HINTERGRUND

Das Überwachungspaket

Am Montag, dem 30. Jänner 2017 hat die Österreichische Bundesregierung ein neues Regierungsprogramm anlässlich des Neustarts der Koalition präsentiert. Darin ist ein umfassendes Paket[1] mit Überwachungsmaßnahmen und neuen Kompetenzen für die Sicherheitsbehörden enthalten. Ob dieses Überwachungspaket auch eine Erhöhung der Sicherheit für die Bevölkerung bringt, ist mehr als zweifelhaft. Eine Evaluierung bestehender Überwachungskompetenzen und -befugnisse sowie der eigentlichen Anforderungen hat die Regierung nicht vorgenommen. Das Paket setzt die Wunschliste von Innenminister Wolfgang Sobotka um und bringt noch nie da gewesene Einschränkungen des Rechts auf Privatsphäre und auf Datenschutz.

Aktueller Status (Stand 21. August 2017):

Am 10. Juli 2017 haben das Innen- und das Justizministerium ihre Vorschläge für Novellen zum Sicherheitspolizeigesetz[2] und zur Strafprozessordnung[3] in Begutachtung geschickt. Die darin enthaltenen Vorschläge sind schlimmer ausgefallen als erwartet. Hier unsere erste Einschätzung dazu: **Österreich steht vor beispielloser Ausweitung des Überwachungsstaats[4]**. Seit 13. Juli 2017 können Bürgerinnen und Bürger über www.überwachungspaket.at[5] Stellungnahmen zu den Gesetzesvorschlägen abgegeben. Diese werden auf der Website des Österreichischen Parlaments veröffentlicht. Das Justizministerium blockiert die Mails mit den Stellungnahmen[6] und ignoriert damit die Kritik Tausender Menschen.

Am 27. Juli 2017 geht SPÖ-Justizsprecher Hannes Jarolim mit der Aussage an die Öffentlichkeit, dass eine Zustimmung seiner Partei zum Überwachungspaket in der vorgeschlagenen Form "absolut nicht vorstellbar"[7] sei. Klubchef Andreas Schieder trägt das mit. Er sagt, die SPÖ werde einem Gesetz "mit einem Bundestrojaner" nicht zustimmen[8]. Sobotka und Brandstetter weisen die Kritik zurück. Angesichts der Vielzahl an Stellungnahmen und der immer lauter werdenden Stimmen von Expertinnen und Experten schreibt der Kurier bereits, das Sicherheitspaket liege "in Scherben"[9].

1 https://www.bka.gv.at/4-sicherheit-und-integration
2 https://parlament.gv.at/PAKT/VHG/XXV/ME/ME_00326/index.shtml
3 https://parlament.gv.at/PAKT/VHG/XXV/ME/ME_00325/index.shtml
4 https://epicenter.works/content/oesterreich-steht-vor-beispielloser-ausweitung-des-ueberwachungsstaats
5 https://www.xn--berwachungspaket-izb.at/
6 https://futurezone.at/netzpolitik/bundestrojaner-justizministerium-blockiert-protest-mails/275.961.619
7 https://futurezone.at/netzpolitik/spoe-zu-ueberwachungspaket-koennen-nicht-zustimmen/277.306.313
8 https://derstandard.at/2000061888663/Schieder-SPOe-wird-keinem-Bundestrojaner-zustimmen
9 https://kurier.at/politik/inland/nach-kritik-beschluss-von-sicherheitspaket-rueckt-in-weite-ferne/277.581.199

Während Bundeskanzler Kern, "Ruhe in der Diskussion"[10] fordert, drängt Justizminister Brandstetter weiterhin auf eine rasche Umsetzung. Allerdings kann er keine zufriedenstellenden Antworten auf die geäußerten Bedenken geben.[11]

Am 18. August 2017 hat epicenter.works zweie Stellungnahmen beim Parlament eingebracht:

1. Stellungnahme zur Novelle der Strafprozessordnung[12]
2. Stellungnahme zur Novelle des Sicherheitspolizeigesetzes (und anderer Gesetze)[13]

Neben epicenter.works haben sich auch der Oberste Gerichtshof, ISPA (Internet Service Providers Austria), die Sozialdemokratischen Rechtsanwältinnen und Rechtsanwälte, die Kinder- und Jugendanwaltschaft Tirol, die Universität Innsbruck, das Amt der Wiener Landesregierung, die Piratenpartei Österreichs, das Österreichische Rote Kreuz und über 9.000 weitere Personen und Organisationen kritisch zum Überwachungspaket geäußert.

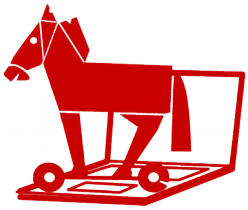
Hier findet sich eine Übersicht über alle bislang publizierten Stellungnahmen: https://überwachungspaket.at/konsultation/.

NAME	DATUM	BMI	BMJ	THEMEN	ORIGINALITÄT
Internet Service Providers Austria (ISPA)	18.8.2017				100
Hutchison Drei Austria GmbH	18.8.2017				100
Verein epicenter.works	18.8.2017				100
Amt der Niederösterreichischen Landesregierung	17.8.2017				100
Club Sozialdemokratischer Rechtsanwältinnen und R...	15.8.2017				100
Bundeskanzleramt	9.8.2017				100
Kinder- und Jugendanwaltschaft Tirol	4.8.2017				100
Land Salzburg	3.8.2017				100
Piratenpartei Österreichs	22.7.2017				100
Verband Alternativer Telekom-Netzbetreiber	18.8.2017				100
Kinder- und Jugendanwaltschaft Wien	18.8.2017				100
Oberstaatsanwaltschaft Linz	18.8.2017				100
Oberlandesgericht Wien	18.8.2017				100
Oberster Gerichtshof	18.8.2017				100
Amt der Wiener Landesregierung	17.8.2017				100
Österreichisches Rotes Kreuz	17.8.2017				100
BM f. Europa, Integration und Äußeres	17.8.2017				100
Wirtschaftskammer Österreich (WKÖ)	17.8.2017				100

10 https://futurezone.at/netzpolitik/sicherheitspaket-kern-fordert-ruhe-in-der-diskussion/277.526.505
11 Siehe Interview in der ZiB2 vom 28. Juli 2017: https://youtu.be/IDIvyYf-nmQ
12 https://epicenter.works/document/654
13 https://epicenter.works/document/653

Inhalte des Überwachungspakets:

Bundestrojaner



Ein Gesetzesvorschlag zur Legalisierung staatlicher Spionagesoftware wurde bereits 2016 vom Justizministerium vorgelegt. Aufgrund der massiven Kritik von juristischer und technischer Seite lenkte Justizminister Brandstetter damals ein und hat das Gesetzesvorhaben zurückgezogen. Im Überwachungspaket findet sich nun die Forderung der "Ermöglichung der Überwachung internetbasierter Kommunikation", hinter der sich zwangsläufig wieder ein Bundestrojaner verbirgt.

Neu und höchst bedenklich am aktuellen Vorschlag ist, dass in Zukunft Jeder Opfer des Bundestrojaners werden kann: Laut Gesetzesentwurf können die Sicherheitsbehörden in Computersysteme jeder Person, jeder Firma oder jedes Vereins einbrechen, von denen sie annehmen, dass diese mit Verdächtigen kommunizieren (§ 135a Abs 1 Z 3 lit b StPO-E). Die Ferninstallation eines Bundestrojaners über sogenanntes *"remote hacking"* ist ebenfalls vorgesehen. Um eine solche Ferninfektion durchzuführen, muss die Überwachungssoftware besonders gefährliche Sicherheitslücken in den gängigsten Betriebssystemen[14] verwenden. Offenbar darf ein Bundestrojaner auch dauerhafte Schäden auf dem Zielsystem anrichten, wenn er nach Beendigung der Maßnahme funktionsunfähig ist (Umkehrschluss aus § 135a Abs 2 Z 1 StPO-E) .

Medienberichten[15] zufolge sind insgesamt 14 Millionen Euro für den Kauf der Überwachungssoftware (inklusive Ankauf von Sicherheitslücken) sowie Schulung des Personals vorgesehen. Auch das Ausmaß der zu überwachenden Inhalte wurde massiv ausgeweitet: Aus den Erläuterungen geht hervor, dass sogar der "Inhalt von Webseiten"[16] überwacht werden soll.

Auf unserer Themenseite[17] zum Bundestrojaner finden sich weitere wichtigen Informationen und Materialien zu diesem Thema.

Status Mai: Anfang Mai berichten mehrere Medien über eine Aussage von SPÖ-Justizsprecher Hannes Jarolim[18], wonach der Bundestrojaner "sicher nicht" kommen wird. Dennoch sei eine Ausschreibung für eine Software geplant, mit der verschlüsselte Nachrichten abgehört werden können. Wie das zusammenpasst, erklärt Jarolim nicht. Wir fordern daher weiterhin ein generelles Verbot staatlicher Spionagesoftware[19].

Status Juni: Vizekanzler und Justizminister Brandstetter wird in mehreren Medien zitiert, dass er eine Software zur Überwachung von WhatsApp und andere Messengerdienste haben will. Er erklärt allerdings nicht, wie dies technisch umgesetzt werden soll. (Siehe etwa ORF Report vom 13. Juni

14 Youtube: „Cyberpeace statt Cyberwar! #WannaCry #WannaCrypt“ https://www.youtube.com/watch?v=St955HBD-7k
15 https://derstandard.at/2000061056685/Sicherheitspaket-Justiz-will-gesamten-Internetverkehr-Verdaechtiger-auslesen
16 https://derstandard.at/2000061056685/Bundestrojaner-Justiz-will-gesamten-Internetverkehr-von-Verdaechtigen-auslesen
17 https://epicenter.works/thema/bundestrojaner
18 https://futurezone.at/netzpolitik/spoe-justizsprecher-bundestrojaner-kommt-sicher-nicht/261.386.522
19 https://epicenter.works/content/staatliche-spionagesoftware-muss-verboten-werden

2017[20] oder in der ORF Pressestunde vom 18. Juni 2017.)[21] SPÖ-Justizsprecher Hannes Jarolim erklärt am 24. Juni 2017, dass sich die SPÖ eine Überwachung von internetbasierter Kommunikation nur vorstellen kann, wenn dafür kein Bundestrojaner eingesetzt wird[22]. Klubobmann Andreas Schieder bekräftigt das am 26. Juni 2017 in einer Pressekonferenz[23].

Warum mit einem Bundestrojaner oder anderen Cyberwaffen die gefährlichen Attacken wie "WannaCry"[24] in Zukunft noch häufiger stattfinden werden, erklärt dieses Video:

Einführung von Netzsperren

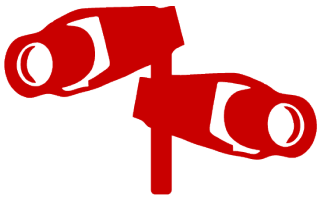
Gänzlich ohne Ankündigung im Arbeitsprogramm der Regierung oder öffentliche Debatte finden sich im Begutachtungsentwurf auch Netzsperren. Durch Nutzung einer Ausnahmeregelung in der EU-Netzneutralitätsverordnung soll es Providern ermöglicht werden, Pornographie, gewaltverherrlichende Darstellungen oder strafrechtlich relevante Urheberrechtsverletzungen im Internet nach eigenem Gutdünken zu sperren. Durch die Regelung bliebe es komplett dem Provider überlassen, ob, wann, wie, warum und wie lange solche Inhalte zensiert werden. Für betroffene Inhalteanbieter und Nutzer sind keinerlei Rechtsschutz oder Beschwerdemöglichkeit vorgesehen.

Das Fehlen jeglicher Diskussion im Vorfeld lässt darauf schließen, dass Telekomprovider oder ihre **Vorfeldorganisationen** wie die "Internetoffensive"[25] unter dem Vorwand einer Sicherheitsgesetzgebung diese Regelung ins Telekommunikationsgesetz schmuggeln wollen, um bestimmte, die Netzneutralität verletzende Produkte weiterhin betreiben zu können.

Es ist überdies sehr fragwürdig, ob der Regierungsvorschlag mit der EU-Verordnung zur Netzneutralität vereinbar ist. Zwar erlaubt die Verordnung Internetzugangsanbietern, Netzsperren durchzuführen, um nationales Recht, EU-Recht oder Gerichtsurteile umzusetzen. Das gilt aber nur "soweit und solange es erforderlich ist" (Art. 3 Abs. 3 Unterabs. 3 der Verordnung (EU) 2120/2015). Österreich könnte die Provider also dazu verpflichten, Netzsperren einzuführen, darf die Entscheidung aber nicht den Providern überlassen, wie dies der Regierungsvorschlag vorsieht. Eine einseitige Änderung der EU-Netzneutralitätsbestimmungen, die Österreich mit dem vorgeschlagenen § 17 (1a) des TKG zu erwirken versucht, widerspricht den Grundprinzipien des EU-Binnenmarkts.

20 https://youtu.be/S0yq3F0V5lU
21 https://youtu.be/uNOV57VV8oM
22 http://derstandard.at/2000059741301/Sicherheitspaket-SPOe-waere-ohne-Bundestrojaner-dabei
23 https://futurezone.at/netzpolitik/whatsapp-ueberwachung-spoe-strikt-gegen-bundestrojaner/271.886.323
24 http://www.spiegel.de/netzwelt/web/wannacry-die-lehren-aus-dem-cyberangriff-a-1147589.html
25 https://www.internetoffensive.at/

Vorratsdatenspeicherung für Videoüberwachung



Der Innenminister fordert eine "lückenlose Überwachung"[26] des öffentlichen Raums mit vernetzten Videokameras. Das Innenministerium soll Zugriff auf die Video- und Tonüberwachung aller öffentlichen und privaten Einrichtungen, denen ein öffentlicher Versorgungsauftrag zukommt, bekommen. Damit gibt es eine zentrale, staatliche Kontrolle aller öffentlichen Plätze und des dortigen Lebens. Für den Zugriff auf diese Daten braucht es keinen konkreten Verdacht, ähnlich wie im Polizeilichen Staatsschutzgesetz reicht als Begründung die Vorbeugung wahrscheinlicher Angriffe (§ 53 Abs 5 SPG-E). Die Sicherheitsbehörden können mittels eines einfachen Bescheids eine zweiwöchentliche Vorratsdatenspeicherung der gesamten Videoüberwachung eines Anbieters verlangen (§ 93a SPG-E).

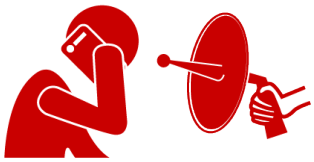
In einem nächsten Schritt könnte dieses Bildmaterial ausgewertet werden, um automatisch auffälliges Verhalten zu registrieren und mittels Gesichtserkennung einzelne Personen zu verfolgen. In Österreich gibt es bereits derartige Forschungsprojekte (siehe z.B. iObserve[27]). In der ORF ZiB1 vom 18. Juni 2017 zeigt Innenminister Sobotka Sympathien für eine mögliche Erweiterung in Richtung Gesichtserkennung. Zitat: *"Die Videografie wird in Zukunft noch viel größere Bedeutung haben als wie jetzt."*[28]

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. Im Gegenteil: Videokameras können Terroristen sogar als Ansporn dienen. Schließlich zielen sie mit ihren Gräueltaten ja auf die größtmögliche Verstörung der Bevölkerung. Im Jänner wurde bekannt, dass die LPD Wien 15 von 17 Überwachungskameras abbauen ließ[29], weil die Kosten zu hoch waren und der Nutzen für die Verbrechensbekämpfung nicht erkennbar war.

Status Juni: In der ORF-Sendung Report vom 13. Juni 2017 werden Details zu geplanten Intensivierung der Videoüberwachung bekannt[30]. Unter anderem ist eine Vorratsdatenspeicherung für das Videomaterial vorgesehen. In der aktuellen Stunde des Bundesrates am 22. Juni 2017 spricht Innenminister Sobotka sogar von einer einmonatigen Speicherfrist[31]. Das ist eine Verletzung unserer Grundrechte.[32]

26 https://derstandard.at/2000050236705/Sobotka-will-Lauschangriff-Fussfessel-fuer-Verdaechtige-und-vernetzte-Videokontrolle
27 http://www.kiras.at/fileadmin/dateien/allgemein/KIRAS%20Projekte-2009-06-NEU_1.pdf
28 https://youtu.be/N58V0hWKLDY
29 https://kurier.at/chronik/kameras-werden-wieder-abgebaut/243.543.107
30 https://www.youtube.com/watch?v=r-2GkCUGqAg
31 http://www.oe-journal.at/index_up.htm?http://www.oe-journal.at/Aktuelles/!2017/0617/W3/32206pkSobotka.htm
32 https://epicenter.works/content/ueberwachungspaket-vorratsdatenspeicherung-fuer-ueberwachungsvideos-geplant

Rechtsgrundlage für IMSI-Catcher



Ebenfalls ohne Debatte wird nun der Einsatz von IMSI-Catchern geregelt. Diese Geräte verhalten sich gegenüber dem Mobiltelefon wie eine Funkzelle (Basisstation). So ist es möglich, Handys ohne Mitwirkung des jeweiligen Netzbetreibers zu lokalisieren. Viel wahrscheinlicher ist es jedoch, dass mit diesen Geräten auch Gesprächsinhalte abgehört werden sollen. Obwohl das die eigentliche Funktion von IMSI-Catchern ist, fehlt dafür weiterhin die Rechtsgrundlage (§134 Z2a StPO-E).

Lauschangriff auf private PKW

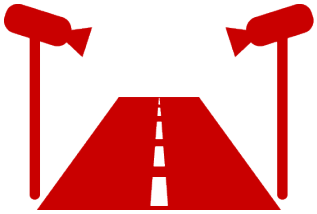
Was von Innenminister Sobotka als "kleiner" Lauschangriff auf Autos beschrieben wird, ist in Wahrheit ein großer Lauschangriff. Die Regierung will die "Schaffung der Möglichkeit der akustischen Überwachung außerhalb von vom Wohnrecht geschützter Räume."

Der "kleine Lauschangriff" betrifft das Abhören und Aufzeichnen (Bild und Ton) von Gesprächen unter gewissen Voraussetzungen. Dabei muss man zwischen der Strafprozessordnung (§ 136 Abs 1 Z 2 StPO) und dem Sicherheitspolizeigesetz (§ 54 Abs. 4 SPG) unterscheiden. Der kleine Lauschangriff setzt jedenfalls voraus, dass einer der Gesprächspartner (verdeckte Ermittler, V-Leute) in die Überwachung eingeweiht ist.

Die vorgeschlagene Maßnahme ist unserer Ansicht nach ein großer Lauschangriff (§ 136 Abs. 1 Z 3 StPO). Laut Innenminister Sobotka sollen Gespräche von Personen in Fahrzeugen abgehört werden, die im Rahmen der organisierten Kriminalität oder terroristischer Aktivitäten koordinierend in Begleitfahrzeugen tätig sind. In diesen Fällen sind eben keine verdeckten Ermittler oder sonst eingeweihte Personen anwesend. Im Arbeitsprogramm der Bundesregierung 2017/2018 wird angekündigt, dass der große Lauschangriff nun schon bei Delikten, die mit einer Freiheitsstrafe von mehr als drei Jahren bedroht sind, zulässig sein soll. Diese höchst eingriffsintensive Maßnahme soll also zukünftig auch bei niederschwelligeren Delikten angeordnet werden können. Hier zeigt sich das in den Sozialwissenschaften beschriebene Phänomen des sog. "Function-Creep" besonders deutlich. Durch eine ständige Ausweitung der Überwachungsmaßnahmen werden die Grund- und Freiheitsrechte Stück für Stück beschnitten – der demokratische Rechtsstaat wird langsam zum Überwachungs- und Polizeistaat.

Der Gesetzesvorschlag sieht deutlich niedrigere Hürden für den Einsatz dieser Maßnahme vor (nämlich schon Straftaten, die mit einer Freiheitsstrafe von mehr als einem Jahr bedroht sind).

Kennzeichenerfassung

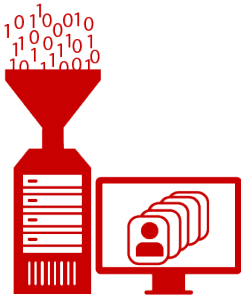


Künftig soll auch auf allen österreichischen Straßen von jedem Auto der Lenker des Fahrzeugs, das Kennzeichen, Marke, Typ und Farbe erfasst werden. Die von den Sicherheitsbehörden selbst ermittelten oder auf deren Ersuchen von der ASFINAG übermittelten Daten, können in Verdachtsfällen bis zu 5 Jahre gespeichert werden (§ 53a Abs 6 SPG-E). Sind die Daten nicht zur weiteren Verfolgung gerichtlich strafbarer Handlungen erforderlich, sind sie nach längstens 48 Stunden zu löschen. Damit entsteht eine neue Form der anlasslosen Massenüberwachung und jeder Autofahrer wird unter Generalverdacht gestellt. Aus grundrechtlicher Perspektive ist dieser Schritt in Richtung einer kompletten Überwachung aller Kennzeichen sehr problematisch. Der VfGH hat 2007 in seiner Entscheidung zur Section Control festgestellt, dass eine Überwachung von Autofahrerinnen und Autofahrern nur auf bestimmten, besonders gefährlichen und per Verordnung festgelegten Strecken zulässig ist. Zudem dürfen laut VfGH nur Kennzeichendaten gespeichert und an die Behörden übermittelt werden, wenn die erfassten Fahrzeuge zu schnell unterwegs oder bereits zur Fahndung ausgeschrieben sind. Diese Form der Vorratsdatenspeicherung ist aus unserer Sicht nicht mit diesem Erkenntnis vereinbar und steht auch im Widerspruch zur Rechtsprechung des EuGH im Fall Watson/Tele 2 Sverige.
Eine anlasslose und verdachtsunabhängige Speicherung der Kennzeichendaten aller Fahrzeuge und eine im Raum stehende Vernetzung sämtlicher Verkehrskameras steht auch im krassen Widerspruch zur Rechtsprechung des EuGHs. Dieser hat im Zusammenhang mit der Vorratsdatenspeicherung mehrfach festgestellt, dass eine anlasslose und verdachtsunabhängige Speicherung von (Kommunikations-)Daten wegen Unvereinbarkeit mit den Grundrechten nicht zulässig ist. Sie stellt eine massive Einschränkung der Grundrechte aller Menschen in Österreich dar. Das so entstehende Gefühl, dass die Menschen Gegenstand ständiger Überwachung sind, steht einem äußerst zweifelhaften Nutzen bei der Verhinderung von Straftaten gegenüber und verstärkt sogenannte "chilling effects" (Selbstzensur).

Status Juni: Mitte Juni 2017 werden Details zur geplanten Kennzeichenerfassung bekannt. Der ORF Report berichtet[33] etwa, dass nicht nur Daten der Fahrzeuge erfasst werden sollen, sondern auch die Bilder der Lenker.

33 https://www.youtube.com/watch?v=r-2GkCUGqAg

Vorratsdatenspeicherung 2.0



Die Regierung fordert in ihrem Überwachungspaket auch die Wiedereinführung der Vorratsdatenspeicherung. Dieses Gesetz wurde schon mehrfach von Höchstgerichten in ganz Europa aufgehoben. Erst im Dezember 2016 hat der Europäische Gerichtshof entschieden, dass die nationalen Regelungen zur Vorratsdatenspeicherung in Großbritannien und Schweden nicht mit den Grundrechten vereinbar sind. In Österreich wurde diese Art der verdachtsunabhängigen, anlasslosen Massenüberwachung 2014 vom Verfassungsgerichtshof wegen Grundrechtswidrigkeit annulliert; aufgrund eines Verfahrens, das der AKVorrat (so der frühere Name unseres Vereins) angestrebt hat.

Auf Anordnung der Staatsanwaltschaft soll ein Telekombetreiber künftig auch wieder Vorratsdaten für bis zu ein Jahr speichern müssen (§ 99 TKG-E). 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.

Registrierung von Prepaid-SIM-Karten

Anonyme Prepaid-Karten sollen mit dem Überwachungspaket der Vergangenheit angehören. Jeder Kauf einer SIM-Karte müsste mit der Registrierung der Identität einhergehen. Damit wird eine weitere Möglichkeit abgeschafft, unbeobachtet zu kommunizieren. Kriminelle können diese Maßnahme leicht mit ausländischen SIM-Karten oder gratis verfügbaren, anonymen Messaging-Diensten umgehen. Für die Mehrzahl der Nutzerinnen und Nutzer in Österreich fällt jedoch eine weitere Möglichkeit weg, anonym zu kommunizieren. Damit werden 4,5 Millionen Nutzerinnen und Nutzer unter Generalverdacht gestellt. Der äußerst zweifelhafte Nutzen für die Bekämpfung von Kriminalität, steht einem Eingriff in das Recht aller Österreicherinnen und Österreicher, frei und unbeobachtet zu kommunizieren gegenüber. Das lässt diese Maßnahme nicht verhältnismäßig erscheinen.

Eine Studie der Interessensvertretung[34] der Telekomindustrie fand keine Belege dafür, dass die Registrierung von SIM-Karten zu einer verbesserten Verbrechensaufklärung führt oder gegen Terrorismus hilft. Mexiko hat das Verbot anonymer SIM-Karten sogar wieder abgeschafft, da die Verbrechensrate sogar stieg und es nur zu einem Schwarzmarkt für SIM-Karten führte. Tschechien,

34 http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf%20

Neuseeland, Kanada, Rumänien, Großbritannien und die EU-Kommission[35] haben die Maßnahme analysiert und sich aufgrund der fehlenden Belege dagegen entschieden. Nach den Terroranschlägen in London 2005 hat sogar eine eigene Kommission von Sicherheitsbehörden[36] diese Maßnahme geprüft und weil es keine Belege für die Nützlichkeit für die Sicherheit gab, von einer Einführung abgeraten.

Des Weiteren wird durch diese Maßnahme die aufblühende Szene der günstigen virtuellen Mobilfunkbetreiber geschwächt. Wenige dieser Diskonter besitzen aktuell die Infrastruktur beim Kauf einer SIM-Karte die Identität ihrer Käufer zu überprüfen.

Beschränkung des Briefgeheimnisses

Die vorgeschlagenen Novelle der Strafprozessordnung 1975 zur Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Auskunft über Vorratsdaten sowie Überwachung von Nachrichten sieht folgende Streichung vor:

> § 135. (1) Beschlagnahme von Briefen ist zulässig, wenn sie zur Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, erforderlich ist ~~und sich der Beschuldigte wegen einer solchen Tat in Haft befindet oder seine Vorführung oder Festnahme deswegen angeordnet wurde.~~

Das bedeutet eine massive Beschränkung des Briefgeheimnisses, eines Grundrechtres, das in der Verfassung demokratischer Staaten garantiert ist. Dies gefährdet eine bedeutende Errungenschaft, die nach der Überwindung des metternischschen Überwachungsstaats erkämpft wurde.

Fußfesseln für nicht verurteilte "Gefährder"

"Gefährder" ist erst einmal nur ein Verdächtiger, die Bundesregierung spricht in diesem Zusammenhang von einer "abstrakten Gefährdungslage". Wenn solche Personen Fußfesseln tragen müssen, werden Maßnahmen angewandt, die bislang nur gegen verurteilte Straftäter im Strafvollzug bzw. bei Vorliegen eines konkreten Tatverdachts und einem Haftgrund als gelinderes Mittel zur Untersuchungshaft zur Anwendung gekommen sind. Eine derartige Maßnahme steht auch im Widerspruch zum Prinzip der Unschuldsvermutung und ist daher höchst problematisch. Zudem steht dieser Eingriff im krassen Widerspruch zum Bundesverfassungsgesetz, in dem der Schutz der persönlichen Freiheit besonderen Stellenwert hat.

Update: In diesem Punkt scheint die Bundesregierung mittlerweile zur Vernunft zu kommen. Laut Kurier hat Justizminister Wolfgang Brandstetter in einem Erlass klargestellt, dass die Fußfessel nicht als

35 http://europarl.europa.eu/RegData/questions/reponses_qe/2012/006014/P7_RE(2012)006014_EN.doc
36 https://www.theyworkforyou.com/wrans/?id=2007-07-16b.4.3&s=%22pay+as+you+go%22+mobile+phones

gelinderes Mittel zur Überwachung von Gefährdern eingesetzt werden kann, sondern nur als Alternative zur U-Haft[37].

Neues Versammlungsrecht

Ein weiterer Vorstoß zur Einschränkung der Meinungsfreiheit ist die Beschränkung[38] des Demonstrationsrechts. Wir haben den Gesetzesentwurf in einer Stellungnahme[39] kritisiert.

Hier eine kurze Zusammenfassung unserer Kritikpunkte: Das Grundrecht auf Versammlungsfreiheit wird untergraben, da aufgrund schwammiger Formulierungen im Gesetz ermöglicht wird, Versammlungen zu verhindern, die vom angegebenen Regulierungszweck der Gesetzesänderung nicht erfasst sind. Demonstrationen für den Whistleblower Edward Snowden oder gegen die Auspeitschung von Bloggern in Saudi-Arabien könnten mit diesem Gesetz untersagt werden. Eine Schutzzone, um den ungestörten Ablauf von Demonstrationen entgegengesetzter Zwecke sicherzustellen, ist sinnvoll. Der Wortlaut der vorgeschlagenen Bestimmung verhindert jedoch auch, dass Demonstrationen mit gleichen Zielen am selben Ort stattfinden. Zudem stellt die Verdopplung der Anzeigefrist von 24 auf 48 Stunden viele Demonstrationen, die aktuelle politische Geschehnisse zum Anlass haben, vor große Hürden.

Dieses Gesetz wurde am 26. April 2017 im Nationalrat beschlossen und ist am 23. Mai 2017 in Kraft getreten. Nicht nur wir sind der Meinung, dass die neuen Regelungen verfassungswidrig sind. Hier ein lesenswerter Artikel, der gute Argumente für weitere Schritte gegen diese Einschränkung unserer Freiheiten liefert: Versammlungsrecht: Der Geruch des Totalitären[40].

Einschränkung der Meinungsfreiheit

Es muss möglich sein, Kritik am Staat oder seinen Institutionen zu üben. Die Regierung will jetzt einen Straftatbestand schaffen, der zunächst einmal nur Meinungsäußerungen betrifft. Damit wird das Grundrecht auf Freiheit der Meinungsäußerung ausgehöhlt. Dies ist eine äußerst gefährliche Entwicklung in Richtung einer "Gedankenpolizei" im Sinne George Orwells. Es gibt aus unserer Sicht ausreichend Straftatbestände, die sich auf konkrete "staatsfeindliche" Handlungen beziehen, um solchen Bewegungen auf rechtsstaatlicher Ebene zu begegnen.[41]

37 https://kurier.at/politik/inland/fussfessel-fuer-gefaehrder-nur-alternative-zur-u-haft/256.749.845
38 https://www.parlament.gv.at/PAKT/PR/JAHR_2017/PK0455/index.shtml
39 https://epicenter.works/sites/default/files/epicenter.works_stellungnahme_versammlungsgesetz_1953_2063_a_0.pdf
40 http://derstandard.at/2000056612049/Versammlungsrecht-Der-Geruch-des-Totalitaeren
41 https://epicenter.works/content/kritik-soll-als-staatsfeindliche-handlung-bestraft-werden

Das Gesetz wurde am 28. Juni 2017 im Nationalrat beschlossen. Wir haben davor alle Abgeordneten aufgerufen, gegen die Einführung eines Gesinnungsstraftatbestandes zu stimmen[42].

Status Mai 2017: Die Regierungsparteien haben sich auf eine Neufassung des Gesetzes geeinigt, die im Ministerrat beschlossen wurde. Die Abstimmung im Nationalrat ist für Juni 2017 vorgesehen. Im neuen Vorschlag sind die "staatsfeindlichen" Handlungen klarer als solche definiert, "die Hoheitsrechte der Republik rundweg ablehnen oder sich eigene Hoheitsrechte anmaßen". Unsere Kritik ist nach wie vor aufrecht: Die Einführung eines Gesinnungsstrafrechts ist eine gefährliche Entwicklung. Justizminister Brandstetter gesteht selbst ein, dass die "theoretische Gefahr" besteht, "dass auch Bewegungen kriminalisiert werden, die man nicht treffen will".

Bundesheer im Inneren

Das Bundesheer soll aus guten Gründen nur im Katastrophenfall Aufgaben der Inneren Sicherheit ausführen. Die Abgrenzung zwischen Polizei und Bundesheer ist nicht nur historisch begründet, sondern auch organisatorisch. Polizisten genießen eine umfassende Ausbildung, um deeskalierend und im Rahmen der Gesetze zu agieren. Soldaten hingegen werden nur im Gebrauch von Waffen und für das Befolgen von Befehlen ausgebildet. Das aktualisierte Regierungsprogramm sieht nun vor, dem Militär noch mehr Aufgaben der inneren Sicherheit zu übertragen.

Darüber hinaus soll das Bundesheer auch Drohnen zur Aufklärung von Grenzregionen, biometrische Systeme zur Personenerkennung und nicht näher spezifizierte "neue Detektionstechnologien" bekommen. Wenn es zur Normalnormal wird, im Alltag schwer bewaffnete Menschen um sich zu haben, verändert dies die Gesellschaft. Wir fordern deshalb, dass die Polizei weiterhin alle Aufgaben erfüllen soll, zu denen Sie in der Lage ist, gegebenenfalls auch mit den dafür nötigen zusätzlichen Ressourcen.

Ausweispflicht in Zügen und Bussen

Mit dem Überwachungspaket soll es bald eine Ausweispflicht beim Kauf von Bus- und Zugtickets geben. Beförderungsunternehmen werden in die Pflicht genommen, Daten von allen ihren Passagieren zu erfassen. Es ist noch unklar ob dies nur in Grenzregionen oder im ganzen Land passieren muss, etwa in S-Bahnen und Regionalzügen.

Gemeinsam mit der der Überwachung von U-Bahnen, Bahnhöfen und öffentlichen Plätzen und der Kennzeichenerfassung von Autos auf der Straße gäbe es dann keine Möglichkeit mehr, sich in Österreich noch unbeobachtet von einer Stadt in die andere zu bewegen, außer man geht zu Fuß. Zu diesem Punkt gibt es noch keinen konkreten Gesetzesvorschlag.

42 https://epicenter.works/content/staatsfeindeparagraf-meinungsfreiheit-darf-nicht-eingeschraenkt-werden

Cybersicherheitsgesetz

Im Koalitionspapier ist der Absatz zum Cybersicherheitsgesetz ist im Koalitionspapier sehr vage formuliert. Wir weisen darauf hin, dass es vermehrt Bestrebungen von Regierungen bzw. Ermittlungsbehörden gibt, Sicherheitslücken oder Hintertüren (Backdoors) in IT-Systemen zu nutzen, offen zu lassen oder gar anzukaufen (ein Beispiel dafür findet sich im Logbuch Netzpolitik[43]). Diesen Bestrebungen muss im Sinne der Sicherheit für alle Anwenderinnen und Anwender eine klare Absage erteilt werden. (Auch der Bundestrojaner kann nur unter Ausnutzung solcher Sicherheitslücken eingeschleust werden.)

Echtes Sicherheitspaket statt Überwachungspaket

Im Überwachungspaket der Regierung ist keine wirkliche Sicherheit enthalten. Statt "subjektivem" Sicherheitsgefühl, Angstmache und Populismus brauchen wir ein "objektives" Sicherheitspaket:

- mehr spezifisch ausgebildete Polizeikräfte statt mehr Kameras
- verbesserte Analysekapazitäten für Sicherheitsbehörden: Mehr speziell ausgebildete Datenanalysten statt mehr Daten
- mehrsprachige Polizeikräfte bzw. mehr Dolmetscherkapazitäten
- mehr Präventionsarbeit gegen Radikalisierungstendenzen
- bessere Vernetzung mit Communities als vertrauensbildende Maßnahmen und zur frühzeitigen Erkennung radikaler Tendenzen
- ein Ablaufdatum für neue Überwachungsgesetze ("Sunset Clauses" mit wissenschaftlicher Evaluierung und Rücknahme wirkungsloser Maßnahmen)
- Evaluierung aller bestehenden Überwachungsgesetze auf ihre Verfassungskonformität[44]

43 https://logbuch-netzpolitik.de/lnp206-goldene-zeiten#t=1:48:08.189
44 https://epicenter.works/thema/heat