LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

**STELLUNGNAHME**
**17/937**

A09, A14

NETZPOLITIK.ORG
DIGITALE SELBSTVERTEIDIGUNG

Marie Bröckling
Redaktion netzpolitik.org
Schönhauser Allee 6/7
10119 Berlin

Telefon: +49-30-92105-986
Marie.Broeckling@netzpolitik.org

# Stellungnahme an den nordrhein-westfälischen Landtag, Innenausschuss

Änderungsantrag zum Entwurf eines Reformgesetzes zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen Drs. 17/3865

Berlin, den 8. November 2018

## 1. Einleitung

Der aktuelle Änderungsantrag zum Entwurf für das „Sechste Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen" steht im Kontext einer Welle von Novellierungen der Länderpolizeigesetze in Deutschland und ist sichtlich von diesen geprägt. Motor hierfür sind die von der Union geführten Innenministerien.[1] In der Berichterstattung bekamen bislang eben jene Landesregierungen besonders viel Aufmerksamkeit, die durch ihre umfangreichen Ausweitung der polizeilichen Befugnisse im präventiven Bereich – bis hin zum „gesetzgeberischen Exzess" – hervortraten: Bayern, Baden-Württemberg, Sachsen, Niedersachsen und NRW.[2]

Es lohnt sich daher, den zeitlichen Blick zu erweitern, um die Unterschiede in der Debatte in eben diesen Bundesländern vor dem Frühjahr 2017 wahrzunehmen: Im Jahr 2013 wollte die damalige niedersächsische Landesregierung das Polizeigesetz *ent*schärfen und die Dauer des Gewahrsams von zehn auf vier Tage *herab*senken.[3] Auch in NRW gab es bis 2017 keine Absichten, die Befugnisse der Polizei auszuweiten.[4]

1 Vgl. Polizeigesetze in Deutschland – Jeder für sich: „Gerade die von der Union geführten Innenministerien scheinen sich die Gelegenheit nicht entgehen lassen zu wollen, die Befugnisse der Polizei deutlich auszuweiten." http://www.spiegel.de/panorama/justiz/polizeigesetze-in-deutschland-jedes-bundesland-fuer-sich-a-1207833.html vom 15. Mai. 2018.
2 Zitat des innenpolitischen Sprechers der Grünen in Schleswig-Holstein, Burkhard Peters, zur Novellierung des PAG in Bayern gegenüber netzpolitik.org. Vgl. https://netzpolitik.org/2018/bayerisches-polizeigesetz-billige-tricks-der-csu-entlarvt/ vom 23. April. 2018.
3 Vgl. Koalitionsvertrag zwischen SPD und Bündnis90/Die Grünen, S. 17 http://www.spd-fraktion-niedersachsen.de/imperia/md/content/ltf/koalitionsvereinbarung_rot-gr__n_20130214.pdf vom 14. Februar 2013.
4 Vgl. Koalitionsvertrag zwischen SPD und Bündnis90/Die Grünen https://netzpolitik.org/wp-upload/Koalitionsvertrag_2012-2017.pdf vom 12. Juni 2012.

Für den Kurswechsel im Frühjahr 2017 liegen keine stichhaltigen Gründe vor. Es werden polizeiliche Maßnahmen geschaffen, wo schlicht keine Bedarfslücke belegt wurde. In vielen Fällen fehlen belegbare Sachgründe für neue Maßnahmen.[5] Vielmehr entschied sich die schwarz-gelbe Landesregierung, die Möglichkeiten, die das Urteil zum BKA-Gesetz im April 2016 schuf, voll auszuschöpfen.[6] Das zu tun ist wohlgemerkt eine politische Entscheidung, es gibt keine gesetzgeberische Verpflichtung, das rechtlich gerade noch Zulässige umzusetzen und bis an seine Grenzen auszureizen.[7]

Denn entgegen der allgemeinen Wahrnehmung wird nicht in allen Bundesländern und auch nicht gleichermaßen verschärft: Weder in Thüringen noch in Berlin sieht man einen Anlass, neue Befugnisse für die Polizei zu schaffen.[8] Es handelt es sich klar um eine parteipolitische Entscheidung.

## 2. Gängige Argumentationsmuster widerlegen

Auch ohne Zutun des Gesetzgebers verändert sich die polizeiliche Praxis. Deshalb ist es „Hausaufgabe für den Gesetzgeber, dass er kontinuierlich kontrollieren muss, ob die Rechtsgrundlagen der veränderten Wirklichkeit noch gerecht werden.“[9] Beispielhaft für eine Maßnahme, die im Zuge der Digitalisierung eine erhöhte Eingriffsintensität erfährt, nennt der Kriminologe Tobias Singelnstein die Beschlagnahme: „Sie war früher nur auf Sachen gerichtet. Dass es heute möglich ist, Datenspeicher zu beschlagnahmen und auszuwerten, wo eine Vielzahl von Informationen drauf ist, hat sich der Gesetzgeber natürlich auch nicht vor Augen geführt.“[10]

Der Einsatz von Predictive-Policing-Software in NRW steht zudem beispielhaft für die Weiterverwendung einmal erhobener Daten. Ohne gesonderte Rechtsgrundlage werden soziokulturelle Daten über Kaufkraft und Bebauung genutzt, um Wahrscheinlichkeitswerte für Einbruchsdiebstahl in bestimmten Stadtteilen zu treffen, die das polizeiliche Handeln beeinflussen.[11]

Der Tatsache, dass neu geschaffene Rechtsgrundlage noch nicht absehbare Anwendungen haben

5 Beispielhaft ist hier die Aussage von Marc Lürbke, dem stellvertretenden FDP-Fraktionsvorsitzenden in NRW, der im Interview gegenüber netzpolitik.org als Grund für die Einführung der Quellen-TKÜ sagte: „Auch die Polizeigesetze anderer Bundesländer sehen Regelungen zur Quellen-TKÜ vor.“ Vgl. https://netzpolitik.org/2018/polizeigesetze-nach-kritik-verschiebt-nrw-den-ausbau-der-polizeibefugnisse-auf-herbst/ vom 20. Juni 2018.

6 Vgl. Begründung zum Gesetzentwurf: „Anlass hierfür sind insbesondere die Vorgaben des Bundesverfassungsgerichts im Zusammenhang mit dem Urteil des Bundeskriminalamtgesetzes vom 20. April 2016.“ https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMD17-2351.pdf vom 10. April 2018.

7 Es gibt keinen „Zwang, verfassungs- und europarechtliche Spielräume stets bis an die Grenze des Zulässigen auszureizen“ oder gar zu „überreizen“, schreibt der Sachverständige Markus Löffelmann, Richter am Landgericht München, in seiner Stellungnahme zum bayerischen PAG-E vom 21. März 2018.

8 Vgl. Ein Musterpolizeigesetz aus Berlin: https://netzpolitik.org/2018/ein-musterpolizeigesetz-aus-berlin/ vom 15. Oktober 2018.

9 Vgl. Interview mit dem Kriminologen Tobias Singelnstein: Der intensivste Grundrechtseingriff in der Strafprozessordnung https://netzpolitik.org/2017/interview-ueber-staatstrojaner-der-intensivste-grundrechtseingriff-in-der-strafprozessordnung/ vom 17. Juni 2017.

10 Ebd.

11 Vgl. Abschlussbericht des dreijährigen Pilotprojekts SKALA https://polizei.nrw/sites/default/files/2018-07/180628_Abschlussbericht_SKALA.PDF vom Juni 2018.

werden, wird der vorliegende Gesetzentwurf nicht gerecht. Es bedarf mindestens einer gesetzlich verankerten zeitnahen und regelmäßigen Evaluation der neuen (technologiebasierten) Maßnahmen, da zum jetzigen Zeitpunkt nicht abzusehen ist, wofür sie in Zukunft genutzt werden können.[12]

Für den Bereich der Infiltration von informationstechnischen Systemen sind zusätzliche änderungsbedürftige Aspekte für den Entwurf zu berücksichtigen: Da die geplante Überwachungssoftware einer der weitgehendsten Eingriffe in Grundrechte ist, der zur Informationsgewinnung vorstellbar ist, und zudem die technische Entwicklung schnell voranschreitet, muss für diesen Bereich eine zeitnahe Evaluation stattfinden. Sie sollte nach nur einem Jahr des Einsatzes der Staatstrojaner erfolgen.

Zudem sollte der Gesetzgeber nicht nur rechtlich, sondern auch ganz praktisch technisch prüfen lassen, welche Funktionalitäten die Überwachungssoftware vorhält und welche zum Einsatz kamen. Aufgrund der Tatsache, dass die Polizei beim Einsatz stets Gefahr läuft, dass eine Fehlfunktion des Trojaners vorkommt oder dass die Bediener der Software pflichtwidrig oder fahrlässig handeln, sollte der Einsatz umfänglich protokolliert und vor allem ausgewertet werden.

### 2.1 Gleichsetzung von technischen Maßnahmen

Die Gleichsetzung von analogen und digitalen technischen Maßnahmen ist ein gängiges Argument in der Debatte um neue polizeiliche Befugnisse.[13] Die Gleichsetzung dient dabei oftmals der Legitimation, hält aber einer Prüfung nicht immer stand.

In der vorliegenden Gesetzesbegründung werden Telekommunikationsüberwachung (TKÜ) und Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) im selben Satz genannt.[14] Tatsächlich handelt es sich um zwei völlig verschiedene Maßnahmen, die sich sowohl im technischen Vorgehen als auch in den betroffenen Rechtsgütern unterscheiden.

Anders als bei der Telekommunikationsüberwachung wird bei der Quellen-TKÜ nicht etwa eine Telefonleitung abgehört, sondern die Telekommunikation direkt auf dem Computer. Daher wird anders als bei Telefonüberwachungen nicht der Anbieter zur Ausleitung der Gespräche herangezogen, sondern das auszuspähende informationstechnische System infiltriert und dabei eine Spionagesoftware aufgebracht.

Im Falle des Einsatz eines Staatstrojaners zum Auslesen laufender Kommunikation, als sogenannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ), ist daher nicht nur das Fernmeldegeheimnis als Rechtsgut verletzt. Da „das betroffene Endgerät nach dem Aufbringen des Trojaners kompromittiert [wurde], [ist] eine sichere und vertrauenswürdige

12 Vgl. Interview mit dem Kriminologen Tobias Singelnstein: Der intensivste Grundrechtseingriff in der Strafprozessordnung, https://netzpolitik.org/2017/interview-ueber-staatstrojaner-der-intensivste-grundrechtseingriff-in-der-strafprozessordnung/ vom 17. Juni 2017.

13 Etwa die rhetorische Gleichsetzung von Durchsuchung und Online-Durchsuchung.

14 Vgl. Begründung zum Gesetzentwurf: „Bislang fehlen der Polizei die insbesondere bei der Bekämpfung des Terrorismus wichtigen Instrumente der präventiv-polizeilichen Telekommunikationsüberwachung (TKÜ) sowie der sog. Quellen-TKÜ, mit der auch auf verschlüsselte Telekommunikationsinhalte zugegriffen werden kann.“ https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMD17-2351.pdf vom 10. April 2018.

Informationsverarbeitung und -übertragung nicht mehr gewährleistet“.[15] Somit ist ein weiteres hohes Rechtsgut verletzt: das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme.

### 2.2 Öffentliche Sicherheit vs. IT-Sicherheit

In der Gesetzesbegründung wird der Einsatz von Telekommunikationsüberwachung damit begründet, dass er „insbesondere bei der Bekämpfung des Terrorismus“ wichtig sei. Diese Begründung ist in zweifacher Hinsicht zweifelhaft.

Zum einen zeigt die Erfahrung und auch die nachträglich erhobenen Zahlen, dass Drogenermittlungen der absolut häufigste Anlass zur Überwachung von Telekommunikation in der polizeilichen Praxis sind. Im Jahr 2016 war in beinahe der Hälfte der Fälle Ermittlungen auf Grund des Betäubungsmittelgesetzes Anlass für eine TKÜ.[16]

Zum anderen wird durch die Einführung der Quellen-TKÜ mit der Begründung die öffentliche Sicherheit zu stärken, gleichzeitig die Gefährdung der allgemeinen IT-Sicherheit billigend in Kauf genommen. Öffentliche Sicherheit und IT-Sicherheit werden gegen einander ausgespielt, was zugunsten der öffentlichen Sicherheit ausfällt.[17]

## 3. Einzelmaßnahmen

### Gefahrenkategorien (§ 8)

Die Streichung des § 8 Abs. 4 und 5 PolG-E, der „drohenden Gefahr“, ist ausdrücklich zu begrüßen.

### TKÜ und Quellen-TKÜ (§ 20c)

Der § 20c PolG-E ist in zweifacher Hinsicht irreführend.

Erstens sollten Telekommunikationsüberwachung und Quellen-TKÜ getrennt betrachtet werden. So schreibt Nikolaos Gazeas in seiner Stellungnahme für die erste Ausschuss-Anhörung: „Die systematische Einordnung der Quellen-TKÜ gemeinsam mit der konventionellen TKÜ in § 20c PolG-E suggeriert, dass es sich um einen vergleichbaren Eingriff handele. Bezogen auf die Eingriffsintensität steht sie in Wahrheit jedoch der Online-Durchsuchung nahe, da beide Maßnahmen die Infiltration des Systems erforderten.“[18] Zweitens wird die Telekommunikationsüberwachung in der Gesetzesbegründung mit dem besonders schweren Fall des Terrorismus gerechtfertigt, tatsächlich lässt Absatz 1 Nummer 1 jedoch eine Anwendung ohne

15 Vgl. Stellungnahme des Chaos Computer Clubs (CCC) https://www.ccc.de/system/uploads/252/original/CCC-staatstrojaner-hessen.pdf vom 4. Februar 2018.
16 Vgl. Auch 2016 waren Drogendelikte häufigster Überwachungsgrund https://netzpolitik.org/2017/auch-2016-waren-drogendelikte-haeufigster-u... vom 2. November 2017.
17 Vgl. auch: Bundeshacker im Verzug: „Zitis ist […] der Beleg dafür, dass die Bundesregierung in letzter Konsequenz Innere Sicherheit und IT-Sicherheit für Gegensätze hält.“ https://www.zeit.de/digital/datenschutz/2017-08/zitis-eroeffnung-thomas-de-maiziere-bundeshacker vom 30. August 2017.
18 Vgl. Stellungnahme zum Sechsten Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen von Nikolaos Gazeas https://www.landtag.nrw.de/Dokumentenservice/portal/WWW/dokumentenarchiv/Dokument/MMST17-662.pdf vom Juni 2018.

jeglichen Terrorismusbezug zu.[19]

**Quellen-TKÜ**

Der staatlichen Einsatz von Spähsoftware hat zum Ziel, informationstechnische Systeme dauerhaft zu infiltrieren, um Kommunikations- oder andere Daten auszuleiten. Im aktuellen Änderungsantrag wurde hier der Zusatz „laufende“ Kommunikation ergänzt. Die Ergänzung ist begrüßenswert, da das der Rechtsprechung des Bundesverfassungsgerichts entspricht und eine Auswertung gespeicherter Kommunikationsinhalte ausgeschlossen wird. Im Urteil des Bundesverfassungsgericht zum BKA-Gesetz heißt es: „Das Gesetz lässt jedenfalls keinen Zweifel, dass eine Quellen-Telekommunikationsüberwachung nur bei einer technisch sichergestellten Begrenzung der Überwachung auf die *laufende* Telekommunikation erlaubt ist.“[20]

Zugleich wirft dieser Zusatz die Sinnhaftigkeit des Paragrafen auf, da es ganz praktisch keine rechtskonforme, einsatzbereite Software zu diesem Zweck gibt.[21] Da „alle bisherigen Versuche, Staatstrojaner für deutsche Behörden zu entwickeln und einzusetzen, entweder gescheitert oder als rechtswidrig eingestuft worden“ sind.[22] Der Grund liegt auf der Hand: Das Ziel einer Quellen-TKÜ ist es, vor die Verschlüsselung zu kommen, also die Nachricht noch vor ihrer Verschlüsselung auf dem Endgerät abzufangen.

Doch eine Kommunikation im engeren Sinne liegt erst vor, wenn die entsprechende Nachricht verschickt wurde, also bereits verschlüsselt ist. Ganz praktisch kann man sich das anhand einer E-Mail vorstellen. Beim Text einer E-Mail handelt es sich zunächst um Inhaltsdaten. Es ist kaum möglich festzustellen, ob ein Entwurf für eine E-Mail tatsächlich verschickt werden wird oder möglicherweise als Entwurf auf dem Endgerät verbleibt oder gelöscht wird. Erst nach dem Versand, und damit unmittelbar nach der Verschlüsselung, handelt es sich um Inhaltsdaten einer laufenden Kommunikation.

Ob sich das Überwachen tatsächlich auf die laufende Kommunikation beschränken lässt, ist allerdings aus technischen Gründen zweifelhaft. Das Bundesverfassungsgericht schreibt zwar in seinem Urteil ausdrücklich, dass die praktische Anwendbarkeit die Verfassungsmäßigkeit eines solchen Maßnahme nicht unmittelbar betrifft: „Ob oder wie sich durch technische Maßnahmen sicherstellen lässt, dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet wird, betrifft die Anwendung der Norm, nicht aber ihre Gültigkeit.“[23] Dabei

19 Vgl. Stellungnahme zum Sechsten Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen von der Landesbeauftragten für den Datenschutz, Helga Block https://www.landtag.nrw.de/Dokumentenservice/portal/WWW/dokumentenarchiv/Dokument/MMST17-645.pdf vom 30. Mai 2018.

20 Vgl. BVerfG, Urteil des Ersten Senats zum BKA-Gesetz, Rn 234 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html vom 20. April 2016.

21 Zu den verschiedenen Modellen des Staatstrojaners vgl. Geheime Dokumente: Das Bundeskriminalamt kann jetzt drei Staatstrojaner einsetzen https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/ vom 26. Juni 2018.

22 Vgl. Stellungnahme zum Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen durch den Chaos Computer Club (CCC) https://www.ccc.de/system/uploads/252/original/CCC-staatstrojaner-hessen.pdf vom 4. Februar 2018.

23 Vgl. BVerfG, Urteil des Ersten Senats zum BKA-Gesetz, Rn 234

berücksichtigten die Richter allerdings, dass sämtliche IT-Experten außerhalb der Ermittlungsbehörden in ihren schriftlichen Stellungnahmen einhellig die Ansicht vertraten und begründeten, dass die theoretischen Anforderungen an eine Quellen-TKÜ praktisch in technischer Hinsicht nicht zu erfüllen sind.

Daher stellt das Verfassungsgericht klar: „Sollten zum gegenwärtigen Zeitpunkt diese Anforderungen nicht erfüllbar sein, liefe die Vorschrift folglich bis auf weiteres leer.“[24] Da es derzeit keine entsprechende Software zur Quellen-TKÜ gibt, dürfte der § 20c PolG-E in der polizeilichen Praxis nicht zur Anwendung kommen.

Ganz grundsätzlich wird durch die Entwicklung von Staatstrojanern die (IT-)Sicherheit aller Bürgerinnen und Bürger gefährdet: „Da für Trojaner Sicherheitslücken benötigt werden, müssen diese gefunden oder erworben werden. Solche Sicherheitslücken, die absichtlich geheimgehalten werden, stellen eine erhebliche Gefährdung für kritische Infrastrukturen, Behörden, Wirtschaft und Privatpersonen dar.“[25] Der Chaos Computer Club hat in einer Stellungnahme die technische Realität und die gesellschaftlichen Implikationen des staatlichen Einsatzes von Spähsoftware treffend zusammengefasst.[26] Aufgrund dieser „erheblichen und strukturellen Risiken für die IT-Sicherheit [ist der Einsatz von Schadsoftware durch den Staat] grundsätzlich abzulehnen.“[27] Das ergibt sich nicht zuletzt auch aus der Cyber-Sicherheitsstrategie für Deutschland, die explizit die Förderung der IT-Sicherheit vorantreiben soll[28] und gerade nicht das Hintertreiben von IT-Sicherheitsmaßnahmen durch das heimliche Ausnutzen von Sicherheitslücken.

Der Gesetzgeber sollte sich zudem bewusst machen, dass es sich um eine heimliche Maßnahme handelt, die weitere heimliche Maßnahmen nach sich zieht. So hat die Justizministerkonferenz im Juni 2018 verlauten lassen, dass es in der Praxis nicht immer leicht ist, die Schadsoftware heimlich auf den Computer der verdächtigen Person zu spielen. Deshalb sollte der Polizei die Möglichkeit geschaffen werden, heimlich in die Wohnung einzudringen, um die Schadsoftware zur Überwachung unbemerkt auf dem Computer zu installieren:

„[Die Justizministerinnen und Justizminister] sind der Auffassung, dass die derzeit zulässigen Möglichkeiten zur Aufbringung der Software auf dem informationstechnischen System des Betroffenen mit erheblichen rechtlichen und tatsächlichen Problemen behaftet sind. Um die neuen Ermittlungsmaßnahmen effektiv und praxistauglich einsetzen zu können, erachten die Justizministerinnen und Justizminister die Schaffung eines gesetzlichen Betretungsrechts zum Zwecke der Aufbringung der Software als zielführende Alternative.“[29]

https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html vom 20. April 2016.

24 Ebd.

25 Vgl. Stellungnahme zum Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen durch den Chaos Computer Club (CCC) https://www.ccc.de/system/uploads/252/original/CCC-staatstrojaner-hessen.pdf vom 4. Februar 2018.

26 Ebd.

27 Ebd.

28 Vgl. Cyber-Sicherheitsstrategie für Deutschland: http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyber-Sicherheitsstrategie/cyber-sicherheitsstrategie_node.html vom 30. April 2017.

29 Vgl. Beschluss der Justizministerkonferenz in Eisenach http://www.jm.nrw.de/JM/jumiko/beschluesse/2018/Fruehjahrskonferenz_2018/II-8-RP---Ergaenzung-der-

**Elektronische Fußfessel (§ 34c)**
Die Aufenthaltsüberwachung mittels elektronischer Fußfessel soll unter anderem als Maßnahme zur Verhütung drohender terroristischer Straftaten und in Fällen von häuslicher Gewalt erlaubt werden.

Die Anordnung eines Aufenthaltsverbots und dessen Durchsetzung mittels elektronischer Fußfessel kann höchstens sinnvoll sein in Fällen, in denen der Zeitraum übersehbar und die bedrohte Person und ihr Wohnort bekannt ist.[30] Im Gesetzesentwurf ist die Maßnahme jedoch langfristig konzipiert: Sie beginnt bei drei Monaten und ist endlos um jeweils drei Monate verlängerbar, eine Höchstdauer ist nicht festgelegt. Folglich dient sie nicht der Abwehr einer konkreten Gefahr. Vielmehr handelt es sich um eine personenbezogene vorbeugende Maßnahme.[31]

Zur Verhinderung (der Vorbereitung) einer terroristischer Straftaten ist die Maßnahme völlig ungeeignet.[32] Denn eine terroristische Straftat und die Vorbereitung dazu können überall stattfinden. Ihrer Sache nach findet sie sogar besonders oft an alltäglichen und viel besuchten Orten statt.[33] Ein Aufenthaltsverbot hingegen kann nicht derart großflächig und allgemein (etwa für jedes öffentliche Verkehrsmittel) ausgesprochen werden.

Da es sich um eine vorbeugende Maßnahme handelt, sind notwendigerweise unschuldige Bürgerinnen und Bürger betroffen. Es muss damit gerechnet werden, dass auch Bürgerinnen und Bürger betroffen sein werden, die in der Zukunft keine Straftat begehen würden. Ein mildes Mittel ist die elektronische Fußfessel unterdessen nicht: Die dauerhafte Kontrolle durch Überwachung des Standorts ist belastend für die betroffene Person und das Tragen einer sichtbaren elektronischen Fußfessel stigmatisierend.[34]

**Überwachung des öffentlichen Raums (§ 15a)**
Der Gesetzentwurf ermöglicht die langfristige Ausweitung der Videobeobachtung im öffentlichen

Regelungen-zur-Quellen-TKUe-und-zur-Online-Durchsuchung-um-ein-Betretungsrecht.pdf vom 7. Juni 2018.

30 Vgl. Jochen Gladow von der Beratungsstelle „Stop Stalking“ sagt: „Wer den Täter nicht festsetzen kann, muss das Opfer schützen“ https://www.sueddeutsche.de/panorama/interview-zu-stalking-wer-den-taeter-nicht-festsetzen-kann-muss-das-opfer-schuetzen-1.3808731 vom 29. Dezember 2017.

31 Vgl. Die Grenzen der elektronischen Fußfessel: Die elektronische Fußfessel wurde in Deutschland zuerst debattiert, nachdem der Europäische Gerichtshof für Menschenrechte 2009 die sogenannte Sicherungsverwahrung für unzulässig erklärte. Die elektronische Fußfessel sollte als Ersatz zum Freiheitsentzug dienen. „Fußfessel statt Knast“ https://www.deutschlandfunk.de/ueberwachung-die-grenzen-der-elektronischen-fussfessel.1148.de.html?dram:article_id=278098 vom 20. Februar 2014.

32 Vgl. BKA-Gesetz: Bundesregierung beschließt elektronische Fußfesseln für „Gefährder“. https://netzpolitik.org/2017/bka-gesetz-de-maiziere-kuendigt-novellierung-an/ vom 1. Februar 2017.

33 Vgl. Fußfessel für Gefährder – „Gefahr, dass wir immer mehr die Grundrechte stutzen“ https://www.deutschlandfunk.de/fussfessel-fuer-gefaehrder-gefahr-dass-wir-immer-mehr-die.694.de.html?dram:article_id=377894 vom 1. Februar 2017.

34 Vgl. Elektronische Fußfessel – Überwachen und Resozialisieren: Gunda Wößner vom Max-Planck-Institut für ausländisches und internationales Strafrecht hat das Modellprojekt des Justizministeriums Baden-Württemberg begleitet: „Fast alle Probanden haben berichtet, dass sie in irgendeiner Form versucht haben zu verbergen, dass sie diese Fußfessel tragen. Im Sommer lange Hosen anziehen oder doppelte Socken drüber ziehen, damit es nicht so auffällt. Da gab es schon einen relativ großen Leidensdruck.“ https://www.deutschlandfunkkultur.de/elektronische-fussfessel-ueberwachen-und-resozialiseren.976.de.html?dram:article_id=416586 vom 26. April 2018.

Raum. Geplant ist, aufgrund von Erfahrungswerten sowie Prognosen Videobeobachtung im öffentlichen Raum durchzuführen.

Die Eignung der Videobeobachtung zur Verhinderung und Aufklärung von Straftaten ist höchst fragwürdig. Punktuelle Videobeobachtung *verdrängt* Kriminalität lediglich an andere Orte. Zudem gilt die vom Bundesverfassungsgericht angeregte „*Überwachungsgesamtrechnung*“. Die Bundesverfassungsrichter haben 2005 befunden, dass man „additive Grundrechtseingriffe“ mitbedenken muss und nicht nur die einzelne Maßnahme, um eine „Rundumüberwachung“ zu verhindern.[35]

## 4. Fazit

Der aktuelle Änderungsantrag hat sinnvolle Korrekturen gegenüber dem ersten Gesetzentwurf eingefügt.

Insgesamt werden jedoch zu hohe Erwartungen an den Nutzen der freiheitsentziehenden und ausforschenden Maßnahmen der Polizei gestellt. Um das Problem an der Wurzel zu packen, müssen vielmehr Akteure der Jugend- und Sozialarbeit einbezogen werden. Hier wäre ein offener, interdisziplinärer Blick auf Präventionsangebote, etwa mithilfe von Sozialprogrammen, Bildung und Stadt- und Raumplanung angebracht. Das Polizeigesetz ist nicht die angemessene Stellschraube, als die es gern dargestellt wird.

**Technische Maßnahmen im präventiven Bereich**

Der Gesetzgeber setzt in der präventiven Polizeiarbeit stark auf technische Maßnahmen: Aufenthaltsüberwachung mittels elektronische Fußfessel, Vorhersage von Einbruchsdiebstahl mittels Predictive-Policing-Software und Videobeobachtung im öffentlichen Raum.

Das Problem: Vorbeugen kann man unendlich früh. Man kann immer noch früher überwachen, ausforschen und wegsperren. Auch technisch wird in den nächsten Jahren noch mehr möglich sein: statistisches Profiling, Gesichtserkennung und weitere biometrische Verfahren, Bewegungsprofile.

Folglich muss der Gesetzgeber sich selbst eine Grenze setzen, bis wohin präventive Maßnahmen reichen dürfen. Es darf nicht einfach gemacht werden, was vielleicht technisch möglich wäre. Denn vorbeugende Maßnahmen führen dazu, dass rechtskonformes Verhalten plötzlich als Grundlage für einen Verdacht und folglich für freiheitsentziehende Maßnahmen ausreichen. Damit werden polizeiliche Maßnahmen nicht mehr vorhersehbar, die Rechtssicherheit geht verloren.

**Empfehlung**

Insgesamt fehlt es an einem Bewusstsein für IT-Sicherheit. Die zur Quellen-TKÜ notwendige Entwicklung von Schadsoftware birgt erhebliche Risiken für die IT-Sicherheit aller Bürgerinnen und Bürger, sie ist deshalb grundsätzlich abzulehnen.

35 Vgl. Überwachungsgesamtrechnung: Vorratsdatenspeicherung ist der Tropfen, der das Fass zum Überlaufen bringt https://netzpolitik.org/2015/ueberwachungsgesamtrechnung-vorratsdatenspeicherung-ist-der-tropfen-der-das-fass-zum-ueberlaufen-bringt/ vom 9. Juni 2015.

Die Eignung von technischen Maßnahmen ist zu prüfen. Die Aufenthaltsüberwachung mittels elektronischer Fußfessel ist – im präventiven Bereich – kein mildes Mittel und zudem schlicht nicht geeignet, terroristische Anschläge vorzubeugen. Auch mit Blick auf Videobeobachtung sollte der Gesetzgeber sich hier zurückbesinnen auf geeignetere und mildere Mittel.

Darüber hinaus ist eine gesetzlich verankerte zeitnahe Evaluierung der neuen Maßnahmen dringend zu empfehlen. Für die technischen Maßnahmen zur Infiltration von informationstechnischen Systemen ist diese Evaluierung zudem erheblich zu erweitern.