digitalcourage

LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

STELLUNGNAHME
17/947

A09, A14

Bielefeld, 9.11.2018

Landtag Nordrhein-Westfalen
Referat I.A.1 / A 09
Platz des Landtags 1
40221 Düsseldorf

Digitalcourage e.V.

Marktstraße 18
33602 Bielefeld

Ansprechpartnerin: Kerstin Demuth
Kerstin.demuth@digitalcourage.de

mail@digitalcourage.de
Fon: 0521 1639 1639
Fax: 0521 61172

Stellungnahme von Digitalcourage zum Sechsten Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen (Drs. 17/2351) und dem Änderungsantrag der Fraktionen CDU & FDP (Drs. 17/3865)

digitalcourage

1. Vorbemerkungen

Digitalcourage nimmt im Folgenden nicht zu allen vorgesehenen Maßnahmen ausführlich Stellung. Aus Gründen der Zeit fokussieren wir uns hier auf einige der Maßnahmen, die uns besonders Sorge bereiten. Das bedeutet ausdrücklich nicht, dass wir zu den Punkten, die hier keine Erwähnung finden, keine Bedenken haben. Digitalcourage verweist auf eine ausführliche und verständliche Erläuterung der Maßnahmen für Bürgerinnen und Bürger unter https://digitalcourage.de/blog/2018/polizeigesetz-nrw-entschaerfung-findet-nicht-statt sowie einen Appell gegen Innere Aufrüstung, den bisher ca. 4.600 Menschen mitgezeichnet haben (https://digitalcourage.de/blog/2018/appell-gruen-spd-fdp-hoeren-sie-auf-ihre-buergerrechtsfluegel).

1.1. Zum Änderungsantrag

Wir wollen lobend erwähnen, dass die Regierungsfraktionen die Kritik der Bevölkerung am Entwurf des „Gesetz zur Stärkung der Sicherheit in Nordrhein-Westfalen – Sechstes Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen“ (Drs. 17/2351 LT NRW) gehört hat und mit dem Änderungsantrag (Drs. 17/3865 LT NRW) punktuell Anpassungen vornehmen will. Unserer Ansicht nach sind die Anpassungen jedoch unzureichend. Es wurde im Vorfeld von Expertinnen und Experten an vielen Aspekten fundierte und umfangreiche Kritik geübt, allem voran an der Verlagerung der Polizeiarbeit in das Vorfeld einer konkreten Gefahr und dem Einsatz von Staatstrojanern, der weltweit die IT-Sicherheit gefährdet. Der Gefährderbegriff wurde zwar mit dem Änderungsantrag entschärft; Sowohl die Polizeiarbeit weit vor einem konkreten Verdacht als auch die Staatstrojaner sind jedoch weiterhin enthalten. Darüber hinaus mangelt es an konkreten und überprüfbaren Erklärungen der Landesregierung, wie die vorgeschlagenen Maßnahmen für Sicherheit sorgen und Terrorakten vorbeugen sollen.

1.2. Zur Bezeichnung „Sicherheitspaket I“

Darüber hinaus weist Digitalcourage auf den von Innenminister Reul verwendeten Kurznamen der Gesetzesänderung, „Sicherheitspaket I“ hin. Daran ist erstens zu kritisieren, dass die Reform unserer Ansicht nach nicht zur Sicherheit beiträgt, sondern schlicht erweiterte Überwachungs- und Repressionsbefugnisse enthält, auch gegenüber Menschen die keiner Straftat verdächtig sind.

Zweitens legt die Ziffer „I“ nahe, dass mindestens ein weiteres „Sicherheitspaket“ verabschiedet werden sollen. Angesichts der erheblichen Eingriffstiefe der vorgesehenen Überwachungs- und Freiheitsentziehungsmaßnahmen, stellt sich die Frage, wie viele Bürgerrechte mit dem zweiten Paket entzogen werden sollen. Digitalcourage gelangt zu dem Eindruck, dass die Regierung und die sie tragenden Fraktionen sich nicht hinreichend über die Bedeutung solcher

Grundrechtseingriffe für eine Demokratie im Klaren sind. Rechtsstaatlichkeit und Abwehrrechte gegen den Staat sind wichtige Stützpfeiler der Demokratie und dürfen nicht derart geschliffen werden.

1.3. Zum Richtervorbehalt

Richtervorbehalte dürfen nach Ansicht von Digitalcourage nicht genutzt werden, um unverhältnismäßige Ausweitungen von Grundrechtseingriffen gesetzgeberisch und politisch zu legitimieren. Verfassungsrechtlich sind Richtervorbehalte in vielen Fällen sinnvoll und notwendig. In der Praxis erweisen sie sich allerdings als ineffizient und oft unwirksam. Die Ablehnungsrate ist nachweislich sehr gering. Des weiteren können Richter.innen lediglich auf Grundlage der Aktenlage und unter Zeitdruck entscheiden. Das Fachwissen, dass für eine differenzierte Beurteilung der Fälle nötig wäre, kann in der Kürze der Zeit nicht erworben werden.

2. Empfehlungen für den Gesetzgebungsprozess

Wir empfehlen der Landesregierung für das weitere Gesetzgebungsverfahren:

- **Belege für die Wirksamkeit** der vorgeschlagenen Maßnahmen vorzulegen.
- Eine **Gefahrenabschätzung** vorzulegen.
- Eine **Datenschutzfolgenabschätzung** für alle geplanten Maßnahmen vorzulegen.
- Eine **IT-Sicherheits- und Technikfolgeabschätzung**, insbesondere bezüglich der Einführung von Q-TKÜ.
- **Grundrechtsschonendere Maßnahmen** der Terror- und Gewaltprävention zu prüfen, z.B. einen Ausbau der psychologischen Betreuung, städtebauliche Maßnahmen, …
- Bereits bestehende **Überwachungsmaßnahmen wissenschaftlich prüfen** zu lassen und gegebenenfalls zurückzunehmen.
- Eine **Überwachungsgesamtrechnung** sowie einen **Überwachungsindex** für das Land Nordrhein-Westfalen aufzustellen.

3. Zu den Maßnahmen in Einzelnen

3.1. Anhalte- und Sichtkontrollen (§ 12a d.E.)

Die sogenannte Schleierfahndung erlaubt es der Polizei Gefahrenorte zu definieren und dort verdachtsunabhängig Personen zu kontrollieren. Als Grundlage gilt nicht der neu eingeführte Begriff einer drohenden terroristischen Gefahr (§8 Absatz 4 d.E.) sondern der bereits bestehende §8 (3). Dieser beinhaltet u.a. Verstöße gegen das Betäubungsmittelgesetz und das Aufenthaltsgesetz. Wir erkennen hier keinen Zusammenhang zu terroristischen Gefahren und

sehen daher nicht, wie die vorgeschlagene Maßnahme dem Ziel des Gesetzes dienen soll. Darüber hinaus sieht Digitalcourage ein Risiko, dass Verstöße gegen das Aufenthaltsgesetz zu Racial Profiling missbraucht werden (Vgl. dazu Stellungnahme 17/646 von Amnesty International).
Das Recht auf informationelle Selbstbestimmung beinhaltet auch, sich anonym im öffentlichen Raum bewegen zu können. Dieses Recht wird stark eingeschränkt, wenn die Polizei in Zukunft vermehrt Passant.innen zur Identitätsfeststellung anhalten darf. Die zufällige Kontrolle an eigenständig definierten Orten öffnet die Tür für Willkür. Von dieser Maßnahme sind nicht etwa, wie in der Gesetzesbegründung angeführt, potentielle Terrorist.innen betroffen, sondern die gesamte Bevölkerung. Besonders in Verbindung mit § 38 Absatz 2 Satz 5 (Ingewahrsamnahme zur Identitätsfeststellung) erscheint die Maßnahme unverhältnismäßig: Durch das Nichtmitführen des Personalausweises – ob absichtlich oder aus Versehen – würde sich in Zukunft jede Person der Gefahr aussetzen, bis zu eine Woche inhaftiert zu werden.

3.2. Videoüberwachung (§15a d.E.)

Von optischer Beobachtung des öffentlichen Raums sind immer unbescholtene Bürgerinnen und Bürger direkt betroffen. Besonders in Verbindung mit Bundesgesetzen wie dem sogenannten „Videoüberwachungsverbesserungsgesetz“ (28.04.2017, Bgbl. Nr. 23 vom 04.05.2017) sehen wir eine Zunahme der optischen Beobachtung des öffentlichen Raums, die das Grundrecht auf informationelle Selbstbestimmung stark einschränkt. Es muss weiterhin gestattet und möglich sein, sich unbeobachtet und anonym durch den öffentlichen Raum zu bewegen.
Für sich genommen hat Videoüberwachung **keinen vorbeugenden Effekt auf Terror- und Gewalttaten**. Das wurde in zahlreichen wissenschaftlichen Untersuchungen belegt. [Eine Auswahl von Studien siehe: https://digitalcourage.de/videoueberwachung/materialsammlung].
Zu begrüßen ist daher, dass im PolG-E eine Einschränkung vorgesehen ist: Die zusätzliche Videobeobachtung soll nur gestattet sein, wenn „jeweils ein unverzügliches Eingreifen der Polizei möglich ist“. Jedoch kann mithilfe des § 15a Absatz 1 Satz 2 d.E. eine Videoüberwachung an praktisch jedem Ort des öffentlichen Raums gerechtfertigt werden. Das ist eindeutig unverhältnismäßig. Darüber hinaus sieht der bereits bestehende § 15a Absatz 2 vor, dass die Bilddaten bis zu 14 Tagen gespeichert werden können. Nach Einschätzung von Digitalcourage ist diese Frist unverhältnismäßig lang. Es kann davon ausgegangen werden, dass Straftaten in einem sehr kurzen Zeitraum nach Ihrer Begehung angezeigt werden.
Insgesamt stellt Digitalcourage in Frage, ob der bereits bestehende §15a Absatz 2 und die vorgeschlagenen Änderungen des §15a Absatz 1 tatsächlich zur Sicherheit beitragen. **Videoüberwachung alleine ist wirkungslos, während sie das Recht auf informationelle Selbstbestimmung aller schädigt.** Die Beamt.innen, die laut Entwurf zur Beobachtung der

Aufzeichnung und für das vorgeschriebene Eingreifen vorgehalten werden müssen, könnten ebenso gut ohne eine Bildaufzeichnung Orte kontrollieren, die als gefährlich eingeschätzt werden. **Es hat sich gezeigt, dass mildere Maßnahmen, die keine Grundrechte verletzen, effektiver Kriminalität vorbeugen als Überwachungskameras; beispielsweise das Zurückschneiden von Hecken und das Aufstellen von Beleuchtung** – belegt ist das bspw. durch die Entwicklung im Ravensberger Park in Bielefeld. Dort konnte die Kriminalität durch o.g. Maßnahmen gesenkt werden, bevor Überwachungskameras installiert wurden. Der Umweg über eine Videoüberwachung erscheint nicht nur umständlich, sondern ist auch kostspielig, da die Anlagen installiert, gewartet und in Stand gehalten werden müssen. Digitalcourage fordert daher, anstatt einer Ausweitung der Videoüberwachung, eine wissenschaftliche Überprüfung der bisher durch das Land betriebenen Anlagen. Wenn sich als wenig wirksam erweisen, müssen sie konsequenterweise rückgebaut werden.

3.3. Quellen-Telekommunikationsüberwachung („Staatstrojaner“; § 20c d.E.)

Der Entwurf sieht unverändert den Einsatz von staatlicher Spähsoftware zur Quellentelekommunikationsüberwachung (Q-TKÜ) vor. Nach der umfangreichen Kritik von Datenschutz-, Menschenrechts-, IT-Sicherheits-, und Wirtschaftsverbänden ist das in keiner Weise nachvollziehbar.

Zunächst zur Bedeutung der Maßnahmen für Betroffene: Staatstrojaner sind sehr eingriffsintensiv. Die Q-TKÜ erlaubt das Auslesen der laufenden Kommunikation u.a. in verschlüsselten Messengern. Im Entwurf ist ein starker Schutz des **Kernbereichs privater Lebensgestaltung** vorgesehen. Uns erschließt sich indes nicht, wie die Regelung dann zum Tragen kommen soll: Wenn tatsächlich gewährleistet ist, dass eine angeordnete Q-TKÜ dann abgebrochen wird, wenn auch Dinge aus dem Kernbereich privater Lebensgestaltung in Erfahrung gebracht werden, sind nur sehr künstliche Szenarien vorstellbar, in denen sie rechtskonform angewendet werden kann. Neben den Zielpersonen werden deren private und berufliche Kontakte geschädigt, da alle Beteiligten der digitalen Kommunikation betroffen sind und nicht nur die Zielperson selbst.

Darüber hinaus gibt es umfassende verfassungsrechtliche Bedenken. Gegen die Staatstrojaner in der Strafprozessordnung liegen dem Bundesverfassungsgericht derzeit vier Verfassungsbeschwerden vor. Eine der hauptsächlich angeführten Begründungen der Beschwerdeführer.innen und der Kritik an Staatstrojanern im allgemeinen, ist eine enorme **Gefährdung der IT-Sicherheit**. Grund dafür ist die **Installation über Sicherheitslücken**. Diese stehen dann nicht nur dem Staat offen, sondern allen – also auch internationalen Geheimdiensten

und Kriminellen. Ironisch ist, dass in NRW die invasiven Staatstrojaner vorgeschlagen werden, nachdem das BverfG in seinem Urteil zum NRW-Trojaner des LfV diesen als verfassungswidrig und nichtig erklärt hat [Bundesverfassungsgericht: Urteil des Ersten Senats vom 27. Februar 2008 (Az. 1 BvR 370/07, 1 BvR 595/07)]. In selbigem Urteil formulierten die Richter.innen des BverfG das ***Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht)*** als spezifische Ausprägung des Rechts auf informationelle Selbstbestimmung. Digitalcourage sieht in dem vorgesehenen §20c d.E. einen Bruch mit dem IT-Grundrecht. Unserem Verständnis nach wäre es zur Gewährleistung des IT-Grundrechts folgerichtig, wenn das Land NRW sich verpflichtete, Sicherheitslücken von denen Landesbehörden Kenntnis erlangen, den Herstellern zu melden, damit die Schwachstellen geschlossen werden. Eine Ausnutzung dieser Sicherheitslücken für polizeiliche Zwecke steht dem diametral entgegen.

Ein Schutz von Berufsgeheimnisträger.innen ist augenscheinlich nicht vorgesehen. Die Arbeit von Journalisten, Anwältinnen, seelsorgerisch Tätigen ist essentiell für eine demokratische Gesellschaft. Diese Berufsgruppen sind in Ihrer Arbeit auf ein solides Vertrauensverhältnis zu ihren Klient.innen bzw. Informant.innen angewiesen. Wenn Angehörige dieser Berufsgruppen sowie ihre Klient.innen sich nicht mehr auf Vertraulichkeit ihrer Kommunikation verlassen können, wird dieses Vertrauensverhältnis empfindlich geschädigt.
Besonders möchten wir die Rolle von Psychotherapeutinnen und anderen Seelsorgern hervorheben. Die Reform soll laut Gesetzesbegründung explizit Sicherheit herstellen und Terrorismus vorbeugen. Wir sind der Überzeugung, dass diesem Ziel besser entsprochen werden kann, wenn gefährdete Jugendliche und Erwachsene eine angemessene psychologische Betreuung erhalten und in das gesellschaftliche Leben eingebunden sind. **Gerade in vertraulichen Gesprächen, in denen Menschen sich gehört fühlen, kann Gewalt verhindert werden.** Die vorgesehene Ausweitung der Telekommunikationsüberwachung stört das Vertrauensverhältnis von Klientin und Therapeutin und hält womöglich Menschen davon ab, sich psychologische Unterstützung zu suchen.

Es sei anerkennend erwähnt, dass mit dem Änderungsantrag zumindest eine Dokumentationspflicht für den Einsatz der Staatstrojaner eingeführt werden soll, sowie Vorkehrungen, die den Kernbereich privater Lebensgestaltung schützen. Bei letzteren stellt sich die Frage, wie dann ein Anwendungsfall der Q-TKÜ rechtskonform realisiert werden kann. Darüber hinaus gibt es keine Antwort auf die Risiken für die IT-Sicherheit. Daher lehnt Digitalcourage eine Einführung von Staatstrojanern für die Landespolizei ab.

3.4. Aufenthalts- und Kontaktverbote (§§ 34b, 34c d.E.)

Die Polizei dürfte mit diesen zusätzlichen Befugnissen Menschen, die nichts verbrochen haben, vorschreiben, dass sie bestimmte Orte nicht betreten oder verlassen dürfen und mit wem sie Kontakt haben. Wir sind besorgt, weil auch hier die fragwürdige Definition des Terrorismus aus § 8 Absatz 4 d.E. angewendet werden soll (dazu siehe 4.1.). Wir sehen eine Gefahr für freie Meinungsäußerung und zivilgesellschaftlichen Protest: **Die Maßnahme birgt ein großes Missbrauchspotential und keine wirksame Vorbeugung dagegen.** Grund für die Sorge sind auch, teils rechtswidrige, Durchsuchungen bei zivilgesellschaftlichen Organisation in NRW (Vgl. https://www1.wdr.de/nachrichten/ruhrgebiet/cybercrime-razzia-dortmund-nordstadt-100.html) und in anderen deutschen Bundesländern (https://netzpolitik.org/2018/gericht-urteilt-durchsuchung-bei-zwiebelfreunden-war-rechtswidrig/).

Ebenfalls alarmierend ist, dass der Entwurf augenscheinlich keine Höchstdauer vorsieht. **Ein lebenslängliches Kontaktverbot greift erheblich in die private und berufliche Lebensgestaltung eines Menschen ein.** Selbiges gilt für die Aufenthaltsvorgaben. Im Entwurf sind keine Beschränkungen für die Aufenthaltsvorgaben und Kontaktverbote erkennbar. D.h. es sind Szenarien denkbar, in denen dadurch Menschen z.B. in ihrer Erwerbstätigkeit eingeschränkt werden, weil ihr Arbeitsplatz in die „Verbotszone“ fällt. Deine derart umfassende Einschränkung der Freiheit steht in keinem Verhältnis zum eventuellen Nutzen.

3.5. Ingewahrsamnahme

Digitalcourage beurteilt die Höchstdauer des Gewahrsams, insbesondere die Dauer von bis zu sieben Tagen zur Identitätsfeststellung, als unverhältnismäßig hoch. Hier erschließt sich nicht, woran die Polizei beurteilen will, ob eine Person vorsätzlich ihre Identität verschleiert. **Eine Woche Gewahrsam beeinträchtigt das private und berufliche Leben einer Person empfindlich.** Es ist zu Erwarten, dass Bürgerinnen und Bürger, in vorauseilendem Gehorsam, ihre Identität preisgeben, auch wenn sie dazu nicht verpflichtet wären.

4. Zum Terrorismusbegriff und der Verhältnismäßigkeit

4.1. Terrorismus-Definition in § 8 Absatz 4 d.E.

Wie eingangs erwähnt, begrüßt Digitalcourage die Streichung der „drohenden Gefahr“. Nach dem Änderungsantrag soll als Definitionsgrundlage für eine „drohende terroristische Gefahr“ ein Straftatenkatalog dienen. Während einige der dort genannten Delikte einleuchten (z.B. §129a StGB Bildung terroristischer Vereinigungen) erscheinen andere sehr geringfügig im Verhältnis zu

den Maßnahmen, denen sie als Rechtfertigungsgrundlage dienen. So sind als Anlassstraftaten u.a. §305a StGB Zerstörung wichtiger Arbeitsmittel und §317 StGB Störung von Telekommunikationsanlagen genannt. Nach §305a können bereits Vergehen wie das Ablassen der Luft aus den Reifen eines Einsatzfahrzeugs der Polizei bestraft werden [Vgl. OLG Hamm, 08.07.1981 - 4 Ss 945/81]. Dein Akt des Terrors ist das nach der gängigen Definition nicht. Wir vermissen hier die Verbindung zwischen der Gesetzesbegründung („Terrorismusprävention“) und den Anlassstraftaten (Sachbeschädigungsdelikte). Ebenfalls verweist Digitalcourage erneut auf die Bezeichnung **„Sicherheitspaket I“. Es besteht Sorge, dass der Straftatenkatalog in einer folgenden Polizeigesetzreform noch erweitert werden könnte.**

4.2. Eingriffe im Vorfeld

In den bisher eingereichten Stellungnahmen wurde eine zu vage Definition der „drohenden Gefahr“ und „drohenden terroristischen Gefahr“ kritisiert. Damit wird ein Dogma der bisherigen polizeilichen Arbeit aufgeweicht, nach dem es zumindest eines Anfangsverdachts Bedarf, um überwachend oder repressiv tätig zu werden.

Beispielsweise schreibt Prof. Clemens Arzt (Stellungnahme 17/652): *„Der Begriff der drohenden Gefahr soll nun offenbar noch eine weitere Wahrscheinlichkeitsebene vor der Wahrscheinlichkeitsprognose gemäß dem Begriff der konkreten Gefahr ‚einziehen‘; es geht als um die (drohende) Wahrscheinlichkeit einer hinreichenden (= konkreten) Wahrscheinlichkeit des Schadenseintritts.“* **Während zwar die „drohende Gefahr“ und „drohende terroristische Gefahr“ keine einzelnen Absätze mehr im Entwurf einnehmen, wird die Prognose der „Wahrscheinlichkeit einer Wahrscheinlichkeit eines Schadens“ weiterhin ermöglicht.** Die entsprechende Formulierung findet sich nunmehr in den Paragraphen, die die jeweiligen Überwachungs- und Freiheitsentziehungsmaßnahmen regeln, beispielsweise in §20c d.E. (Staatstrojaner) *„[…]deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehharen Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat nach § 8 Absatz 4 begehen wird, […]“*. Die verfassungsrechtlich bedenkliche Gefährder-Definition wurde also nicht etwa entfernt, sondern lediglich an andere Stellen des Entwurfs verschoben.

Dadurch wird eine erhebliche Rechtsunsicherheit entstehen. Es ist nicht bekannt, auf welcher Basis die Prognose einer „Wahrscheinlichkeit einer Wahrscheinlichkeit eines Schadenseintritts“ stattfinden werden. Weiterhin stellt sich die Frage, wie diese Prognose nachvollziehbar dokumentiert werden soll. Somit kann auch niemand wissen, welches Verhalten erlaubt ist und welches sanktioniert werden kann. **Insofern ist an dieser Stelle die rechtsstaatliche Garantie der Bestimmtheit von Rechtsvorschriften nicht erfüllt** (Art. 20 Abs. 3 und Art. 103

Grundgesetz). Zahlreiche Studien belegen, dass Menschen dadurch verunsichert werden und sich konformistischer Verhalten (**„Chilling Effects“**). Freiheit und Bürgerrechte nehmen durch diese vorauseilende Selbstzensur Schaden. Besonders das Recht, sich frei zu informieren und das Recht auf freie Meinungsäußerung wird nach Einschätzung von Digitalcourage durch diese Rechtsunsicherheit und die daraus folgenden Chilling Effects eingeschränkt.
Daher können wir die Einschätzung der Fraktionen von CDU und FDP im Landtag NRW nicht teilen, dass die Bedenken gehört und der Entwurf verbessert wurde.

4.3. Trennungsgebot

Durch die Verlagerung der Polizeiarbeit ins Vorfeld von Straftaten verschwimmt die Grenze zur, von Digitalcourage als höchst fragwürdig eingeschätzten, Arbeit von Geheimdiensten.
Die Polizei hat weitreichende repressive Befugnisse, die zur Erfüllung ihrer Aufgaben notwendig sind. Eine Ausweitung der Befugnisse, sowohl der Überwachung als auch der Repressionsmaßnahmen, produziert besonders in Verbindung mit den Prognosebefugnissen (siehe 4.2.) über das Bestehen einer drohenden oder abstrakten Gefahr ein gefährliches Machtgefälle der Polizei gegenüber der Bevölkerung und eine insgesamt bedenkliche Machtfülle der Polizei.

4.4. Gefährdungslage

In der Gesetzesbegründung heißt es, die Bundesrepublik sei *„derzeit Aktionsraum für terroristische Anschläge insbesondere durch islamistische Täter“* und die Landesregierung *„fühlt sich den Bürgerinnen und Bürgern Nordrhein-Westfalens gegenüber verpflichtet, alle geeigneten und angemessenen Maßnahmen zu ergreifen, um ein sicheres Leben führen zu können.“*
Jedoch sind auf Bundes- wie Landesebene die Verbrechenszahlen in 2017 alles andere als alarmierend: **In NRW sank die Kriminalität** im Vergleich zum Vorjahr um 6,5 % [PKS NRW 2017]. Auf Bundesebene ist die Kriminalitätsrate auf dem niedrigsten Stand seit 25 Jahren [PKS Bund 2017]. Daher erschließt sich uns nicht, warum die polizeilichen Befugnisse erweitert werden müssen. Im Gegenteil ist Digitalcourage der Ansicht, dass es einer Wiederinstandsetzung von Grund- und Bürgerrechten eher Bedarf. Schließlich sind auf Landes- und Bundesebene in den vergangenen Jahren, unter dem Vorwand der Sicherheit, bereits umfangreiche und tiefgreifende Überwachungsmaßnahmen eingeführt worden. In ihrer Summe haben sie bereits ein Maß erreicht, das die Demokratie gefährlich nahe an einen autoritären Überwachungsstaat rückt.
Gleichzeitig ist unklar, ob die vorgeschlagenen Verschärfungen des Entwurfs überhaupt „geeignet und angemessen“ sind, Sicherheit herzustellen. Bei Videoüberwachung ist das nachweislich nicht der Fall. Auch bei der elektronischen Fußfessel zeigen viele Fälle, dass es eine

bloße Überwachungsmaßnahme ist, die wirkungslos ist. Es sind Fälle bekannt in denen Straftaten begangen wurden, trotz Einsatz einer elektronischen Fußfessel (Vgl. Stellungnahme des Chaos Computer Clubs an den niedersächsichen Landtag vom 7.8.2018). Staatstrojaner sind sogar eine greifbare Gefahr für die IT-Sicherheit.

4.5. Verhältnismäßigkeit

Die Befugnisse zur Überwachung und Freiheitsentziehung sind erheblich – besonders angesichts der **Verlagerung in ein Vorfeld des Verdachts, die viel Spielraum für Willkür lässt**. Einige der Maßnahmen sollen sogar bereits bei Verstößen auf Grundlage des bestehenden §8 (3) angewendet werden. Darin enthalten sind unter anderem Tatbestände aus dem BtMG und dem Aufenthaltsgesetz. Hierin lässt sich kein Zusammenhang zur Gesetzesbegründung erkennen, die auf eine Gefährdung durch Terrorismus verweist. **Darüber hinaus werden die Vorgaben des Bundesverfassungsgericht, z.B. zum BKA-G-Urteil bis aufs äußerste ausgereizt, wenn nicht überschritten.** Digitalcourage hält es für bedenklich, dass als Maßstab hier angesetzt wird, was das höchste Gericht als – in Ausnahmefällen! – eben noch zulässig ansieht. Ebenfalls rätselhaft ist, warum eine große Gefahr durch islamistischen Terror beschworen wird, während die polizeilichen Kriminalstatistiken dafür keinerlei Anhaltspunkte geben.

5. Fazit

Insgesamt sieht Digitalcourage **keine Notwendigkeit für eine Verschärfung** des Polizeirechts in NRW. Vielmehr wäre es nötig, Bürgerrechte zu stärken und nutzlose Überwachungsmaßnahmen wieder abzuschaffen. Digitalcourage betrachtet mit Sorge den Abbau der grundgesetzlich verbrieften Rechte und Freiheiten. Es sei hier erwähnt, dass vor allem auch Abwehrrechte gegen den Staat Sicherheit und Frieden langfristig gewährleisten. **Der Entwurf weist somit eine Diskrepanz zwischen Gesetzesbegründung und Maßnahmen auf. Es gibt keine Belege dafür, dass mehr Überwachung für mehr Sicherheit sorgt.** Selbst wenn sich Belege dafür fänden: Ohne einen Ausgleich, der Bürgerrechte stärkt, ist unserer Ansicht nach kein Spielraum für weitere Überwachungsmaßnahmen.

Digitalcourage verweist erneut auf die Empfehlungen zum Gesetzgebungsprozess in Punkt 2 dieser Stellungnahme. Bevor die dort genannten Voraussetzungen erfüllt sind, sollte nach Ansicht von Digitalcourage das Gesetzgebungsverfahren ausgesetzt werden. Die Schädigung bürgerlicher Freiheiten und Rechte übersteigen den mutmaßlichen Nutzen bei Weitem. **Eine Notwendigkeit und Angemessenheit der Verschärfungen ist nicht belegt.**