Neues Polizeigesetz in Baden-Württemberg

Militarisierung der Polizei und schwere Eingriffe in Grundrechte

von Alexander Kleiß

Ein weiterer Schritt hin zu einer militarisierten Polizei und Innenpolitik wurde am 15. November 2017 vom baden-württembergischen Landtag vollzogen. Ministerpräsident Winfried Kretschmann hatte bereits im Januar 2017 verkündet, mit dem nun verabschiedeten neuen Polizeigesetz „an die Grenzen des verfassungsrechtlich Möglichen zu gehen“.[1] Die Grenzen des Grundgesetzes werden durch das neue Gesetzespaket[2] tatsächlich ausgereizt, wenn nicht gar überschritten. Das in den Medien immer wieder fälschlicherweise als „Anti-Terror-Gesetz“ bezeichnete Gesetzespaket enthält zahlreiche kritische Änderungen, bei denen zum Teil keinerlei Zusammenhang mit Terrorismus besteht. Die Bezeichnung „Überwachungs- und Polizeistaatsgesetz“ wäre zutreffender. So sind zahlreiche datenschutzrechtlich bedenkliche Neuerungen und eine weitere militärische Aufrüstung der Polizei vorgesehen:

Staatstrojaner

1. Die Polizei und der Landesverfassungsschutz[3] werden künftig Chats – auch auf (mehr oder weniger gut) verschlüsselten Messenger-Diensten, wie WhatsApp, Telegram oder Signal – mitlesen können. Dies wird bereits beim Verdacht auf schwere Kriminalität und präventiv, also allein aufgrund des Verdachts, eine Person könnte in der Zukunft eventuell eine schwere Straftat[4] begehen, möglich sein. So können auch unbescholtene Bürger_innen, die noch nie eine Straftat begangen haben, allein aufgrund des Verdachts einer ermittelnden Behörde überwacht werden. Grundsätze rechtsstaatlichen Handelns in der BRD, wie die Unschuldsvermutung oder das Fernmeldegeheimnis, werden somit einfach missachtet und über Bord geworfen. Die Ausforschung von Chats soll nicht durch eine Brechung der Verschlüsselung der einzelnen Nachrichten erreicht werden, sondern durch sogenannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ). Das heißt, dass die Nachrichten nicht unterwegs abgefangen und entschlüsselt werden, sondern dass sie durch den Einsatz eines „Staatstrojaners“, der den Betroffenen ohne ihr Wissen auf ihr Gerät gespielt wird, bereits auf dem Smartphone oder Computer selbst mitgelesen werden können. Um die Staatstrojaner auf die jeweiligen Geräte zu spielen, werden jedoch unbedingt mittlere bis schwere Sicherheitslücken benötigt. Der Chaos Computer Club schreibt hierzu:

„Für jeden Einsatz von Schadsoftware im Rahmen der Quellen-TKÜ oder Online-Durchsuchung wird [...] ein Angriffspunkt auf diesem System benötigt, der zur Infektion genutzt werden kann. […] Eine Infektion durch Dritte ist grundsätzlich nur bei fehlenden oder fehlerhaften Zugangsbeschränkungen oder durch Ausnutzung einer Software-Schwachstelle möglich. Da vollständig fehlende Zugangsbeschränkungen in den seltensten Fällen vorkommen und diese darüber hinaus direkten physischen Zugriff auf das Gerät voraussetzen würden, wären vorhandene Software-Schwachstellen für den größeren Teil der Einsätze Grundvoraussetzung. […] Um eine fortwährende Ausnutzung der Schwachstelle sicherzustellen, muss diese geheim gehalten werden, da sonst mit ihrer Beseitigung zu rechnen wäre. Dies bedeutet im Umkehrschluss, dass die Schwachstelle ausnahmslos auf allen betroffenen Geräten weltweit vorhanden sein muss. Damit geht zwingend das Risiko einher, dass die Schwachstelle von anderen interessierten Gruppen, insbesondere von Kriminellen oder anderen staatlichen Akteuren ebenfalls entdeckt und ausgenutzt wird.“[5]

Das Ausnutzen von Software-Schwachstellen ist eine bisher vor allem bei Geheimdiensten und militärischen Cyber-Kommandos vieler Staaten gängige Praxis. Dass nun auch die deutsche Polizei so vorgeht, ist unverantwortlich. Denn dieses Vorgehen führt keineswegs zu mehr Sicherheit, sondern verhindert vielmehr die Schließung von Sicherheitslücken. Noch brisanter wird dies, wenn man bedenkt, dass nicht nur Smartphones, Computer und Tablets betroffen sind, sondern auch andere internetfähige Geräte, wie z.B. Heizungs- und Lichtanlagen, Smart TVs oder Smart Cars durch staatlich aufgespielte Schadsoftware angegriffen werden können. Es ist dann möglich, diese unbemerkt zu steuern und z.B. Kameras und Mikrofone einzuschalten und auszuwerten.[6] Dies ist zwar im neuen Polizeigesetz nicht vorgesehen, es ist jedoch bisher vollkommen ungeklärt, wie sichergestellt werden soll, dass durch die Schadsoftware nur die aktuellen Nachrichten und nicht alle anderen gespeicherten Daten, Kameras und Mikrofone überwacht werden können, da bei einer Infektion Zugriff auf das gesamte Gerät bestünde. Dies mahnte auch Ulf Buermeyer, Richter am Landgericht Berlin und Vorsitzender der Gesellschaft für Freiheitsrechte e.V., als Gutachter zu diesem Thema im Bundestag an.[7] Ob dieser Teil des Gesetzes einer Überprüfung durch das Verfassungsgericht standhalten wird, bleibt abzuwarten. Allein der Versuch ist jedoch alarmierend.

Handgranaten und Sprengstoff für die Polizei

2. Die fortschreitende Militarisierung der Polizei wird durch eine weitere Änderung vorangetrieben. Diese sieht vor, dass die Spezialeinsatzkommandos (SEK) der Polizei[8] künftig unter bestimmten Umständen Explosivmittel gegen Personen einsetzen dürfen. Dies umfasst z.B. Handgranaten, Sprenggeschosse, die aus Schusswaffen verschossen werden können, und konventionelle Sprengmittel. Diese Waffen, die eigentlich eher an Kriegsszenarien erinnern als an Polizeiarbeit, dürfen jedoch „nur“ eingesetzt werden, wenn andere Waffen keinen Erfolg versprechen. Sie dürfen auch nicht gegen Menschenmengen eingesetzt werden. Der Anwaltsverband Baden-Württemberg kritisierte diese Änderung im Rahmen des Gesetzgebungsprozesses, da die Notwendigkeit eines polizeilichen Einsatzes von Explosivmitteln nicht gegeben sei. Die Landesregierung teilte die Bedenken jedoch nicht und sah keinen Grund, die Passage zu ändern oder zu streichen. Die polizeilichen SEKs agieren somit immer ähnlicher den militärischen Kommando-Soldat_innen.

Intelligente Videoüberwachung

3. Die Polizei erhält darüber hinaus die Möglichkeit, Kameraaufnahmen im öffentlichen Raum automatisch auszuwer-

Aufnahmen von Überwachungskameras im öffentlichen Raum können künftig in Echtzeit ausgewertet werden. Quelle: Picasa via Wikipedia (CC BY 3.0).

ten. In Echtzeit können durch diese sogenannte intelligente Videoüberwachung Verhaltensmuster erkannt werden, die „auf die Begehung einer Straftat hindeuten".[9] Eine biometrische Gesichtserkennung ist dabei nicht vorgesehen, sie wird im Gesetzestext jedoch auch nicht ausdrücklich ausgeschlossen. Wie die eingesetzte Software Straftaten – im besten Fall schon bevor sie begangen werden – erkennen will, bleibt im Gesetzestext ebenfalls offen. Auffällig könnte z.B. das Abstellen eines Koffers und anschließendes Weggehen sein; aber auch Rennen, Hinfallen, der längere Aufenthalt auf einem Bahnsteig, sich in einer Gruppe zu bewegen oder Hin- und Herlaufen könnte künftig zu einer Alarmierung von Polizeibeamten führen, die dann aufgrund der Überwachungssoftware entsprechende Kontrollen durchführen.[10] Problematisch daran ist, dass die Definition dessen, was als verdächtig oder kriminell wahrgenommen wird, den Entwickler_innen der Analysesoftware überlassen wird. Das Internationale Zentrum für Ethik in den Wissenschaften schreibt in einer Publikation zu intelligenter Videoüberwachung: „Generell bedeutet die technische Herstellung von Sicherheit, dass die Definitionsmacht darüber, was als sicher und was als Bedrohung gilt, zumindest teilweise an die Entwickler(innen), Hersteller(innen) und Betreiber(innen) der Technik übergeht [...]. Damit birgt die technische Herstellung von Sicherheit die Gefahr, demokratische Prozesse, in denen der Wert von Sicherheit ausgehandelt wird, einzuschränken."[11] Das Wissen über die Überwachung und die Unsicherheit darüber, wann die Analysesoftware anschlägt, könnte dazu führen, dass die Bürger_innen unter Druck gesetzt werden, sich möglichst unauffällig und angepasst zu verhalten. Außerdem könnte intelligente Videoüberwachung zu verschiedenen Formen von Diskriminierung führen. Es ist nicht transparent, inwiefern die Technik Hautfarbe, Geschlecht oder Alter der Überwachten in die Bewertung einer Situation als gefährlich oder ungefährlich miteinbezieht. Außerdem „könnte das System Menschen mit einem besonderen Gang als ungewöhnlich und potenziell ‚gefährlich' einstufen. Dies könnte dazu führen, dass beispielsweise Menschen mit Gehbehinderungen vom technischen System als Sicherheitsrisiko wahrgenommen werden."[12] Nicht nur vor diesem Hintergrund ist es gefährlich, dass die Forschung zu intelligenter Videoauswertung extrem militarisiert ist: „Intelligente Videoauswertung ist schon jetzt im militärischen Bereich verbreitet und es besteht eine große Nachfrage nach einer verbesserten Technologie für den Einsatz von Drohnen. Darüber hinaus wäre die intelligente Videoüberwachung ausgezeichnet zur Unterdrückung demokratischer Bewegungen einzusetzen oder generell zur Unterdrückung politisch oder religiös abweichender Personen und Gruppierungen."[13] Mit der Entwicklung und Implementierung der Analysesoftware wurde das rüstungs- und militärnahe Fraunhofer Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) beauftragt.[14] Das Land Baden-Württemberg und das Fraunhofer IOSB werden gemeinsam einen „Modellversuch in einer Einkaufsstraße sowie auf dem Bahnhofsvorplatz von Mannheim"[15] durchführen. Es ist explizit Teil der Strategie des Fraunhofer IOSB,[16] nicht nur zu militärisch relevanten Themenfeldern zu forschen, sondern auch durch vermeintlich zivile Dual-Use-Forschung „wissenschaftliche Erkenntnisse zu generieren und zu identifizieren, die wehrtechnisch relevant sind, diese aufzugreifen und auf mögliche militärische Nutzungen zu prüfen."[17] Von der Entwicklung der Technik zur intelligenten Videoüberwachung in Baden-Württemberg profitieren letztendlich also auch Militär und Rüstungskonzerne. Gleichzeitig war und ist es umgekehrt explizites Ziel der Dual-Use-Strategie des Fraunhofer IOSB, „‚zivile' Märkte für militärische Technologien zu erschließen".[18] Diese Strategie wurde unter der Federführung des Verteidigungsministeriums bei der Fusion des wehrtechnischen FGAN-Instituts FOM und des sowohl im militärischen als auch im zivilen Bereich forschenden Fraunhofer IITB, aus der dann das Fraunhofer IOSB entstand, erarbeitet.[19] Militärische Technologien halten dadurch Einzug in die alltägliche Überwachung.

Aufenthaltsverbote und elektronische Fußfessel

4. Ein weiterer strittiger Punkt im neuen Polizeigesetz Baden-Württembergs ist die Legalisierung eines massiven Eingriffs in die Privatsphäre: Sogenannte Gefährder_innen – also Menschen, die nicht unbedingt strafrechtlich in Erscheinung getreten sein müssen, aber von staatlichen Behörden (auf welcher Rechtsgrundlage auch immer) als gefährlich eingestuft werden – können seit dem 15. November 2017 mit Aufenthalts- und Kontaktverboten für bestimmte Orte und Personen belegt werden. Sie können explizit auch unter Hausarrest gestellt werden. Zur Überwachung der Einhaltung dieser Maßnahmen können die Betroffenen auch zur Anlegung einer elektronischen Fußfessel, einem technischen Gerät, das den Aufenthaltsort der Betroffenen überwacht, gezwungen werden. Dies stellt einen mehrfachen empfindlichen Eingriff in die Grundrechte der Betroffenen dar. Ob dadurch Terroranschläge verhindert werden, wird von vielen – sogar von der Gewerkschaft der Polizei[20] – bezweifelt. Vor allem Selbstmordattentäter_innen lassen sich durch eine Fußfessel kaum abschrecken. Seit das neue Überwachungsmittel im Sommer 2017 auf Bundesebene legalisiert wurde, gab es nur einen islamistischen Gefährder, der gezwungen wurde, eine elektronische Fußfessel zu tragen. Dieser setzte sich im Oktober erfolgreich per Flugzeug (!) nach Griechenland ab.[21]

Alkoholverbote im öffentlichen Raum

5. Teil des Gesetzespakets ist auch eine neue Regelung, die es Ortspolizeibehörden erlaubt, per Verordnung den Konsum und das Mitführen alkoholischer Getränke auf bestimmten öffentlichen Plätzen zeitlich begrenzt zu verbieten. Im Gegenzug wird das nächtliche Alkoholverkaufsverbot ab 22 Uhr aufgehoben.[22] Dies hat keinerlei Bezug mehr zur Bekämpfung von Terrorismus und zeigt besonders eindrücklich, dass das Gesetzespaket auch nicht vorrangig dieses Ziel verfolgt. Vielmehr geht es der „grün-schwarzen" Landesregierung darum, die Bürger_innen, welche z.T. allesamt unter Generalverdacht gestellt werden, auszuspionieren und zu überwachen, unliebsame Bürger_innen aus dem öffentlichen Raum zu verbannen, die Polizei massiv zu militarisieren, ihre Befugnisse in verfassungswidriger Weise zu erweitern und einem Teil der Bürger_innen dabei gleichzeitig noch ein subjektives Gefühl von vermeintlicher Sicherheit zu vermitteln.

Große Koalition der Überwachenden

Das Gesetzespaket wurde von den Regierungsparteien in Baden-Württemberg – den „Grünen" und der CDU – erarbeitet. Hans-Ulrich Sckerl von den „Grünen" spricht von einer gelungenen „Balance zwischen Freiheit und Sicherheit".[23] Wo er den freiheitlichen Teil des Gesetzes wähnt, bleibt wohl sein Geheimnis. Ohne dass dies nötig gewesen wäre, stimmte nach minimalen Nachbesserungen auch die oppositionelle SPD dem Gesetz zu. Das autoritäre Gesetzespaket wurde somit von einer besonders großen Koalition der Überwachenden (Grüne, CDU und SPD) im Ländle angenommen. Von den im Landtag vertretenen Parteien sprachen sich nur FDP und AfD gegen das Gesetz aus. Auch der Landesdatenschutzbeauftragte kritisierte das Gesetz: Es führe zu einer „realen Einbuße an Freiheit",[24] wobei gleichzeitig offen bleibe, ob das Gesetz zu einer tatsächlichen Verbesserung der Sicherheitslage beitrage. Außerdem kritisierte er, dass Teile des Gesetzes möglicherweise verfassungswidrig seien und: „Wer an die Grenze des verfassungsrechtlich Zulässigen geht, provoziert zwei Konsequenzen: Er überantwortet die Letztentscheidung zu sicherheitspolitischen Fragen dem Verfassungsgericht und er läuft Gefahr, Anlass und Zweck der Sicherheitsnovelle aus den Augen zu verlieren."[25]

Angesichts der zahlreichen Eingriffe in die Grundrechte und die Privatsphäre der Bürger_innen hätten die Medien die Aufgabe gehabt, über das Thema ausgiebig zu berichten und eine gesellschaftliche Debatte anzustoßen. Leider war die mediale Aufarbeitung – vielleicht auch mangels wirklicher Opposition im Landtag – sehr unkritisch und vielen Zeitungen nur eine Randnotiz wert.

Wirklich neu sind die meisten baden-württembergischen Änderungen am Polizeigesetz nicht. Vieles findet sich wortgleich für das Bundeskriminalamt im von der Großen Koalition in der vergangenen Legislaturperiode verabschiedeten BKA-Gesetz. Dieses Gesetz war auch genauso gedacht: als Vorlage für entsprechende Gesetze auf Landesebene. Bayern hat z.B. die elektronische Fußfessel für Gefährder_innen bereits ebenfalls eingeführt. Baden-Württemberg hat nun eines der schärftsten Polizeigesetze überhaupt. Andere Bundesländer könnten folgen.

Anmerkungen

1 Merkur: Kretschmann: Notfalls verfassungsrechtliche Grenzen ausreizen. 14.1.2017.

2 Landtag von Baden-Württemberg: Gesetz zur Änderung des Polizeigesetzes. Drucksache 16/3011. 15.11.2017; Landtag von Baden-Württemberg: Gesetz zur Änderung des Landesverfassungsschutzgesetzes und des Ausführungsgesetzes zum Artikel 10-Gesetz. Drucksache 16/3010. 15.11.2017; Landtag von Baden-Württemberg: Gesetz zur Abwehr alkoholbedingter Störungen der öffentlichen Sicherheit. Drucksache 16/3012. 15.11.2017.

3 Dieselben Befugnisse zum Einsatz eines „Staatstrojaners" wurden neben der Polizei auch dem Landesverfassungsschutz zugesprochen. Vgl. Landtag von Baden-Württemberg: Gesetz zur Änderung des Landesverfassungsschutzgesetzes und des Ausführungsgesetzes zum Artikel 10-Gesetz. Drucksache 16/3010. 15.11.2017.

4 Eine besonders schwere Straftat liegt dem Gesetz zufolge vor, wenn „Leib, Leben oder Freiheit einer Person, [der] Bestand oder die Sicherheit des Bundes oder eines Landes oder [...] wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen", gefährdet sind.
Vgl. Landtag von Baden-Württemberg: Gesetz zur Änderung des Polizeigesetzes. Drucksache 16/3011. 15.11.2017.

5 Chaos Computer Club: Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung. 31.5.2017.

6 KONTEXT:Wochenzeitung: Sicherheitslücken für mehr Sicherheit. 1.11.2017.

7 Ulf Buermeyer: Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess. Ausschuss-Drucksache 18(6)334. 31.5.2017.

8 … und theoretisch auch andere Einheiten; dies wird im Gesetzestext offen gelassen.

9 Landtag von Baden-Württemberg: Gesetz zur Änderung des Polizeigesetzes. Drucksache 16/3011. 15.11.2017.

10 Vgl. Netzpolitik: Intelligente Videoüberwachung: Regierung will Folgen der Grundrechtseingriffe später reflektieren – vielleicht. 27.10.2016; Südwest Presse: Sicherheit: Die neuen Befugnisse der Behörden. 16.11.2017.

11 Regina Ammicht Quinn: Intelligente Videoüberwachung: eine Handreichung. 2015, S. 30.

12 Ebd., S. 25.

13 Ebd., S. 24.

14 Südwest Presse: Sicherheit: Die neuen Befugnisse der Behörden. 16.11.2017.

15 Südwest Presse: Überwachungskameras im Test: Beginnt jetzt der große Scan? 1.8.2017.

16 Für ausführlichere Informationen zum Fraunhofer IOSB: vgl. IMI-Studie 2017/2. Christoph Marischka: Fraunhofer IOSB: Dual Use als Strategie.

17 Wissenschaftsrat: Stellungnahme zur Neustrukturierung der Forschungsgemeinschaft für Angewandte Naturwissenschaften e.V. (FGAN). 2007.

18 IMI-Studie 2017/2. Christoph Marischka: Fraunhofer IOSB: Dual Use als Strategie.

19 Ebd.

20 Süddeutsche Zeitung: Fußfessel für Extremisten: Selbst Polizei kritisiert CSU-Pläne. 23.4.2017.

21 Süddeutsche Zeitung: Islamist fliegt trotz Fußfessel nach Griechenland. 16.11.2017.

22 Landtag von Baden-Württemberg: Gesetz zur Abwehr alkoholbedingter Störungen der öffentlichen Sicherheit. Drucksache 16/3012. 15.11.2017.

23 Landtag von Baden-Württemberg: Plenarprotokoll 16. Wahlperiode, 47. Sitzung. 15.11.2017.

24 Netzpolitik: Überwachung. Baden-Württemberg: Datenschutzbeauftragter kritisiert grün-schwarzes Anti-Terror-Paket. 10.10.2017.

25 Ebd.