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 saarländischen Landtag, Innenausschuss

Entwurf eines Gesetzes zur Neuregelung der polizeilichen Datenverarbeitung im Saarland
Drs. 16/1180

Berlin, den 6. Mai 2020

1. Vorbemerkung

Am Ende der Stellungnahme steht eine Zusammenfassung aller Empfehlungen mit konkreten Formulierungsvorschlägen.

NETZPOLITIK.ORG
DIGITALE SELBSTVERTEIDIGUNG

2. Einordnung: Neue polizeiliche Befugnisse zu schaffen, ist eine politische Entscheidung.

Der vorliegende Gesetzentwurf steht im Kontext einer Welle von Novellierungen der Länderpolizeigesetze in Deutschland und ist sichtlich von diesen geprägt. In der Berichterstattung bekamen in den letzten beiden Jahren jene Landesregierungen besonders viel Aufmerksamkeit, die durch ihre umfangreichen Ausweitungen der polizeilichen Befugnisse im präventiven Bereich – bis hin zum „gesetzgeberischen Exzess“ – hervortraten: Bayern, Baden-Württemberg, Sachsen, Niedersachsen und NRW.[1] Motor hierfür sind die von der Union geführten Innenministerien.[2]

Entgegen der allgemeinen Wahrnehmung **wird jedoch nicht in allen Bundesländern und auch nicht gleichermaßen das Polizeirecht verschärft**: Weder in Thüringen noch in Berlin sieht man derzeit einen Anlass, neue Befugnisse für die Polizei zu schaffen.[3] Es handelt sich klar um eine parteipolitische Entscheidung.

Im Saarland soll nun die „drohende Gefahr“ als niedrigere polizeiliche Eingriffsschwelle eingeführt werden. Damit würde sich der saarländische Gesetzgeber entscheiden, die Möglichkeit, die das Urteil zum BKA-Gesetz im April 2016 schuf, voll auszuschöpfen.[4] 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.[5]

Richtig ist, dass das Saarland die europäische JI-Richtlinie in Landesrecht umzusetzen muss. Das hätte bereits im Mai 2018 geschehen sollen und ist längst überfällig. Der Ausbau der polizeilichen Befugnisse hingegen –etwa im Bereich Videoüberwachung und Eingriffen bei „drohender Gefahr“– sind hingegen politische Entscheidungen, die gründlich abgewogen werden sollten.

1 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.

2 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.

3 In Berlin soll ein*e Polizeibeauftragte*r eingeführt werden. Auf die Ausweitung der Videoüberwachung und die elektronische Fußfessel wird hingegen verzichtet. Vgl. https://taz.de/Polizeigesetz-Berlin/!5646170/ vom 15. Dezember 2019

4 „Auch wenn er die Begrifflichkeiten vermeidet, so ist doch erkennbar, dass der Gesetzentwurf die Ausführungen des BVerfG im Urteil vom 20. April 2016 - 1 BvR 966/09 – zu den Eingriffsvoraussetzungen bei einer drohenden Gefahr für sich geltend machen will“, schreibt die Landesbeauftragte für den Datenschutz in ihrer Stellungnahme zum SpolDVG-E vom 25. Oktober 2019.

5 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.

3. Einzelmaßnahmen im SPolDVG-E

Im Folgenden werden ausgewählte Einzelmaßnahmen kommentiert. Der Fokus liegt auf jenen Befugnissen, die neu eingeführt werden sollen. Am Ende steht eine Zusammenfassung aller Empfehlungen mit konkreten Formulierungsvorschlägen.

DIE ELEKTRONISCHE FUßFESSEL (§ 38)

Seit etwa zehn Jahren wird die elektronische Fußfessel in Deutschland zur Überwachung von verurteilten Straftäter*innen nach Entlassung aus der Haft diskutiert und auch angewendet. In solchen Konstellationen gibt es stets eine rechtskräftige Verurteilung und einen direkten Kontakt zu den Betroffenen, es gilt: „Fußfessel statt Knast“.[6]

Im Saarland sollen nun Personen, die keine Straftat begangen haben, sondern lediglich verdächtigt werden gefährlich zu sein, auf diese Weise rund um die Uhr überwacht werden. Da es sich um eine vorbeugende Maßnahme handelt, muss damit gerechnet werden, dass auch solche Bürgerinnen und Bürger betroffen sein werden, die in der Zukunft keine Straftat begehen würden.

Eine konkrete Gefahr durch die Person braucht nicht vorzuliegen, die Maßnahme ist durch den Gesetzgeber langfristig konzipiert: Sie beginnt bei drei Monaten und ist endlos um jeweils drei Monate verlängerbar, eine Höchstdauer ist nicht festgelegt.

Die Anordnung eines Aufenthaltsverbots hingegen 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 sind, beispielsweise bei Stalking**.[7]

Die elektronische Fußfessel ist nicht geeignet, um terroristische Straftaten zu verhindern. 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.[8] Ein Aufenthaltsverbot hingegen kann nicht derart großflächig und allgemein (etwa für jedes öffentliche Verkehrsmittel) ausgesprochen werden. Ohne ein Aufenthaltsverbot läuft die Überwachung mittels elektronischer Fußfessel jedoch ins Leere.

Ein mildes Mittel ist die elektronische Fußfessel nicht: Die dauerhafte Kontrolle durch Überwachung des Standorts ist belastend für die betroffene Person und das Tragen einer sichtbaren

6 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. Vgl. Die Grenzen der elektronischen Fußfessel https://www.deutschlandfunk.de/ueberwachung-die-grenzen-der-elektronischen-fussfessel.1148.de.html?dram:article_id=278098 vom 20. Februar 2014.

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

8 Um nur ein Beispiel zu nennen: 2016 fand ein Attentat in einer Kirche statt, einer der Angreifer trug dabei eine elektronische Fußfessel. Vgl. https://www.faz.net/aktuell/politik/ausland/angreifer-in-franzoesischer-kirche-trug-elektronische-fussfessel-14359132.html vom 26. Juli 2016.

elektronischen Fußfessel stigmatisierend.[9]

ANLASSLOSE VIDEOÜBERWACHUNG (§ 32 Abs. 1 und 2)

Der Gesetzentwurf ermöglicht die langfristige Ausweitung der Videoüberwachung im öffentlichen Raum. Geplant ist, aufgrund von Erfahrungswerten sowie Prognosen dauerhaft Kameras an bestimmten Orten zu installieren und vermehrt Veranstaltungen zu filmen.

Derzeit werden Personen, die sich rund um die Johanneskirche in Saarbrücken aufhalten, gefilmt und beobachtet. Am Hauptbahnhof in Saarbrücken beginnt die Videobeobachtung demnächst.

Zukünftig könnten weitere Bahnhöfe und Plätze rund um die Uhr abgefilmt werden mit der Begründung, dass es an diesem Objekt oder an einem anderen Objekt „dieser Art“ wiederholt zu Straßen- und Betäubungsmittelkriminalität kam. Bei Veranstaltungen würde die Annahme genügen, dass Ordnungswidrigkeiten begangen werden könnten.

In der Halbzeitbilanz der Landesregierung steht, dass das Ziel der Videoüberwachung ist, das „subjektiven Sicherheitsgefühls“ zu stärken und die objektive Sicherheitslage zu verbessern.[10] Tatsächlich sind objektive Effekte der Videoüberwachung auf die Kriminalität nicht wissenschaftlich belegt. Das Kriminologische Forschungsinstitut Niedersachsen (KFN) schreibt mit Blick auf das nordrhein-westfälische Polizeigesetz, dass "der wissenschaftliche Nachweis eines allgemein kriminalitätsreduzierenden Effekts der Videoüberwachung bisher nicht überzeugend geführt werden“ konnte.[11] Die Befundlage bezüglich des Nutzens für die polizeiliche Ermittlung und Aufklärung ist laut des kriminologischen Forschungsberichts ebenfalls uneindeutig.[12]

Punktuelle Videoüberwachung führt zu Verdrängung von Kriminalität, als zu ihrer Vorbeugung. Um der sogenannten Straßenkriminalität zu begegnen, sollten 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.

QUELLEN-TELEKOMMUNIKATIONSÜBERWACHUNG (§ 35 Abs. 2)

Im vorliegenden Gesetzentwurf werden Telekommunikationsüberwachung (TKÜ) und Quellen-

9 „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.“ sagt Gunda Wößner vom Max-Planck-Institut für ausländisches und internationales Strafrecht, die das Modellprojekt des Justizministeriums Baden-Württemberg begleitet hat. Vgl. https://www.deutschlandfunkkultur.de/elektronische-fussfessel-ueberwachen-und-resozialiseren.976.de.html?dram:article_id=416586 vom 26. April 2018.

10 Halbzeitbilanz der Landesregierung. https://www.saarland.de/dokumente/res_stk/Halbzeitbilanz_2019_Inhverz.pdf vom 19. November 2019

11 Forschungsbericht des Kriminologisches Forschungsinstitut Niedersachsen (KFN). https://kfn.de/wp-content/uploads/Forschungsberichte/FB_143.pdf vom Juni 2018

12 Ebd.

Telekommunikationsüberwachung (Quellen-TKÜ) im selben Paragrafen geregelt. Diese Gleichsetzung hält jedoch einer Prüfung nicht stand. Tatsächlich handelt es sich um zwei völlig verschiedene Maßnahmen, die sich sowohl im technischen Vorgehen als auch in den betroffenen Rechtsgütern unterscheiden.

Zur Klarstellung wäre es empfehlenswert, die Telekommunikationsüberwachung (TKÜ) und Quellen-TKÜ getrennt voneinander zu behandeln.[13] Eine vergleichbare Regelung findet sich im Hamburgischen Gesetz über die Datenverarbeitung der Polizei.[14]

Anders als bei der Telekommunikationsüberwachung wird bei der Quellen-TKÜ nicht eine Telefonleitung abgehört, sondern die Telekommunikation direkt auf dem Endgerät. 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 Einsatzes 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 Informationsverarbeitung und -übertragung nicht mehr gewährleistet“.[15] Somit ist ein weiteres hohes Rechtsgut verletzt: das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme.

Die Regelung weist weitergehend schwere inhaltliche Mängel auf. **Es wird nicht klar, ob ausschließlich laufende oder auch bereits gespeicherte Kommunikation ausgelesen werden soll**. Der Gesetzestext und seine Begründung widersprechen sich hier. In der Begründung steht, dass: Neben der „laufenden Kommunikation *auch die bereits abgeschlossene und gespeicherte [Kommunikation] überwacht und aufgezeichnet werden darf, soweit diese im überwachten System gespeichert sind.*“ Das entspräche einer Online-Durchsuchung.

Der saarländische Gesetzgeber muss sich jedoch entscheiden, ob er ausschließlich laufende oder auch gespeicherte Kommunikationsinhalte auslesen möchte. In der Rechtsprechung des Bundesverfassungsgerichts ist eine Auswertung gespeicherter Kommunikationsinhalte ausgeschlossen. Lediglich das Ausleiten der laufenden Kommunikation ist unter strengen Voraussetzungen zulässig.

13 „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..“ schreibt Nikolaos Gazeas. Vgl. Stellungnahme zum Sechsten Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen https://www.landtag.nrw.de/Dokumentenservice/portal/WWW/dokumentenarchiv/Dokument/MMST17-662.pdf vom Juni 2018.

14 Konkret geht es um PolDVG HH § 23 (TKÜ) und § 24 (Quellen-TKÜ).

15 Vgl. Stellungnahme des Chaos Computer Clubs (CCC) https://www.ccc.de/system/uploads/252/original/CCC-staatstrojaner-hessen.pdf vom 4. Februar 2018.

Im Urteil des Bundesverfassungsgerichts 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.**“[16]

Eine laufende 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 Whatsapp-Nachricht vorstellen. Beim Text einer Nachricht handelt es sich aus technischer Sicht zunächst um Inhaltsdaten. Es ist kaum möglich festzustellen, ob ein Entwurf für eine Nachricht 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 aus technischen Gründen zweifelhaft. Das Bundesverfassungsgericht schreibt zwar in seinem Urteil ausdrücklich, dass die praktische Anwendbarkeit die Verfassungsmäßigkeit einer 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.“[17] Dabei 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.“[18] Da es derzeit keine entsprechende Software zur Quellen-TKÜ gibt, dürfte der § 35 Abs. 2 SPolDVG-E n 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“.[19]

Aufgrund der erheblichen Risiken für die IT-Sicherheit ist das Offenhalten und heimliche

16 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.
17 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.
18 Ebd.
19 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.

Ausnutzen von Sicherheitslücken grundsätzlich abzulehnen.[20] Das ergibt sich nicht zuletzt auch aus der Cyber-Sicherheitsstrategie für Deutschland, die explizit die Förderung der IT-Sicherheit vorantreiben soll.[21] **Der Gesetzgeber sollte daher festschreiben, dass nur bereits bekannte Sicherheitslücken verwendet werden dürfen.**[22]

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.“

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.

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.

DIE BODYCAM (§ 32 Abs. 3)

Bereits heute besitzt die saarländische Polizei 66 Bodycams, nun wird eine eigenständige Rechtsgrundlage für deren Einsatz geschaffen. Ziel dieser Maßnahme ist es, Angriffe auf Beamt*innen vorzubeugen und ggf. Videomaterial zur Strafverfolgung zu verwenden.

Ausdrücklich erlaubt wird den saarländischen Polizist*innen das Filmen in Wohnungen. Die Landesbeauftragten für Datenschutz und Informationsfreiheit weist darauf hin, dass „bislang lediglich die Bundesländer Nordrhein-Westfalen und Bayern den Einsatz von Körperkameras in

20 Ebd.
21 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.
22 „Erfolgt der Einsatz technischer Mittel unter Ausnutzung von Sicherheitslücken in der Hard- und Software des informationstechnischen Systems, so dürfen nur solche Sicherheitslücken verwendet werden, die dem jeweiligen Hersteller bereits bekannt sind.“ schreibt die Landesbeauftragten für Datenschutz und Informationsfreiheit in ihrer Stellungnahme zum SPolDVG-E. Vom 25. Oktober 2019.

Wohnungen kodifiziert haben.“[23]

An den Nutzen von Bodycams als Beweismittel sollten keine hohen Erwartungen geknüpft werden. Denn Bodycams können „niemals die ganze Geschichte erfassen, schon allein, da sie keine 360-Grad-Sicht erlauben. Daher ist es zweifelhaft, ob Bodycams tatsächlich dazu taugen, eine beweissichere Dokumentation der Vorgänge möglich zu machen.“[24]

Bislang fehlt die konsequente Einbeziehung der Perspektive von Betroffenen. In der Sachverständigenanhörung im Bundestag zur Einführung von Bodycams für die Bundespolizei[25] sagte der Kriminologe Andreas Ruch von der Ruhr-Universität Bochum: „Gewalt kann man nur interaktiv und kommunikativ begreifen […] **Deswegen können und müssen Aufnahmen von Bodycams auch dazu genutzt werden, um polizeiliches Fehlverhalten zu dokumentieren.**“[26]

Betroffene müssen ein Recht auf Einsicht in das Videomaterial bekommen, um ggf. Polizeigewalt anzufechten. Dafür muss sichergestellt sein, dass Aufnahmen nicht manipuliert oder gelöscht werden können.

Eine solche Regelung findet sich unter anderem im nordrhein-westfälischen Polizeigesetz, dort heißt es „auf Verlangen der betroffenen Person für die Überprüfung der Rechtmäßigkeit von aufgezeichneten polizeilichen Maßnahmen“ wird die Löschung der Aufnahmen aufgeschoben.[27] Zudem ist dort festgehalten, dass Aufzeichnungen „verschlüsselt sowie manipulationssicher gefertigt und aufbewahrt“ werden müssen.[28]

Auch aus dem vom saarländischen Innenministerium in Auftrag gegeben Rechtsgutachten[29] ergibt sich weiterer Regelungsbedarf:

- Es fehlt eine umfassende Hinweispflicht.[30]
- **Es fehlt eine eindeutige Regelung zum Pre-Recording.** Eine vergleichbare Regelung findet sich im niederächsischen Polizeigesetz, dort heißt es: Die Bodycams „dürfen auch im Bereitschaftsbetrieb Aufzeichnungen anfertigen, diese sind automatisch nach höchstens 30 Sekunden zu löschen, es sei denn, es beginnen in dieser Zeitspanne Aufzeichnungen. In

23 Konkret geht es um die § 15c PolG NRW, und Art. 33 Abs. 4 S. 3 BayPAG. Vgl. Stellungnahme der Landesbeauftragten für Datenschutz und Informationsfreiheit zum SPolDVG-E vom 25. Oktober 2019.
24 Kriminologen Andreas Ruch von der Ruhr-Universität Bochum. Vgl.: Lass Dich überwachen: Die neue „informationelle Sozialpflichtigkeit“, https://netzpolitik.org/2017/lass-dich-ueberwachen-die-neue-informationelle-sozialpflichtigkeit/ vom 7. März 2017.
25 Vgl. Gesetzentwurf der Bundesregierung zum Einsatz von Bodycams, http://dip21.bundestag.de/dip21/btd/18/109/1810939.pdf vom 23. Januar 2017.
26 Vgl. Lass Dich überwachen: Die neue „informationelle Sozialpflichtigkeit“, https://netzpolitik.org/2017/lass-dich-ueberwachen-die-neue-informationelle-sozialpflichtigkeit/ vom 7. März 2017.
27 PolG NRW § 15c Abs. 4
28 PolG NRW § 15c Abs. 3:
29 Rechtsgutachten von Markus Thiel und Knud Dietrich vom 18. März 2019.
30 In der Begründung zum Gesetzentwurf steht, dass „der Umfang der Hinweispflicht“ hier niedriger sei, sodass „auch QR-Codes o. ä. verwenden zu können. Die umfassende Informationspflicht ist bei Einsatz von Body-Cams nicht in dem Maße erforderlich, da hier Vollzugskräfte und den Betroffene in direkter Interaktion stehen.“

diesem Fall werden die Aufzeichnungen erst gemeinsam mit den Aufzeichnungen gelöscht.“[31]

- **Es fehlt ein Verweis auf die Bedeutung der Maßnahme für Berufsgeheimnisträger*innen und den Kernbereichsschutz.** Eine vergleichbare Regelung findet sich im nordrhein-westfälischen Polizeigesetz. Dort heißt es: „Aufzeichnungen sind unzulässig in Bereichen, die der Ausübung von Tätigkeiten von Berufsgeheimnisträgern (…) dienen.“[32] und „Die Aufzeichnung personenbezogener Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, ist unzulässig“[33]
- Es fehlt eine Regelung zur unabhängige Evalueriung des tatsächlichen Nutzens der Maßnahme zur Vorbeugung von Angriffen.

BERUFSGEHEIMNISTRÄGER*INNEN (§ 41)

Berufsgeheimnisträger*innen werden im vorliegenden Gesetzesentwurf in ein *Zweiklassensystem* einsortiert. Geistliche genießen in der Folge einen höheren Schutz als Mitarbeiterinnen und Mitarbeiter von Beratungsstellen. Das ist nicht zeitgemäß.

In § 41 wird der besondere Schutz vor Überwachung für „zeugnisverweigerungsberechtigte Personen“ geregelt. Allerdings nicht für alle gleichermaßen: Rechtsanwält*innen, Mitglieder des Bundestags und der Landtage sowie Geistliche genießen einen absoluten Schutz. Davon explizit ausgenommen sind Ärzt*innen, Psychotherapeut*innen, Mitarbeiter*innen von Beratungsstellen und Journalist*innen. Für sie gilt lediglich ein relatives Verwertungsverbot. Demnach ist eine Überwachung nicht per se unzulässig, sondern ist im Rahmen der Verhältnismäßigkeit zu prüfen.

Die rechtliche Zulässigkeit[34] genügt nicht als Begründung. **Das geschaffene Zweiklassensystem unter den Berufsgeheimnisträger*innen ist nicht zeitgemäß.** Es gibt keinen ersichtlichen Grund, Geistliche im Rahmen des Berufsgeheimnisses besser zu stellen als Mitarbeiterinnen und Mitarbeiter von Beratungsstellen. Schließlich sollte es **für den Schutz der Vertraulichkeit keinen Unterschied machen, ob sich eine Person in einer Notsituation entscheidet, sich einem Geistlichen oder einer Mitarbeiterin einer Beratungsstelle anzuvertrauen.**

Zudem irritiert der Begriff „ausschließlich“ in § 41 Abs. 1 Satz 2 SPolDVG-E. Der Gesetzgeber sollte hier klarstellen, dass es genügt, wenn eine Rechtsanwältin und ihr Mandant sich in einem Beratungsgespräch befinden, um einen besonderen Schutz der Vertraulichkeit zu beanspruchen.[35] Sie müssen nicht *ausschließlich* über mandats-bezogene Inhalte sprechen.

31 NPOG § 32 Abs. 4
32 PolG NRW § 15c Abs. 3:
33 PolG NRW § 15c Abs. 5:
34 Im SPolDVG-E steht: „Die an den verschiedenen Berufsgruppen orientierte Differenzierung zwischen absoluten Erhebungsverboten und relativen Verwertungsverboten ist durch das Bundesverfassungsgericht als verfassungskonform bestätigt. vom Februar 2020.
35 „ Mit anderen Worten darf bspw. die Telekommunikation zwischen Rechtsanwalt und Mandant bereits dann überwacht und aufgezeichnet werden, wenn im Rahmen *des jeweiligen Telefonats auch über nicht-mandatsbezogene Dinge gesprochen werden soll.“ Vgl. Stellungnahme der Landesbeauftragten für Datenschutz und Informationsfreiheit vom 25. Oktober 2019.*

AUSKUNFT DURCH TELEMEDIENANBIETER (§ 36)

In § 36 SPolDVG-E wird der Richtervorbehalt für die Bestimmung des Aufenthaltsortes und für die Bestandsdatenauskunft ersatzlos gestrichen. Mindestens für die Bestandsdatenauskunft ist nicht ersichtlich, weshalb der Gesetzgeber den Richtervorbehalt aufheben will.

Die Polizei bekommt zudem die Befugnis, die Nutzungsdaten von Personen, die sie verdächtigt, schwere Straftaten zu planen bei den Telemedienanbietern abzufragen. Nutzungsdaten geben einen tiefen Einblick in das Privatleben, die Eingriffschwelle für die Polizei sollte dementsprechend hoch angesetzt sein.

ABGLEICH PERSONENBEZOGENER DATEN (§ 28 Abs. 1)

Durch die Verknüpfung unterschiedlicher Datensätze können Personen in das Visier der Sicherheitsbehörden geraten, die sonst nicht aufgefallen wären. Eine Annahme über eine Person lediglich auf der Grundlage von abgerufen Daten zu treffen, birgt dabei die Gefahr, dass Personen fälschlicherweise als gefährlich eingestuft und in der Folge heimlich ausgeforscht werden.

Der Gesetzgeber sollte näher ausführen welche Fälle hier vorgesehen sind und **rechtlich präzisieren zu welchem Zweck das Abrufen der Daten zulässig** ist. Die Landesbeauftragten für Datenschutz und Informationsfreiheit stellt richtigerweise fest: „Es ist unverhältnismäßig, im Rahmen einer allgemeinen Verkehrskontrolle den kontrollierenden Beamten die Art, Zahl und den Umfang bisher gegen den Fahrer geführter Ermittlungsverfahren zu offenbaren. Ebenso unverhältnismäßig ist es etwa, jeden Anzeigeerstatter oder Hinweisgeber einem Abgleich mit den Fahndungsbeständen zu unterziehen. Die beiden vorgenannten Beispielfälle wären derzeit unzweifelhaft von der Formulierung des § 28 Abs. 1 SPolDVG-E gedeckt.“[36]

ALGORITHMEN (§ 25)

Mit § 25 SPolDVG-E soll laut Gesetzesbegründung verhindert werden, dass allein aufgrund eines Algorithmus eine Person observiert wird, zur Kontrolle ausgeschrieben wird oder anderweitige Maßnahmen zu ihrem Nachteil ergriffen werden.

Allerdings dürfen Algorithmen sehr wohl zu „Binnenentscheidungen“ führen. Hier fehlt es an einer allgemeinverständlichen Ausführung, was polizeiliche Binnenentscheidungen sind.

BENACHRICHTIGUNG VON BETROFFENEN (§ 10)

Die nachträgliche Benachrichtigung von Personen, die durch die Polizei oder andere Sicherheitsbehörden überwacht wurden, ist unabdingbar. Nur so wird Betroffenen überhaupt der Weg zur rechtlichen Überprüfung eröffnet.

36 Vgl. Stellungnahme der Landesbeauftragten für Datenschutz und Informationsfreiheit vom 25. Oktober 2019.

Grundsätzlich sollten alle betroffenen Personen über einen Eingriff in ihre Privatsphäre benachrichtigt werden. Dazu gehören nach diesem Gesetz regelmäßig auch Kontaktpersonen und andere Mitbetroffene. Es empfiehlt sich eine Regelung, die für jede Maßnahme benennt, welche Personen benachrichtigt werden, wie sie im nordrhein-westfälischen Polizeigesetz bereits existiert.[37]

DIE MITZIEHREGEL (§ 26)

Die Mitzieh-Regel ist in ihrer Pauschalität unverhältnismäßig und daher abzulehnen. Sie entspricht nicht dem datenschutzrechtlichen Grundgedanken der Erforderlichkeit.

Bei jedem neuen Speicheranlass werden alle bisherigen Daten der betroffenen Person mitgezogen. Für alle Speicherungen gilt dann die Frist, die als letztes endet. Besonders fragwürdig erscheint das im präventiv-polizeilichen Bereich, wo es in der Regel nicht um rechtskräftige Verurteilungen geht, sondern um Verdachtsmomente.

Die Landesdatenschutzbeauftragte schreibt in ihrer Stellungnahme: „Dies kann im Einzelfall dazu führen, dass es bei Personen, die beispielsweise bereits im jugendlichen Alter von 15 Jahren einmalig straffällig werden (z.B. wegen Cannabiskonsums) und die danach nur einmal im Jahrzehnt auffällig werden, sei es durch einen Geschwindigkeitsverstoß oder eine andere Bagatelle, bis zu deren Tod nicht ein einziges Mal zu einer Überprüfung kommt und der Datensatz über das jugendliche Bagatelldelikte zeitlebens mitgeführt wird.“[38] **Es fehlt mindestens eine genauere Benennung der Tatbestandsvoraussetzungen, unter denen eine längere Speicherung zulässig wäre**.[39]

Grafik: Darstellung der Mitzieh-Regel von Nathalie Meyer

37 PolG NRW § 33
38 Vgl. Stellungnahme der Landesbeauftragten für Datenschutz und Informationsfreiheit vom 25. Oktober 2019.
39 Marion Albers schreibt in ihrer Stellungnahme zum hamburgischen Polizeigesetzentwurf „Die pauschale Regelung ist nicht tragfähig. Das schließt nicht aus, dass in bestimmten Konstellationen ein Gesamtbild betroffener Personen sinnvoll erscheint und zur Verfügung stehen soll. Hierfür müssen aber engere Tatbestandsvoraussetzungen vorgesehen werden.“ https://www.linksfraktion-hamburg.de/wp-content/uploads/2019/09/StellungnahmeAlbers.pdf vom 18. September 2019.

4. Fazit

Der Gesetzgeber setzt in der präventiven Polizeiarbeit stark auf technische Maßnahmen: Aufenthaltsüberwachung mittels elektronische Fußfessel, Quellen-TKÜ, Bodycam und Videoüberwachung im öffentlichen Raum. Insgesamt werden dabei zu hohe Erwartungen an den Nutzen der ausforschenden Maßnahmen gestellt.

Um Probleme 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 immer die angemessene Stellschraube.

Ausschließlich die JI-Richtlinie muss im saarländischen Polizeirecht umgesetzt werden. Alle weiteren geplanten Befugnisse bedürfen einer Begründung, die über ihre rechtliche Zulässigkeit hinaus geht.

5. Empfehlungen und Formulierungsvorschläge

Im § 36 SPolDVG-E sollte der derzeit geltende Richtervorbehalt bei der Bestandsdatenauskunft beibehalten werden.

Im § 28 SPolDVG-E sollte präzisiert werden, zu welchem Zweck das Abrufen der Daten zulässig ist.

Der § 10 SPolDVG-E sollte in Bezug auf Kontaktpersonen und andere Mitbetroffene weiter ausdifferenziert werden. So sollte für jede heimliche Maßnahme benannt sein, welche Personen benachrichtigt werden müssen.[40]

In der Begründung zu § 25 SPolDVG-E fehlt eine allgemeinverständliche Beschreibung, was polizeiliche Binnenentscheidungen sind, bei denen automatisierte Entscheidungen zulässig sind.

Im § 38 SPolDVG-E sollte mindestens der Anwendungsbereich der elektronischen Fußfessel auf solche Fälle beschränkt werden, in denen die gefährdet/n Person/en bekannt sind und bereits ein Aufenthaltsverbot für einen begrenzten Bereich ausgesprochen wurde. Nur in solchen Fällen ist ein Nutzen der elektronischen Fußfessel im präventiven Bereich überhaupt denkbar.

Der § 41 SPolDVG-E sollte dahingehend überarbeitet werden, dass die Hierarchisierung innerhalb der Gruppe der Berufsgeheimnisträger*innen aufgehoben wird. Für den Schutz der Vertraulichkeit sollte es keinen Unterschied machen, ob sich eine Person in einer Notsituation entscheidet, sich einem Geistlichen oder einer Mitarbeiterin einer Beratungsstelle anzuvertrauen. Zudem sollte der Begriff „ausschließlich“ in § 41 Abs. 1 Satz 2 SPolDVG-E gestrichen werden.

Der § 32 Abs. 3 SPolDVG-E sollte um folgende Punkte ergänzt werden:

1. Betroffene müssen ein Recht auf Einsicht in das Videomaterial bekommen.[41]
2. Aufzeichnungen müssen „verschlüsselt sowie manipulationssicher gefertigt und aufbewahrt“ werden.[42]
3. Eine umfassende Hinweispflicht
4. Eine Regelung zur unabhängigen Evaluierung des Nutzens der Maßnahme, wie sie auch im vom saarländischen Innenministerium in Auftrag gegeben Rechtsgutachten gefordert wird.
5. Eine eindeutige Regelung zum Pre-Recording.[43]
6. Ein Verweis auf die Bedeutung der Maßnahme für Berufsgeheimnisträger*innen und den

40 Eine vergleichbare Regelung existiert bereits im nordrhein-westfälischen Polizeigesetz. Vgl. § 33 PolG NRW

41 Eine solche Regelung findet sich unter anderem im nordrhein-westfälischen Polizeigesetz, dort heißt es „auf Verlangen der betroffenen Person für die Überprüfung der Rechtmäßigkeit von aufgezeichneten polizeilichen Maßnahmen“ wird die Löschung der Aufnahmen aufgeschoben. Vgl. PolG NRW § 15c Abs. 4.

42 Vgl. PolG NRW § 15c Abs. 3

43 Im niederächsischen Polizeigesetz findet sich eine vergleichbare Regelung, dort heißt es: Die Bodycams „dürfen auch im Bereitschaftsbetrieb Aufzeichnungen anfertigen, diese sind automatisch nach höchstens 30 Sekunden zu löschen, es sei denn, es beginnen in dieser Zeitspanne Aufzeichnungen. In diesem Fall werden die Aufzeichnungen erst gemeinsam mit den Aufzeichnungen gelöscht.“ Vgl. NPOG § 32 Abs. 4

Kernbereichsschutz.[44]

Der § 33 Abs. 2 SPolDVG-E sollte herausgelöst und in einem eigenständigen Paragrafen geregelt werden.[45] Darüber hinaus sollte § 33 Abs. 2 grundlegend überarbeitet werden. Zunächst muss unbedingt klargestellt werden, ob laufende oder auch bereits gespeicherte Kommunikation ausgelesen werden soll. Nach bisheriger Rechtsprechung ist das Auslesen von gespeicherten Kommunikationsinhalten unzulässig.
Der Gesetzgeber sollte zudem festschreiben, dass nur bereits bekannte Sicherheitslücken verwendet werden dürfen.[46] 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 zudem umfänglich protokolliert und vor allem ausgewertet werden.
Da die technische Entwicklung schnell voranschreitet, muss für diesen Bereich eine zeitnahe Evaluation stattfinden. Sie sollte nach nur einem Jahr des Einsatzes der Staatstrojaner erfolgen.

Im § 26 SPolDVG-E sollten mindestens die Tatbestandsvoraussetzungen benannt werden, unter denen eine längere Speicherung zulässig wäre.[47] In der derzeitigen Pauschalität ist die Mitzieh-Regel abzulehnen.

Der § 32 Abs. 1 und 2 SPolDVG-E sollten gestrichen werden. Videoüberwachung an öffentlichen Orten führt lediglich zu Verdrängung von Straßenkriminalität, ihr Nutzen für die polizeiliche Aufklärungsarbeit ist nicht bewiesen. 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.

44 Eine vergleichbare Regelung findet sich im nordrhein-westfälischen Polizeigesetz. Dort heißt es: „Aufzeichnungen sind unzulässig in Bereichen, die der Ausübung von Tätigkeiten von Berufsgeheimnisträgern (…) dienen.“ und „die Aufzeichnung personenbezogener Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, ist unzulässig.“ Vgl. PolG NRW § 15c Abs. 3 und 5

45 Eine vergleichbare Regelung findet sich im Hamburgischen Gesetz über die Datenverarbeitung der Polizei. Vgl. PolDVG HH § 23 (TKÜ) und § 24 (Quellen-TKÜ).

46 Vgl. Stellungnahme der Landesbeauftragten für Datenschutz und Informationsfreiheit vom 25. Oktober 2019.

47 Marion Albers schreibt in ihrer Stellungnahme zum hamburgischen Polizeigesetzentwurf „Die pauschale Regelung in § 35 Abs. 3 S. 2 PolDVG-E ist nicht tragfähig. Das schließt nicht aus, dass in bestimmten Konstellationen ein Gesamtbild betroffener Personen sinnvoll erscheint und zur Verfügung stehen soll. Hierfür müssen aber engere Tatbestandsvoraussetzungen vorgesehen werden.“