „mittels“ des informationstechnischen Systems.

Daraus folgt einerseits, dass im Rahmen der Maßnahme nicht Daten produziert und gespeichert werden dürfen. Vielmehr beschränkt sich die Befugnis auf die passive Kenntnisnahme. Daher ist eine – technisch ohne weiteres mögliche – Nutzung von Mikrofon und Kamera des gekaperten informationstechnischen Systems ebenso unzulässig wie eine Veränderung der dort gespeicherten Daten. Beides würde sich nicht mehr als Durchsuchung des jeweiligen Systems darstellen, sondern als dessen manipulative Nutzung. Andererseits muss sich die Maßnahme – wie jede andere Ermittlungsmaßnahme auch – auf solche Daten beschränken, die für das jeweils in Rede stehende Strafverfahren als Beweismittel in Betracht kommen. Ebenso wie bei der normalen Durchsuchung ist daher eine umfassende Untersuchung des informationstechnischen Systems grundsätzlich unzulässig. Vielmehr darf nur auf solche Datenbestände zugegriffen werden, bei denen nach dem bisherigen Ermittlungsstand davon ausgegangen werden kann, dass sich dort beweiserhebliche Informationen finden.

Gefahren und Nutzen der neuen Befugnisse

Quellen-TKÜ und Online-Durchsuchung, die das BKAG bereits zu präventiv-polizeilichen Zwecken gestattet, sind sowohl fachlich als auch gesellschaftspolitisch hoch umstritten. Im Vordergrund stehen dabei folgende Probleme:

1. Bei der Online-Durchsuchung handelt es sich nun um den schwersten Grundrechtseingriff zu Ermittlungszwecken, den die StPO kennt. Die Maßnahme geht insofern über den Großen Lauschangriff hinaus, als die Durchsicht eines informationstechnischen Systems angesichts der dort gespeicherten Vielfalt von Daten potentiell einen umfassenden Überblick über das gesamte Leben des Betroffenen ermöglicht. Sie versetzt also in die Lage, eigentlich verbotene, umfassende Persönlichkeitsprofile zu erstellen. Darüber hinaus handelt es sich um einen heimlichen Eingriff, gegen den der Betroffene erst im Nachhinein mit den Mitteln des Rechtsschutzes vorgehen kann, was die Eingriffsintensität nach der Rechtsprechung des BVerfG erheblich vertieft.

2. Anders als bei anderen strafprozessualen Ermittlungsmaßnahmen erfordern Quellen-TKÜ und Online-Durchsuchung einen manipulativen Eingriff in das Beweismittel selbst. Um heimlichen Zugriff auf das System zu erlangen, muss verändernd in selbiges eingegriffen werden, anstatt dieses – wie sonst auch im Bereich der IT-Forensik üblich – im Ist-Zustand zu sichern. Dies zusammengenommen handelt es sich um Maßnahmen, deren konkrete Umsetzung durch die Polizei im Nachhinein nur sehr schwer nachzuvollziehen und zu kontrollieren ist.

3. Wegen der Maßnahme hat der Staat nunmehr ein strukturelles Interesse daran, IT-Sicherheitslücken nicht zu schließen, sondern offen zu halten, da diese zum Aufbringen der Schadsoftware auf das informationstechnische System benötigt werden.

Diesen Gesichtspunkten steht auf der anderen Seite der Nutzen gegenüber, den solche geheimdienstlichen Methoden für die Strafverfolgungsbehörden haben können. Insbesondere die Polizei hatte die Notwendigkeit dessen stets damit begründet, andernfalls nicht auf verschlüsselte Kommunikation zugreifen zu können. Abgesehen davon, dass es sich hierbei um ein technisches Defizit der Strafverfolgungsbehörden handelt – rechtlich wäre der Zugriff auf verschlüsselte Telekommunikation bereits zuvor ohne weiteres möglich gewesen – wirft diese Argumentation die Frage auf, ob es denn tatsächlich so sein muss und soll, dass der Staat die Befugnis hat, heimlich auf alle Bereiche des menschlichen Lebens zugreifen zu können. Oder ob es nicht vielmehr auch außerhalb des Kernbereichs privater Lebensgestaltung Räume geben sollte, in denen der Einzelne geschützt und ohne Eingriffe kommunizieren kann.

Diese Frage wird umso bedeutsamer, wenn man sich vor Augen führt, dass die Notwendigkeit des heimlichen

Zugriffs auf informationstechnische Systeme keineswegs so drängend ist, wie die Polizei dies in der Debatte darstellt. Erstens kann auf einen Großteil der in Rede stehenden Daten durchaus auch bereits heute zugegriffen werden – nämlich in Form einer „offenen“ Durchsuchung (§§ 102 ff. StPO) und Beschlagnahme (§§ 94 ff. StPO). Im Rahmen dieser Maßnahmen ist es ohne weiteres möglich, Datenträger sicherzustellen und auszuwerten. Zweitens führt der technische Fortschritt nicht zu einem strukturellen Nachteil für die Sicherheitsbehörden, wie es häufig heißt, sondern vervielfacht vielmehr deren Möglichkeiten. Auch wenn ein Teil der Kommunikation verschlüsselt ist, können die Strafverfolgungsbehörden heute doch auf viel mehr Daten zugreifen als in der Vergangenheit und stehen Ihnen somit Informationen aus nahezu allen Lebensbereichen zur Verfügung. Drittens schließlich ist durchaus fraglich, inwiefern Quellen-TKÜ und Online-Durchsuchung in der Praxis tatsächlich Verbesserung für die Ermittler bringen werden. Die technische Umsetzung der neuen Befugnisse für die Vielzahl verschiedener Geräte und Systeme, die sich ständig verändern, ist äußerst anspruchsvoll. Es wird daher zu jeder Zeit informationstechnische Systeme geben, die für die Sicherheitsbehörden nicht zugänglich sind. Wer sich informiert, kann sich also auch weiterhin einem Zugriff der Strafverfolgungsbehörden entziehen.

Verfassungsrechtlicher Ausblick

Eine andere Frage ist es, inwiefern dieser rechtstatsächlichen und rechtspolitischen Erwägungen Eingang in die verfassungsrechtliche Debatte finden werden. Man kann mit Sicherheit davon ausgehen, dass sich das Bundesverfassungsgericht mit den neuen Befugnissen auseinandersetzen müssen wird – erste Verfassungsbeschwerden sind bereits angekündigt. Dabei dürften vor allem folgende Aspekte eine Rolle spielen:

1. In seiner Entscheidung 2008 hatte das Gericht für die präventiv ausgerichtete Online-Durchsuchung festgelegt, dass dieser äußerst intensive Eingriff nur zulässig sein kann, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen, das heißt für „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“. Diesen Maßstab gilt es nun auf den Bereich der Strafverfolgung zu übertragen und also die Frage zu beantworten, wann das Interesse der Allgemeinheit an der Strafverfolgung ein solches Gewicht erlangt, dass diese sehr hohe Hürde erreicht wird. In diesem Zusammenhang spielen erstens Nutzen und Gefahren der Maßnahmen, wie sie vorstehend erläutert wurden, eine Rolle. Zweitens wird sich das Gericht fragen müssen, ob die durchaus üppigen Straftatenkataloge in § 100a Abs. 2 und § 100b Abs. 2 StPO n.F. – die keineswegs nur sehr schwere Straftaten erfassen – eine solche Begrenzung zu leisten vermögen.

2. Nach § 100b Abs. 3 StPO n.F. richtet sich die Online-Durchsuchung nicht nur gegen Beschuldigte, sondern kann auch gegen unverdächtige Dritte eingesetzt werden, wenn „aufgrund bestimmter Tatsachen anzunehmen ist“, dass der Beschuldigte deren informationstechnische Systeme nutzt. Wer die Praxis kennt weiß, dass diese Voraussetzung in der Praxis faktisch keine Rolle spielt. Angesichts dessen wird sich das Gericht mit der Frage auseinandersetzen müssen, ob dies den strengen Anforderungen an eine Eingriffsrechtfertigung gerecht wird.

3. Mit der bisherigen Rechtsprechung des Verfassungsgerichts unvereinbar ist die Regelung in § 100a Abs. 1 S. 3 StPO, wonach bei der Quellen-TKÜ nicht nur auf laufende, sondern auch auf gespeicherte Kommunikation zugegriffen werden darf, wenn diese „während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können“. Die Beschränkung auf laufende Kommunikation in Abgrenzung zu gespeicherten Daten markiert nach der Entscheidung zur Online-Durchsuchung gerade die Grenze zwischen Art. 10 Abs. 1 GG und dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Die Vorschrift ist daher nicht mehr nur am Fernmeldegeheimnis, sondern am deutlich strengeren Computer-Grundrecht zu messen ist, dessen Anforderungen die Voraussetzungen des § 100a StPO nicht genügen.

4. Wegen des manipulativen Charakters des Eingriffs in das informationstechnische System und damit in das Beweismittel selbst kommt der Transparenz und den Möglichkeiten der (nachträglichen) Kontrolle des polizeilichen Handelns herausragende Bedeutung zu. Dies gilt nicht alleine im Hinblick auf Art. 19 IV GG und die Möglichkeit des

nachträglichen Rechtsschutzes. Vielmehr hängt auch die Zuverlässigkeit der so generierten Beweismittel und damit deren Beweiswert stark davon ab, inwiefern das polizeiliche Handeln nachvollzogen und kontrolliert werden kann. Die insofern bestehenden Protokollierungspflichten in § 100a Abs. 6 StPO n.F. – die über § 100b Abs. 4 StPO auch für die Online-Durchsuchung Geltung erlangen – werden dem nicht gerecht. Danach müssen jeweils nur die Metadaten des Einsatzes des staatlichen Trojaners dokumentiert werden. Welche Schritte die Ermittler auf dem infizierten System unternommen haben, bleibt hingegen offen, obwohl dies gerade wesentlich ist, um im Nachhinein die Rechtmäßigkeit des konkreten Vorgehens überprüfen zu können.

5. Schließlich stellt sich die Frage, ob die Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung den Anforderungen der Verfassung genügen. Bekanntlich sind Eingriffe in den Kernbereich im Hinblick auf Art. 1 Abs. 1 GG generell unzulässig und nicht zu rechtfertigen. Staatliche Eingriffsmaßnahmen müssen dies schon auf der Erhebungsebene berücksichtigen – und zwar umso stärker, je verletzungsgeneigter sie hinsichtlich des Kernbereichs sind. Nach dem neuen § 100d Abs. 1 StPO sollen die Maßnahmen allerdings nur dann generell unzulässig sein, wenn zu erwarten ist, dass „allein“ Erkenntnisse aus dem Kernbereich erlangt werden, was praktisch kaum der Fall sein dürfte. Lediglich bei der Online-Durchsuchung ist nach § 100d Abs. 3 StPO n.F. zudem „soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden“. Abgesehen von der mangelnden Klarheit dieser Formulierung darf bezweifelt werden, dass die Regelung in der Praxis zu einer wirksamen Begrenzung führt. Dies ist nicht überzeugend, da Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme solchen in Art. 13 GG gleichen. Dementsprechend läge es nahe, für die Online-Durchsuchung ähnliche Grenzen vorzusehen wie für den Großen Lauschangriff. Diesbezüglich regelt § 100d Abs. 4 StPO n.F., dass die Maßnahme nur angeordnet werden darf, „soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden“. Eine solche Prüfung vor Anordnung der Maßnahmen auch bei der Online-Durchsuchung würde den verfassungsrechtlichen Anforderungen gerecht und ist der nun beschlossenen wachsweichen Forderung nach technischen Sicherungen – deren praktische Realisierbarkeit mehr als fraglich ist – vorzuziehen.

SUGGESTED CITATION Singelnstein, Tobias: *Hacken zur Strafverfolgung? Gefahren und Grenzen der strafprozessualen Online-Durchsuchung, VerfBlog,* 2017/7/02, http://verfassungsblog.de/hacken-zur-strafverfolgung-gefahren-und-grenzen-der-strafprozessualen-online-durchsuchung/, DOI: https://dx.doi.org/10.17176/20170702-133023.