

**Gabriel Übleis**

**17.07.2017**

**Gabriel Übleis nimmt zu dem Entwurf wie folgt Stellung:**

## **Stellungnahme im Begutachtungsverfahren zum Ministerialentwurf des Justizministeriums, Strafprozessrechtsänderungsgesetz 2017 (325/ME)**

Sehr geehrte Damen und Herren,

Bereits 2013, im Zuge des "Demokratie-Enquete zur Stärkung der Demokratie in Österreich", haben sich alle Parteien für mehr Bürgerbeteiligung ausgesprochen. Demnach werde ich genau das tun, was man von mir wünscht. Ich beteilige mich aktive an der Diskussion, indem ich folgende Punkte des geplanten Überwachungspaketes kritisiere und entschärft wissen möchte:

### **Bundestrojaner**

Ich bin gegen die Legalisierung einer staatlichen Spionagesoftware, einem sogenannten Bundestrojaner, in § 135a StPO-E zur Überwachung verschlüsselter Nachrichtenübertragung.

Durch die Einführung staatlicher Spionagesoftware investiert der Staat gezielt in die Unsicherheit der häufigsten Betriebssysteme. Um einen Bundestrojaner auf dem Zielgerät zu installieren, müssen Sicherheitslücken geheim- und damit offengehalten werden, da eine unbemerkte Installation sonst nicht zu bewerkstelligen ist. Die desaströsen Folgen von staatlicher Spionagesoftware wurden eindrücklich mit dem weltweiten Angriff des "WannaCry"-Erpressungstrojaners demonstriert. Diese global agierende Schadsoftware, die Krankenhäuser, Bahnhöfe und tausende Firmen lahmgelegt hat, wurde erst dadurch ermöglicht, dass die NSA eine ihr bekannte Sicherheitslücke in Microsoft Windows für ihre Spionagesoftware geheim gehalten hatte, anstatt durch Meldung an Microsoft für deren Behebung zu sorgen [1]. Derartige Sicherheitslücken werden zumeist für viel Geld auf zweifelhaften Märkten gehandelt. Einerseits werden diese Märkte bei Ankauf der Lücken durch

österreichische Steuergelder finanziert, andererseits wird die gesamte IT-Sicherheit unterminiert, da die Bundesregierung Interesse daran haben muss, dass (durch die Überwachungssoftware ausgenutzte) kritische Sicherheitslücken in den gängigsten Betriebssystemen nicht geschlossen werden, um die Funktionalität dieser Software zu gewährleisten.

Insbesondere durch die Ermöglichung der Ferninstallation der Software im Entwurf wird in den Fortbestand der gefährlichsten Art von Sicherheitslücken für die Ferninfektion eines Rechners investiert. Somit ist jeder Mensch, der einen Personal-Computer, ein Smartphone, ein Tablet oder eine Spielekonsole verwendet, von dem in Begutachtung gegebenen Gesetz unmittelbar betroffen [2]. Diese und andere Argumente haben 2016 zu einer Kehrtwende von Justizminister Brandstetter geführt, als dieser den bislang letzten Versuch staatliche Spionagesoftware zu legalisieren fallen gelassen hat. [3]

Eine von BMI und BMJ eingesetzte interministerielle Expertenarbeitsgruppe [4] unter der Leitung von Univ.-Prof. Dr. Bernd-Christian Funk hat im Jahr 2008 festgestellt, dass „Online-Durchsuchungen“ von Computersystemen mittels „Trojanern“ nach der österreichischen Rechtsordnung (insb. StPO, SPG und MBG) nicht zulässig sind, da die erforderlichen Ermächtigungen *de lege lata* nicht vorliegen. Eine Abgrenzung der "Online-Durchsuchung" der Dateien auf dem Computer (Fotos, Tagebücher, etc) von der "Online-Überwachung" der getätigten Kommunikation (WhatsApp, Skype) ist jedoch technisch nicht möglich. Um auch nur einen Bruchteil der gängigsten Messenger erfassen zu können, muss die staatliche Überwachungssoftware einen kompletten Überblick über alle Dateien des Zielsystems haben. Durch die Erläuterungen des Gesetzes wird darüber hinaus klar, dass sogar der "Aufruf von Websites" unter die Überwachung fallen soll.

Die Überprüfung der Software soll laut dem Entwurf durch die Datenschutzbehörde erfolgen. Dies erscheint angesichts der Tatsache, dass der Datenschutzbehörde kein einziger Techniker angehört, und diese seit Jahren chronisch unterfinanziert ist, wie das bewusste Ausschalten von Kontrolle, was zum nächsten Überwachungsskandal geradezu einlädt.

Aus technischer Sicht kommen berechtigte Zweifel auf, ob der Einsatz der geplanten Überwachungssoftware überhaupt geeignet ist, das legitime Ziel der Bekämpfung und Verfolgung von Terrorismus und (organisierter) schwerer Kriminalität zu verfolgen. Der aktuelle Stand der Technik lässt eine treffsichere, schadlose, unbemerkte und zuverlässige Anwendung gar nicht mit ausreichender Sicherheit zu. Technische Zwischenfälle im Rahmen des Einsatzes könnten leicht zu einem Fehlschlagen oder Bekanntwerden der Ermittlungen führen.

Einerseits werden auch nur halbwegs technisch versierte Benutzer des kompromittierten Computersystems die aufgespielte Schadsoftware erkennen und ihr Verhalten dementsprechend ändern. Andererseits ist es sehr wahrscheinlich, dass der Einsatz der Überwachungssoftware durch Anti-Viren-Software erkannt und unterdrückt wird. Kaspersky Lab gab in einer Stellungnahme bekannt, dass, wenn ein Staatstrojaner von einer Antivirus-Software erkannt wird, dieser daran gehindert wird, Überwachungsdaten nach außen zu leiten. Ein erhöhtes ausgehendes Datenaufkommen oder eine

unerklärt erhöhte CPU-Leistung kann auch von technisch nicht versierten Benutzern leicht selbst erkannt werden. Sollte der Betroffene die Überwachungssoftware entdecken, könnte er diese missbrauchen und den Ermittlern falsche Ergebnisse liefern (gezielte Beweismanipulation, Legen einer falschen Fährte). Durch diese falschen Ergebnisse wäre die Ermittlung im besten Fall nutzlos. Noch bedenklicher erscheint aber die Tatsache, dass fehlgeleitete Ermittlungen dazu führen können, dass Kriminelle vom tatsächlich geplanten Vorhaben ablenken und dieses in Ruhe verwirklichen können. Der Einsatz der Überwachungssoftware selbst wird somit zu einer erheblichen Gefahr für die

Wir haben bereits einen Text für Sie vorbereitet. Wenn Sie Ihre persönliche Kritik zum Ausdruck bringen möchten, können Sie hier Änderungen vornehmen. 326/ME Ihre Stellungnahme an das Bundesministerium für Inneres Themen: Videoüberwachung, Quick freeze

## **Vorratsdatenspeicherung für Videoüberwachung**

Ich bin gegen die Vernetzung von Videoüberwachung nach § 53 Abs. 5 SPG-E und gegen die Vorratsdatenspeicherung von Videoüberwachung für 2 Wochen mittels einfachem Bescheid nach § 93a SPG-E.

Ob Videoüberwachung überhaupt ein geeignetes Mittel ist, um Terroranschläge zu verhindern, muss bezweifelt werden. Schließlich wurde auch die gesamte Uferpromenade von Nizza mit Videokameras überwacht und der Anschlag dort konnte damit auch nicht verhindert werden. Großbritannien ist eines der am meisten überwachten Länder, trotzdem ist es in letzter Zeit von Anschlägen geplagt. Im Gegenteil: Videokameras können Terroristen sogar als Ansporn dienen. Schließlich zielen sie mit ihren Gräueltaten ja auf größtmögliche Verstörung der Bevölkerung und somit auf größtmögliche Sichtbarkeit ab.

Im Jänner wurde bekannt, dass die LPD Wien 15 von 17 Überwachungskameras abbauen ließ, weil die Kosten zu hoch waren und der Nutzen für die Verbrechensbekämpfung nicht erkennbar war.

## **Quick freeze**

Ich bin gegen die Neuauflage der Vorratsdatenspeicherung in Form von Quick Freeze nach § 99 Abs. 1a bis 1f TKG-E.

Auf Anordnung der Staatsanwaltschaft soll ein Telekombetreiber künftig wieder Vorratsdaten für bis zu ein Jahr speichern müssen. Somit kann diese Überwachungsmaßnahme eingesetzt werden noch bevor ein Gericht zugestimmt hat, da der Entwurf nach § 99 Abs. 1b TKG-E erst bei der Beauskunftung der Daten, aber nicht bei der Speicherung auf Vorrat eine gerichtliche Bewilligung vorsieht. Jedoch wird bereits durch die Speicherung, in Grundrechte eingegriffen, nicht erst durch die Beauskunftung.

Im Arbeitsprogramm der Regierung fand sich hier noch eine Pflicht, fälschlicherweise überwachte Personen beim Abschluss der Maßnahme über ihre Überwachung zu informieren. Diese Verpflichtung findet sich nicht im Entwurf, stattdessen kann der Betroffene offenbar lediglich ein

Auskunftsbegehren nach Datenschutzrecht stellen, was in keiner Weise ein Ersatz wäre.

Insgesamt stellt sich die Frage, ob eine Vorratsdatenspeicherung überhaupt effektiv ist. Eine entsprechende Evaluierung von EDRi (European Digital Rights) [5] zeigt, dass die Maßnahme viel kostet, aber wirkungslos ist. Aus den Ländern, die Vorratsdatenspeicherung einsetzen, sind keine Beispiele bekannt, dass diese zur Verhinderung oder Aufklärung von schweren Verbrechen oder Terroranschlägen beigetragen hätte.

325/ME Ihre Stellungnahme an das Bundesministerium für Justiz Themen:  
Bundestrojaner

## **Bundestrojaner**

Ich bin gegen die Legalisierung einer staatlichen Spionagesoftware, einem sogenannten Bundestrojaner, in § 135a StPO-E zur Überwachung verschlüsselter Nachrichtenübertragung.

Durch die Einführung staatlicher Spionagesoftware investiert der Staat gezielt in die Unsicherheit der häufigsten Betriebssysteme. Um einen Bundestrojaner auf dem Zielgerät zu installieren, müssen Sicherheitslücken geheim- und damit offengehalten werden, da eine unbemerkte Installation sonst nicht zu bewerkstelligen ist. Die desaströsen Folgen von staatlicher Spionagesoftware wurden eindrücklich mit dem weltweiten Angriff des "WannaCry"-Erpressungstrojaners demonstriert. Diese global agierende Schadsoftware, die Krankenhäuser, Bahnhöfe und tausende Firmen lahmgelegt hat, wurde erst dadurch ermöglicht, dass die NSA eine ihr bekannte Sicherheitslücke in Microsoft Windows für ihre Spionagesoftware geheim gehalten hatte, anstatt durch Meldung an Microsoft für deren Behebung zu sorgen [6]. Derartige Sicherheitslücken werden zumeist für viel Geld auf zweifelhaften Märkten gehandelt. Einerseits werden diese Märkte bei Ankauf der Lücken durch österreichische Steuergelder finanziert, andererseits wird die gesamte IT-Sicherheit unterminiert, da die Bundesregierung Interesse daran haben muss, dass (durch die Überwachungssoftware ausgenutzte) kritische Sicherheitslücken in den gängigsten Betriebssystemen nicht geschlossen werden, um die Funktionalität dieser Software zu gewährleisten.

Insbesondere durch die Ermöglichung der Ferninstallation der Software im Entwurf wird in den Fortbestand der gefährlichsten Art von Sicherheitslücken für die Ferninfektion eines Rechners investiert. Somit ist jeder Mensch, der einen Personal-Computer, ein Smartphone, ein Tablet oder eine Spielekonsole verwendet, von dem in Begutachtung gegebenen Gesetz unmittelbar betroffen [7]. Diese und andere Argumente haben 2016 zu einer Kehrtwende von Justizminister Brandstetter geführt, als dieser den bislang letzten Versuch staatliche Spionagesoftware zu legalisieren fallen gelassen hat. [8]

Eine von BMI und BMJ eingesetzte interministerielle Expertenarbeitsgruppe [9] unter der Leitung von Univ.-Prof. Dr. Bernd-Christian Funk hat im Jahr 2008 festgestellt, dass „Online-Durchsuchungen“ von Computersystemen mittels „Trojanern“ nach der österreichischen Rechtsordnung (insb. StPO, SPG und MBG) nicht zulässig sind, da die erforderlichen Ermächtigungen *de lege lata*

nicht vorliegen. Eine Abgrenzung der "Online-Durchsuchung" der Dateien auf dem Computer (Fotos, Tagebücher, etc) von der "Online-Überwachung" der getätigten Kommunikation (WhatsApp, Skype) ist jedoch technisch nicht möglich. Um auch nur einen Bruchteil der gängigsten Messenger erfassen zu können, muss die staatliche Überwachungssoftware einen kompletten Überblick über alle Dateien des Zielsystems haben. Durch die Erläuterungen des Gesetzes wird darüber hinaus klar, dass sogar der "Aufruf von Websites" unter die Überwachung fallen soll.

Die Überprüfung der Software soll laut dem Entwurf durch die Datenschutzbehörde erfolgen. Dies erscheint angesichts der Tatsache, dass der Datenschutzbehörde kein einziger Techniker angehört, und diese seit Jahren chronisch unterfinanziert ist, wie das bewusste Ausschalten von Kontrolle, was zum nächsten Überwachungsskandal geradezu einlädt.

Aus technischer Sicht kommen berechtigte Zweifel auf, ob der Einsatz der geplanten Überwachungssoftware überhaupt geeignet ist, das legitime Ziel der Bekämpfung und Verfolgung von Terrorismus und (organisierter) schwerer Kriminalität zu verfolgen. Der aktuelle Stand der Technik lässt eine treffsichere, schadlose, unbemerkte und zuverlässige Anwendung gar nicht mit ausreichender Sicherheit zu. Technische Zwischenfälle im Rahmen des Einsatzes könnten leicht zu einem Fehlschlagen oder Bekanntwerden der Ermittlungen führen.

Einerseits werden auch nur halbwegs technisch versierte Benutzer des kompromittierten Computersystems die aufgespielte Schadsoftware erkennen und ihr Verhalten dementsprechend ändern. Andererseits ist es sehr wahrscheinlich, dass der Einsatz der Überwachungssoftware durch Anti-Viren-Software erkannt und unterdrückt wird. Kaspersky Lab gab in einer Stellungnahme bekannt, dass, wenn ein Staatstrojaner von einer Antivirus-Software erkannt wird, dieser daran gehindert wird, Überwachungsdaten nach außen zu leiten. Ein erhöhtes ausgehendes Datenaufkommen oder eine unerklärt erhöhte CPU-Leistung kann auch von technisch nicht versierten Benutzern leicht selbst erkannt werden. Sollte der Betroffene die Überwachungssoftware entdecken, könnte er diese missbrauchen und den Ermittlern falsche Ergebnisse liefern (gezielte Beweismanipulation, Legen einer falschen Fährte). Durch diese falschen Ergebnisse wäre die Ermittlung im besten Fall nutzlos. Noch bedenklicher erscheint aber die Tatsache, dass fehlgeleitete Ermittlungen dazu führen können, dass Kriminelle vom tatsächlich geplanten Vorhaben ablenken und dieses in Ruhe verwirklichen können. Der Einsatz der Überwachungssoftware selbst wird somit zu einer erheblichen Gefahr für die öffentliche Sicherheit.

öffentliche Sicherheit.

Ich halte es für falsch, dass alle Österreicher unsicherer leben müssen, nur damit dadurch eine kleine Gruppe Verdächtiger besser überwacht werden kann. Dies hat mit Verhältnismäßigkeit nichts mehr zu tun. Opfern Sie bitte nicht die digitale Sicherheit aller Bürger für den zweifelhaften Versuch, einige wenige Straftaten zu verhindern. Bedenken Sie bitte auch, dass für Europa irgendwann wieder eine Zeit ohne Terroranschläge kommen wird. Diese Form

von Anlassgesetzgebung sieht vielleicht gegenwärtig gut aus, öffnet aber Tür und Tor für Missbrauch in der Zukunft.

Mit freundlichen Grüßen, Gabriel Übleis

[1] <http://www.spiegel.de/netzwelt/web/wannacry-die-lehren-aus-dem-cyberangriff-a-1147589.html>

[2] [https://epicenter.works/sites/default/files/epicenter\\_works\\_1pager\\_-\\_bundestrojaner.pdf](https://epicenter.works/sites/default/files/epicenter_works_1pager_-_bundestrojaner.pdf)

[3] <https://epicenter.works/thema/bundestrojaner>

[4] [https://epicenter.works/sites/default/files/1pager-legalitaet\\_bundestrojaner.pdf](https://epicenter.works/sites/default/files/1pager-legalitaet_bundestrojaner.pdf)

[5] <https://edri.org/data-retention-shadow-report/>

[6] <http://www.spiegel.de/netzwelt/web/wannacry-die-lehren-aus-dem-cyberangriff-a-1147589.html>

[7] [https://epicenter.works/sites/default/files/epicenter\\_works\\_1pager\\_-\\_bundestrojaner.pdf](https://epicenter.works/sites/default/files/epicenter_works_1pager_-_bundestrojaner.pdf)

[8] <https://epicenter.works/thema/bundestrojaner>

[9] [https://epicenter.works/sites/default/files/1pager-legalitaet\\_bundestrojaner.pdf](https://epicenter.works/sites/default/files/1pager-legalitaet_bundestrojaner.pdf)