Stellungnahme zum Ministerialentwurf betreffend eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 geändert wird (XXV. GP 325/ME)

Michael Preisach

Email: michael@preisach.at

21. August 2017

Inhaltsverzeichnis

Einleitung

In der heutigen Zeit basiert ein Gutteil unserer Kommunikation auf dem Internet. Wir halten Kontakt mit Freunden über WhatsApp, speichern die neuesten Fotos in der Google Cloud und nutzen Informationen, die und mittels Cloud Computing zur Verfügung gestellt werden. Das Internet ist damit eine Art digitales Zuhause geworden. Diese Gesetzesnovelle möchte nun einige Befugnisse der Rechtsdurchsetzung hin zu mehr Überwachung setzen. Dabei werden die Befugnisse nicht nur im Internet erweitert, sondern auch in der Überwachung im öffentlichen Raum. Dies birgt in meinen Augen einige Probleme, die ich im Folgenden erläutern möchte.

1. **Mehr Heu** bringt die Ausweitung der Überwachung. Sascha Lobo zeichnete in seiner Kolumne *Unsere Sicherheit ist eine Inszenierung* [1] ein Bild, das objektiv analysiert keine Erweiterung der Überwachungsbefugnisse begründet. Stattdessen sollten die Möglichkeiten der Polizei zur internationalen Terrorismusbekämpfung effektiv ausgeschöpft werden. Mir ist es bis jetzt nicht begreiflich, warum es keine effektive, EU-weite Zusammenarbeit der Strafverfolgungsbehörden gibt. Damit hätten laut Medienberichten einige der letzten Terroranschläge verhindert werden können.

2. **Veränderungen der Gesellschaft** werden mit der Zeit offensichtlich. Unsere gesellschaftliche Vielfalt wird nicht nur durch Hass, Anfeindungen und Ausländerfeindlichkeit bedroht. Unterbewusst möchte man in einem Staat mit stark ausgebauter Überwachung auch nicht auffallen und lieber mit dem Strom schwimmen. Eine gute Visualisierung dafür liefert der Kurzfilm *Wir Lieben Überwachung* [2] von Alexander Lehmann.

[1] `http://www.spiegel.de/netzwelt/web/islamistischer-terror-in-europa-unsere-sicherheit\-ist-eine-inszenierung-a-1150015.html`

[2] `https://www.youtube.com/watch?v=qGvZveB1osw`

3. **Missbrauch** durch den Staat muss unterbunden werden. Daher ist es sinnvoll neben zusätzlichen Überwachungsmaßnahmen auch den Rechtsschutz zu verbessern. Zwar werden im der Novelle die Befugnisse des Rechtsschutzbeauftragten erweitert. Es ist allerdings nicht geplant, das Personal dafür zu vergrößern.

4. **Objektive Legislative** wird benötigt, um sinnvolle und effektive Gesetze zu entwickeln, die auch die Rechte jedes Einzelnen unserer Gesellschaft schützt, ohne dabei die Sicherheit hintanstellen zu müssen. Hierfür wurde von `epicenter.works` ein Handbuch [3] entwickelt, das helfen kann dem Ziel objektiv verbesserter Gesetzgebung näher zu kommen.

WFA Überwachung verschlüsselter Kommunikationsverkehre

In dieser Novelle wird die Überwachung verschlüsselter Telekommunikationsverkehre eingeführt. Der Einsatz solcher Software, im Folgenden *Bundestrojaner* genannt, birgt einige Probleme, die zwar juristisch sehr einfach zu lösen sind, aber technisch nicht umsetzbar sind.

Ich nehme zuerst an, dass ein Team von Entwicklern einen Bundestrojaner entwickeln möchte. Die folgenden technischen und organisatorischen Probleme gilt es hierfür zu lösen:

1. **Support für alle Betriebssysteme**: Ein Bundestrojaner muss grundsätzlich alle oder zumindest die gängigsten Betriebssysteme unterstützen. Dafür sind neben Windows Linux und MacOS auch Android und iOS von essentieller Bedeutung. Allerdings ist es bei den mobilen Betriebssystemen, speziell iOS mittlerweile sehr schwierig geworden ohne die Erlaubnis von Apple Software zu installieren und damit dann Messenger dieses Telefons abzuhören.

2. **Schwachstellen der gängigen Betriebssysteme finden**: Eine weitere Hürde ist das Finden von Schwachstellen. Selbst gute Sicherheitsforscher sind nicht immer in der Lage eine Sicherheitslücke zu finden. Daher wird es kaum möglich sein die Lücken in einem Forschungsteam ohne externe Hilfe aufzuspüren.

3. **Schwachstellen extern zukaufen**: Die externe Anschaffung von Sicherheitslücken birgt mehrere Probleme. Einerseits sind die Kosten teilweise schon sehr hoch; Apple zahlt mittlerweile für iOS Sicherheitslücken mehrere 100.000 Euro. Zum Anderen fördert der Staat damit auch einen illegalen Schwarzmarkt für Sicherheitslücken und bricht damit implizit das eigene Recht.

4. **Schwachstellen offen halten**: Hat man für den Bundestrojaner nun eine Sicherheitslücke gefunden, hegt man auch großes Interesse, dass die Lücke in möglichst vielen Endgeräten offen bleibt. Egal, ob das mit oder ohne Hilfe des Herstellers passiert, es werden die Systeme der eigenen Bürger damit wissentlich verwundbar gemacht. Es ist nämlich davon auszugehen, dass diese Lücke auch von anderen Interessensgruppen, speziell für Erpressungssoftware eingesetzt wird. Der Fall *WannaCry* gibt dafür ein sehr gutes Beispiel ab.

[3] `https://epicenter.works/sites/default/files/heat_1.1_0_0.pdf`

Die hier genannten Probleme gelten generisch für alle Varianten von Trojanersoftware und Gesetzen. Das bedeutet auch, dass die deutschen und die amerikanischen Ermittlungsbehörden diese Probleme lösen müssen. Da es nicht möglich ist, jeden Punkt moralisch korrekt und technisch vollständig zu lösen, müssen hier alle Staaten, die Bundestrojaner einsetzen, in irgend einer Form faule Kompromisse eingehen.

Im Weiteren nehme ich nun an, dass die Polizei einen solchen Trojaner besitzt und einsetzen kann. Weiters gilt die Annahme, dass diese Software auch für das Zielsystem funktioniert. Hier steht die Technik vor dem nächsten Problem: Üblicherweise wird für die Installation nämlich ein Administratorzugang benötigt. Da das ohne Nachricht an den Benutzer passieren soll, muss die genutzte Schwachstelle einen solchen Zugang mit sich bringen. Solche Schwachstellen verändern das System meist sehr stark. Diese wesentlichen Änderungen und die Tatsache, dass mittels Adminrechten grundsätzlich alles verändert werden kann, macht das Computersystem als Beweismittel unbrauchbar. Damit können auch auf dem System gefundene Daten nicht als Beweismittel verwendet werden, was die Prozessführung gegen den Beschuldigten meiner Auffassung nach signifikant erschweren kann.

Abschließend ist in § 135a Abs 2 definiert, dass die Software nur dann eingesetzt werden kann, wenn sie auch wieder entfernt oder zumindest funktionsunfähig gemacht werden kann. Leider ist es technisch nicht beweisbar, dass sich eine Software deinstalliert hat. Daher kann nur der Nachweis erbracht werden, dass die Software funktionsunfähig ist.

In diesem Zusammenhang finde ich auch die finanziellen Auswirkungen für viel zu gering eingeschätzt. Mit den geplanten personellen und finanziellen Mitteln kann eine Organisation samt Infrastruktur. Die 4 Stellen, die den Bundestrojaner entwickeln sollen, werden für herausragende Sicherheitsforscher weit unter ihren Wert bezahlt. Eine externe Lösung wird aber wahrscheinlich den gesetzlichen Anforderungen nicht genügen. Zumindest wird es nicht möglich sein den gesamten Quellcode der zugekauften Software einzusehen. Schließlich müssen, wie zuvor bemerkt, auch die Sicherheitslücken gefunden oder zugekauft werden. Diese Kosten wurden in der bisherigen Schätzung noch gar nicht berücksichtigt. Daher gehe ich davon aus, dass das Projekt in der anberaumten Zeit mindestens das Doppelte kostet, sofern in der geplanten Zeit ein funktionsfähiger, den Gesetzen entsprechender Bundestrojaner zur Verfügung stehen soll.

Bemerkungen zu den einzelnen Bestimmungen

Zu Z 4 (§ 76a Abs 1)

Es ist mir nicht ersichtlich, was mit der Erweiterung der Stammdaten um den PUK-Code bezweckt werden soll. Der PUK-Code dient einzig dem Entsperren oder Neusetzen des PIN-Codes. Der PIN hingegen schützt nur die auf der SIM gespeicherten Daten. Das können Kontakte und Kurznachrichten sein. Zusätzlich kann das Telefon zum Entsperren der SIM auffordern, bevor diese benützt werden kann.

Allerdings wird der Speicher der SIM-Karte heute kaum bis gar nicht mehr verwendet, da einerseits der Speicher sehr klein ist und andererseits die allermeisten Telefone über Cloud-Dienste von Google, Microsoft oder Apple gesichert werden. Es gibt also keine verbreitete Anwendung mehr, die den PUK unumgänglich erfordert. Aus diesem Grund

ist es mir nicht ersichtlich, warum die Aufnahme des PUK-Codes in die Stammdaten notwendig ist.

In den Erläuterungen zu dieser Änderung wird erwähnt, dass die Erlangung des PUKs bisher nur mittels Sicherstellung gem. § 110 StPO möglich ist und diese gegenüber dem Kommunikationsdienstanbieter begründet werden muss. Meiner Ansicht nach ist der PUK-Code als Passwort (also ein sensibles Datum) zu verstehen und daher auch in Zukunft nur in begründeten Fällen zu verlangen. Deshalb ist für mich diese Gesetzesänderung nur eine Herabsetzung der notwendigen Voraussetzungen. Die abnehmende Anwendung und der vertrauliche Grad der Information sind Grund für die Ablehnung dieser Änderung.

Zu Z 8 (§ 134 Z 2a)

Man kann mit IMSI-Catchern nicht nur die geografische Lage eines Mobilfunkgerätes feststellen, sondern auch die Kommunikation dieser Geräte abfangen und mitlesen. Ein IMSI-Catcher muss dazu das gesuchte Gerät in seine Zelle locken, indem es den besten Empfang in der Umgebung bereitstellt. Dazu muss es geografisch ebenfalls in der Nähe aufgestellt werden. Die einigermaßen kleinräumige und gezielte Überwachungsmethode ist grundsätzlich als positiv anzusehen.

Allerdings melden sich automatisch auch andere Geräte von Unbeteiligten bei der simulierten Basisstation an, da diese ja den besten Empfang bietet. Diese Endgeräte sind logischerweise unerwünscht und werden blockiert. Die Mobilfunk-Standards sehen allerdings keine Alternative zur Basisstation mit dem besten Empfang vor, weswegen diese Geräte oftmals ganz aus dem Netz fallen und nicht mehr kommunizieren können. Das bedeutet auch, dass sie keinen Notruf mehr absetzen können, wenn ein IMSI-Catcher in der nahen Umgebung eingesetzt wird.

Da Unbeteiligte technisch an einer potentiell wichtigen Kommunikation gehindert werden, ist der Einsatz von IMSI-Catchern abzulehnen. Zumindest wäre eine Zusatzbestimmung, die einerseits die geografisch begrenzte Ortung sowie den Schutz Unbeteiligter sicherstellt, in diesem Fall dringend notwendig. Da IMSI-Catcher eine weitaus größere Funktionalität, als die in der Norm beschriebene bieten, müsste auch hier eine klare Definition zur Anwendung formuliert bzw. Missbrauch unterbunden werden.

Zu Z 13 (§ 135 Abs 1)

Der Entfall des zweiten Halbsatzes stellt eine weitgehende Aufhebung des Briefgeheimnisses dar, da nun auch Briefe und Pakete Unbeteiligter geöffnet werden dürften. Der Bezug auf den Beschuldigten wurde indes völlig entfernt. Es wird in der Erläuterung darauf eingegangen, dass man im Zuge des Online-Handels auch Pakete von auf freiem Fuß befindlichen Beschuldigten beschlagnahmen möchte. Diesem Argument kann ich im Grunde folgen. Es ist jedoch nicht nachvollziehbar, dass auch die Definition des Beschuldigten aus der Norm fällt und nun jede mögliche Postsendung geöffnet werden kann, sofern sie nur irgendwie mit einer Tat mit mehr als einjähriger Haftstrafe in Verbindung gebracht werden kann. Der schwere Eingriff in die Privatsphäre und die potentiell sehr große Streuwirkung sind zwei wesentliche Gründe um diese Änderung abzulehnen.

Zu Z 16 (§ 135a)

Diese Norm enthält mehrere Punkte, die ich im folgenden kommentieren möchte:

- **Abs 1 Z 3:** Es wird hier vom Einsatz des Bundestrojaners gesprochen, wenn *die Aufklärung oder Verhinderung einer . . . begangenen oder geplanten Straftat ansonsten wesentlich erschwert wäre . . .*
  Das Installieren einer Software ist oftmals viel leichter oder zumindest kostengünstiger, als der Einsatz mehrere Polizisten für eine Observierung. Deshalb sehe ich in dieser Formulierung die Möglichkeit zum vielmaligen Einsatz des Bundestrojaners dort, wo Maßnahmen mit besserer Wahrung der Privatsphäre auch möglich gewesen wären.

- **Abs 1 Z 3b:** Diese Formulierung zielt offensichtlich auch auf die Verwendung von Cloud-Diensten. Allerdings wird hier die Möglichkeit eingeräumt, dass auf entfernten Rechnern auch der Bundestrojaner installiert werden darf. Dies ist wieder ein schwerer Eingriff in die Privatsphäre potentiell Unbeteiligter, da auch deren Computersysteme in diese Definition fallen können Daher eröffnet dies ein weites Feld des potentiellen Missbrauchs. Des Weiteren ist es meiner Meinung nach nicht sinnvoll, einen Trojaner auf Cloud-Diensten, wie Amazon oder Google zu installieren, da hier die Streuwirkung unvorhersehbar wäre.

- **Abs 3:** Bei Installation des Bundestrojaners mittels Eindringens in eine Wohnung sind *die Eigentums- und Persönlichkeitsrechte sämtlicher Betroffener soweit wie möglich zu wahren.* Hier ist nicht ersichtlich, wie die Einschätzung vorgenommen werden soll. Es sit offensichtlich eine subjektive Entscheidung der Behörden, was dieser Norm noch entspricht und was nicht. Diese mangelnde Definition verursacht Rechtsunsicherheit.

Zu Z 17 (§ 136 Abs 1a)

In Verbindung mit §135 Abs 3 Z 3b ist es also auch möglich Geräte akustisch abzuhören zu denen eine verdächtige Person Verbindung herstellen werde. Damit wäre es auch möglich Geräte abzuhören, dessen Besitzer mit der Straftat keinen Bezug haben, sondern "nur"mit dem Verdächtigen in Kontakt stehen. Wie schon bei den vorigen Punkten kann hier wieder in die Privatsphäre Unbeteiligter eingegriffen werden, ohne Konsequenzen zu befürchten. Dass die Eingriffsintensität einer rein akustischen Überwachung die gleiche sein soll wie die Überwachung von Telekommunikationsverkehre, wie in den Erläuterungen beschrieben, halte ich für nicht nachvollziehbar, da dies unterschiedliche judizierte Klassen sind. Daher sollten sie nicht gleichgestellt werden.

Zu Z 31 (§ 147 Abs 1 Z 3)

Hier müsste ein Verweis auf die akustische Fahrzeugüberwachung bestehen (§ 136 Abs 1a). In der aktuellen Fassung gibt es keine rechtliche Grundlage für den Rechtsschutzbeauftragten, rein akustische Überwachung zu kontrollieren, wenn Personen beteiligt sind, die die Aussage nicht verweigern dürften. Damit sind meiner Auffassung nach alle Zeugen und Unbeteiligten ohne Rechtsschutz einer akustischen Überwachung ausgeliefert. Diese Norm muss daher um eine entsprechende Formulierung erweitert werden.

Evaluierung der Novelle

Grundsätzlich ist es sehr positiv zu sehen, dass eine Evaluierungsphase für die gesamte Novelle bis 2022 durchgeführt wird.

Die Evaluierung sollte allerdings konkreter sein als *. . . die Bestimmungen entsprechen unter Wahrung des Grundrechtsschutzes dem Stand der Technik und den Erfordernissen der Ermittlungsbehörden*, denn dies ist eine tautologische Evaluierung. Vielmehr sollten einige Eckpunkte in diesem Gesetz evaluiert werden, mit der die Sinnhaftigkeit der Novelle gezeigt wird. Im Folgenden sind einige Evaluierungspunkte angeführt, die - mit einer sinnvollen Schwelle versehen - eine faktenbasierte Evaluierung ermöglicht:

- **Wie viele Betroffen wurden über ihre Überwachung informiert?**. Ein gutes Verhältnis von überwachten Personen zu informierten Personen nach Beendigung der Maßnahme belegt geringen Missbrauch durch die Ermittlungsbehörden.
- **Wie viele Personen wurden ohne Grund überwacht?** Da es mit dieser Novelle wesentlich mehr Möglichkeiten gibt unabsichtlich oder äls BeifangÜnbeteiligte zu überwachen, ist dies eine Zahl, die in Relation zu erfolgreich überwachten Personen die Güte von Maßnahmen angibt.
- **Wie viele der durchgeführten Fälle hat der Rechtsschutzbeauftragte tatsächlich überprüfen können?** Diese Zahl ist Relation zur Gesamtzahl der Fälle ein direktes Maß zur Rechtssicherheit der eingesetzten Maßnahmen.
- **Wie hoch ist die Auklärungsquote?** Da in der Motivation zu dieser Novelle beanstandet wird, dass die Aufklärung bestimmter Fälle gar nicht mehr möglich sei, sollte sich die Quote in Zukunft signifikant verbessern.
- **Wie oft werden Grundrechtseingriffe gebilligt? Welche Rechte werden eingeschränkt** Die Grundrechte werden nicht vollständig gewahrt, nachdem die Persönlichkeits- und Eigentumsrechte teilweise beschnitten werden. Um Missbrauch vorzubeugen, kann diese Statistik wesentlich helfen.

Sollten einige dieser Zahlen nicht zufriedenstellend sein, so ist meine Erwartungshaltung, dass spätestens nach Abschluss der Evaluierung diese Novelle aufgehoben wird. Es darf die folgende Novelle nur in Kraft treten, wenn die Probleme für alle Beteiligten gelöst sind.

Die Maßnahmen, die zur RL Unschuldsvermutung umgesetzt werden sollen, sind vertretbar und sollten als eigenständige Novelle umgesetzt werden.