Die Mitgliederversammlung der Jusos Bremen-Stadt möge beschließen,
Der UB-Parteitag der SPD Bremen-Stadt möge beschließen,
Der Landesparteitag möge beschließen,

A14 Maß halten! Verschärfung des Polizeigesetzes überdenken!

Der Parteitag erkennt an, dass es in der Bevölkerung ein Bedürfnis nach mehr Sicherheit gibt und wir begrüßen die stetigen Bemühungen des Senators für Inneres dieses Bedürfnis zu befriedigen. Die geplante Neuregelung des BremPolG sehen wir jedoch teilweise kritisch, insbesondere:

- die massive Ausweitung der Überwachung von Computern und Smartphones durch Schadsoftware und "Staatstrojaner"
- den massiven Ausbau staatlicher Videoüberwachung im öffentlichen Raum
- die Einführung von "elektronischen Fußfesseln" zur lückenlosen Kontrolle von mutmaßlichen "Gefährdern" (Als "Gefährder" gelten Menschen, die nicht etwa Straftaten begangen haben, sondern denen solche aufgrund bestimmter Anhaltspunkte lediglich zugetraut werden)

Deshalb fordern wir den Senat und besonders den Senator für Inneres sowie die Bürgerschaftsfraktion auf die geplante Verschärfung des BremPolG nicht weiter zu verfolgen.

Begründung:
Mit dem Argument der Terrorismusabwehr werden der Polizei weitreichende Eingriffe auch in unser aller Privat- und Intimsphäre ermöglicht. Der Gesetzentwurf lässt sich in eine aktuelle Entwicklung in Bund und Ländern einreihen, mühsam errungene Freiheitsrechte für eine vermeintliche Sicherheit einzuschränken. Von diesen Maßnahmen können aber auch unbeteiligte und unschuldige Dritte betroffen sein. Die für Betroffene zum Teil sehr schwerwiegenden Maßnahmen sollen auf bloßen Verdacht hin präventiv durchgeführt werden, ohne dass eine Straftat begangen wurde oder eine konkrete Gefahr unmittelbar bevorsteht! Für die Video- und Fußfesselüberwachung lässt sich zusätzlich sagen, sie werden nur notwendig durch die zu schlechte finanzielle Ausstattung des öffentlichen Haushalts. Eine ausreichend finanzierte Polizei kann auch tatsächlich Sicherheit schaffen, eine Kamera oder eine Fußfessel kann das nicht, sie kann nur Freiheit und Daten-Souveränität einschränken. Wir müssen dringend aufhören als Partei der Bürger*innenrechte auf Grund von Kostendruck die Freiheit der Bürger*innen weiter einzuschränken.

Im Falle des Trojaners kommt hinzu, ein Staatstrojaner macht alle Geräte unsicher. Der "Staatstrojaner" ("Brementrojaner") gefährdet die Sicherheit von informationstechnischen Systemen (IT-Systemen). Er zerstört das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von IT-Systemen und öffnet Missbrauch und gefährlichen Cyberattacken Tür und Tor. Die geplanten Maßnahmen sind zudem gerichtlich oder parlamentarisch kaum zu kontrollieren.
Der Einsatz von Trojanern zur Telekommunikationsüberwachung birgt eine strukturelle Gefahr für die Allgemeinheit. Wer ein Gerät mit einer Software infizieren will, muss dafür Lücken in dem System

ausnutzen. Dafür aber müssen diese Systeme unsicher sein – damit man sie infizieren kann. Genau hier ist das Dilemma: um im Einzelfall auf ein System zu kommen, beteiligen sich Polizei und Geheimdienste daran, Unsicherheiten für alle zu schaffen. Werden Sicherheitslücken unter Verschluss gehalten, bringt das alle Nutzer*innen von Geräten in Gefahr, denn diese Möglichkeiten stehen auch Kriminellen oder feindlichen Geheimdiensten zur Verfügung. Außerdem sind auch staatliche Institutionen und große Firmen nicht vor Hacker*innenangriffen sicher. Immer wieder wurden in der Vergangenheit Quellcodes von solchen Programmen geklaut.

Auf diese Weise gefährden Trojaner ein Grundrecht, das ein Urteil des Bundesverfassungsgerichts (BVerfG) vom 27. Februar 2008 definiert: das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (auch: „IT-Grundrecht“). In diesem wird festgestellt, dass digitale Systeme allgegenwärtig sind und einen extrem hohen Stellenwert in der persönlichen Lebensführung haben. Aus den damit verbundenen Gefahren für Einzelne leitet das Gericht eine besondere Schutzwürdigkeit dieser digitalen Systeme und Geräte ab.

Trojaner haben immer die Möglichkeit, später weitere Funktionen nachzuladen. Für solche Zwecke sind diese Programme normalerweise auch gedacht: sie ermöglichen vollen Zugriff auf Geräte, damit fremde Personen infizierte Geräte fernsteuern können. Ihre Funktionsweise kann also je nach Einsatz oder Gerät variieren. Das bedeutet aber auch: Niemand kann garantieren, dass sie wirklich nur gesetzeskonform eingesetzt werden. Durch bestehende Software-Lücken oder einen Trojaner kann auch „Beweismaterial“ auf einem Gerät platziert werden. Dem Chaos Computer Club (CCC) wurde 2011 jedoch die damalige Version des Staatstrojaners zugespielt. Untersuchungen zeigten, dass „aufgrund von groben Design- und Implementierungsfehlern […] außerdem eklatante Sicherheitslücken in den infiltrierten Rechnern [entstehen], die auch Dritte ausnutzen können.“ Expert*nnen haben also schon einmal einen solchen Staatstrojaner als nachweislich rechtswidrig entlarvt.

Das Problem bei der Überwachung von Geräten ist weiter, dass es eigentlich nur erlaubt ist, aktuell laufende Kommunikation mitzuschneiden – und auch das nur unter bestimmten Bedingungen. Der Staatstrojaner aber kann technisch viel mehr: Behörden haben durch ihn vollen Zugriff auf alle Daten auf dem infizierten Gerät. Damit gibt es quasi keine Unterschiede mehr zwischen einer Überwachung laufender Kommunikation („Quellen-TKÜ“) und einer vollumfänglichen „Online-Durchsuchung“, bei der Daten sogar gezielt manipuliert werden könnten. Letztere hat das Bundesverfassungsgericht 2008 verboten und das oben genannte „IT-Grundrecht“ geschaffen.

Das Bundesverfassungsgericht kippte 2016 auch das BKA-Gesetz. Verdeckte Maßnahmen dürften ausschließlich zur Abwehr von Gefahren durch den internationalen Terrorismus eingesetzt werden, um nicht die Grundrechte aller Bürger*innen zu verletzen, so die Richter. Die Verhältnismäßigkeit dieser Maßnahmen sei nur dann gegeben, wenn „überragend bedeutende Rechtsgüter“ betroffen seien. Die Bundesregierung musste im BKA-Gesetz daher 2017 die bemängelten Passagen neu formulieren.

Scharfe Kritik kam auch von der Bremer Landesbeauftragten für Datenschutz und Informationsfreiheit: “Der Entwurf zur Änderung des Bremischen Polizeigesetzes wirft erhebliche rechtsstaatliche und datenschutzrechtliche Bedenken auf.”
(Dr. Imke Sommer, Landesbeauftragte für Datenschutz und Informationsfreiheit, 3. Januar 2018)
Die Landesbeauftragte bemängelte außerdem die Verwendung des Begriffs der “terroristischen Straftat”, der

im Strafgesetzbuch nicht vorkommt. Im geplanten BremPolG wurde dieser jedoch wie selbstverständlich als Grundlage für weitgehende neue Befugnisse der Bremer Polizei verwendet.