KOMintern
Kommunistische Gewerkschaftsinitiative – International

Antrag Nr. 5

der Liste Kommunistische Gewerkschaftsinitiative International [KOMintern]
an die Vollversammlung der Arbeiterkammer

Sicherheit und Grundrechtsschutz für Alle statt Überwachungspaket

Österreich hat – selbst innerhalb Europas – eine der am weitesten entwickelten Demokratien. Nach den Gräueln des Faschismus mit Krieg, Massenmord und Überwachung hat sich Österreich eine der fortgeschrittensten Demokratien gegeben.
Die ökonomische Entwicklung, das Nachhinken der Arbeitseinkommen gegenüber Kapital- und Unternehmensgewinnen bewirken eine Aufspaltung und immer stärkeres Auseinanderbrechen der Gesellschaft. Die Ausweitung dieses Bruchs wird von manchen politischen Parteien und auflagenstarken Massenmedien gefördert. Für Arbeiterkammern und Gewerkschaften ist es unumgänglich, diese Tendenzen in Gesellschaft und Verwaltung aufzuzeigen und zu verhindern.

Österreich zählt zu den sichersten Ländern der Welt. Laut dem Global Peace Index von 2017 liegt Österreich in der Rangliste der sichersten Länder der Welt auf Rang vier. Hinter Island, Neuseeland und Portugal. Umgekehrt erscheinen Sicherheit, Vertraulichkeit und gesetzeskonformer Umgang mit Privatsphäre und sensiblen und vertraulichen Daten im Behördenbereich zudem alles andere als hinreichend gesichert: Die Vorgänge rund um das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung lassen berechtigte Zweifel am Umgang und der Gesetzeskonformität im Vorgehen von Behörden aufkommen: unzureichende Löschung von sensiblen Daten, Abgreifen und Kopieren von Daten zur Verwendung bei anderen Behörden ...

In dieser Situation legt die schwarz-blaue Regierung ein Überwachungspaket vor, das massive Eingriffe in Grundrechte und verschärfte Überwachung ermöglichen soll.

Dabei zeigt sich besonders deutlich, dass durch ständige Ausweitung der Überwachungsmaßnahmen die Grund- und Freiheitsrechte Stück für Stück beschnitten werden – der demokratische Rechtsstaat wird langsam zum Überwachungs- und Polizeistaat.

Das Überwachungspaket der schwarz-blauen Regierung umfasst:

1. ***Bundestrojaner (staatliche Überwachungssoftware)***
   Damit soll es dem Staat ermöglicht werden, mit Schadsoftware in „Computersysteme“ und Handys von „Verdächtigen“ und „Gefährdern“ einzubrechen. Zweck sei es, Kommunikationsüberwachung sowie Telefonüberwachung zu ermöglichen. Telefonüberwachung ermöglicht das Mithören und Aufzeichnen von Kommunikation von

außerhalb der intimsten Privatsphäre Betroffener. Die neuen Überwachungsmöglichkeiten erfordern jedoch das Eindringen in die intimsten Bereiche der Privatsphäre. Um technisch zu funktionieren, muss der Zugriff auf Systemebene erfolgen. Damit ist jede Manipulation am betroffenen Gerät möglich: Zugriff auf alle vorhandenen Funktionen und Datenbestände des Geräts, lesen, kopieren, verändern, löschen, hinzufügen und ausleiten von Daten auf dem Gerät, unbemerkt vom Benutzer. Dabei ist die juristische Definition von „Computersystem" dermaßen vage, dass vom selbstfahrenden Auto über Herzschrittmacher, Notebooks und Privaten bis zum Computersystem einer Großbank alles umfasst ist (Anzumerken ist, dass schon jetzt – unter strengen Auflagen und richterlicher Zustimmung im Zuge des „großen Lauschangriffs" das Eindringen in Intimbereiche wie Wohnungen und das Anbringen von Überwachungstechnik zulässig ist und angewandt wird).

Damit die Software eingesetzt werden kann, müssen staatliche Behörden darüber hinaus wie Hacker oder Kriminelle vorgehen und das Programm Verdächtigen unterjubeln, da aktuelle Handys mit starken Schutzmechanismen und starker Verschlüsselung ausgestattet sind. Etwa mit manipulierten E-Mails und durch die Ausnutzung von Sicherheitslücken.

2. **Einschränkung des Briefgeheimnisses**
   Die vorgeschlagene Novelle der Strafprozessordnung 1975 zur Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Auskunft über Vorratsdaten sowie Überwachung von Nachrichten bedeutet eine massive Beschränkung des Briefgeheimnisses, eines Grundrechtes, das in der Verfassung demokratischer Staaten garantiert ist. Dies gefährdet eine bedeutende Errungenschaft, die nach der Überwindung des metternichschen Überwachungsstaats erkämpft wurde.

3. **Lauschangriff im Auto**
   Mit dieser vorgeschlagenen Maßnahme wird die Barriere für den „großen Lauschangriff (§ 136 Abs. 1 Z 3 StPO)" drastisch reduziert.
   Im Arbeitsprogramm der Bundesregierung 2017/2018 wurde 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 niederschwelligen Delikten angeordnet werden können.
   Der aktuelle Gesetzesvorschlag sieht eine noch deutlich niedrigere Hürde für den Einsatz dieser Maßnahme vor (nämlich schon bei Straftaten, die mit einer Freiheitsstrafe von mehr als einem Jahr bedroht sind).

4. **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" angestrebt hat.

5. **IMSI-Catcher**
   Auch der Einsatz von IMSI-Catchern für die Überwachung von Mobiltelefonie soll kommen. 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 (§ 135 Abs 2a StPO-E).

6. **Vernetzung von Videoüberwachung (inkl. Gesichtserkennung!)**
   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). 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, weil die Kosten zu hoch waren und der Nutzen für die Verbrechensbekämpfung nicht erkennbar war.

7. **Lückenlose Überwachung des Autoverkehrs (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 jedoch 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. Die geplante Form der Vorratsdatenspeicherung ist nicht mit diesem Erkenntnis vereinbar und steht auch im Widerspruch zur Rechtsprechung des EuGH im Fall Watson/Tele 2 Sverige, nach der eine Vorratsdatenspeicherung unter anderem nur zur Bekämpfung schwerer Kriminalität zulässig sein kann.

8. **Registrierungspflicht für Wertkarten**
   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 gegenüber, frei und unbeobachtet zu kommunizieren. Das lässt diese Maßnahme nicht verhältnismäßig erscheinen. 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, Neuseeland,

Kanada, Rumänien, Großbritannien und die EU-Kommission haben die Maßnahme analysiert und sich aufgrund der fehlenden Belege dagegen entschieden.

Die Grundrechtsorganisation epicenter.works fasst ihre Kritik wie folgt zusammen:

1. Die Sicherheit der IT-Infrastruktur in Österreich wird schwer gefährdet.
2. Eine Überwachungsgesamtrechnung wurde nicht durchgeführt.
3. Eine Wirkungsfolgenabschätzung bzgl. Auswirkungen auf Grundrechte und Gesellschaft fehlt im Begutachtungsentwurf.
4. Durch die Anlassdatenspeicherung soll eine Vorratsdatenspeicherung durch die Hintertür eingeführt werden.
5. Die Schwellen für viele Grundrechtseingriffe werden sukzessive herabgesetzt.
6. Insgesamt sollen eine Fülle an (weiteren) Bestimmungen mit polizeistaatlichen Tendenzen Einzug in den österreichischen Rechtsbestand halten. Es ergibt sich zunehmend das Bild, dass Österreich in einen Polizei- und Überwachungsstaat umgebaut wird.
7. Es entstehen enorme finanzielle Kosten für eingriffsintensive Maßnahmen, die die Sicherheit erwiesenermaßen nicht erhöhen.
8. Der Rechtsschutz ist in vielen Punkten der Entwürfe nicht ausreichend gewährleistet.

Selbst der renommierte Kriminalsoziologe Reinhard Kreissl pointierte dazu kürzlich: „Der Sinn dieses Überwachungspakets ist eher symbolischer Natur". „Man dramatisiert die Situation und schiebt dann spektakulär ein Gesetzespaket hinterher, um die vermeintliche Bedrohung zu bekämpfen. Die Frage, was die Sicherheit Österreichs gefährdet, wird dabei nur schlampig beantwortet." Mit Argumenten wie „Migranten", „Extremisten" und „Cybercrime". Bundestrojaner oder das „Quick Freeze" sind laut Kreissl für die Polizeiarbeit von marginaler Bedeutung.

<u>Deshalb beschließt die Vollversammlung der Arbeiterkammer:</u>

- *Die AK* lehnt das vorgeschlagene Überwachungspaket ab!

- *Die AK fordert stattdessen:*

  - Überprüfung und Evaluierung bestehender Überwachungsgesetze hinsichtlich ihrer Grundrechtskonformität, Sinnhaftigkeit und Wirksamkeit vor Erlassung neuer Überwachungsmaßnahmen
  - Schutz der BürgerInnen vor Bedrohung und Übergriffen insbesondere im Bereich technischer Infrastruktur und digitaler Privatsphäre; dazu gehört auch – nach Information der Hersteller -Veröffentlichung aller bekannten Sicherheitslücken
  - Rigorose Umsetzung der Datenschutzgrundverordnung (DSGVO) sowie ausreichende materielle und qualifizierte personelle Dotierung der Datenschutzbehörden (ausreichend JuristInnen und TechnikerInnen)
  - Sicherstellung, dass Amtsträger und BehördenvertreterInnen auch persönlich für Grundrechtsverstöße und Datenschutzvergehen haften

- Zwingendes Ablaufdatum ("Sunset Clauses" mit wissenschaftlicher Überprüfung der Wirksamkeit/Evaluierung und Rücknahme wirkungsloser Maßnahmen) bei allen Überwachungsgesetzen
- Mehr Präventionsarbeit

- Breite öffentliche Diskussion und Berücksichtigung der Stellungnahmen von ExpertInnen und Zivilgesellschaft

- Verankerung der Integrität informationstechnischer Systeme und Schutz der digitalen Privatsphäre in der Verfassung