Niedersächsischer Staatsgerichtshof
Herminenstraße 31
31675 Bückeburg

DATUM

Abstrakter Normenkontrollantrag

der ….. (1/5 der Mitglieder des Landtages)

I.

Hiermit beantragen wir gem. Art. 54 Nr. 3 NV die Entscheidung des Staatsgerichtshofs über die Vereinbarkeit der §§ 12 Abs. 6, 17c Abs. 3 Satz 2, 21 Satz 2, 3, 30 Abs. 4 Satz 1, 32 Abs. 2, 3 Nr. 1, Abs. 4 Satz 4, Abs. 5, Abs. 7, § 33 a Abs. 2, § 33 d des Niedersächsisches Polizei- und Ordnungsbehördengesetz (NPOG), in Kraft getreten am 24. Mai 2019, mit der Niedersächsischen Verfassung.

II.

Mit der am 14.05.2019 beschlossenen und am 24.05.2019 in Kraft getretenen Novelle des Polizeigesetzes wurden die polizeilichen Eingriffsbefugnisse erheblich erweitert. Ob und inwieweit verschiedene Vorschriften des geänderten niedersächsischen Polizeirechts mit der Landesverfassung vereinbar sind, ist zwischen den Antragstellern, die den Fraktionen von SPD und CDU im Niedersächsischen Landtag angehören, und den Antragstellern, die den Fraktionen von Bündnis 90/Die Grünen und der FDP im Niedersächsischen Landtag angehören umstritten und wird von den letztgenannten Antragstellern bezweifelt.

Die Meinungsverschiedenheiten über bzw. Zweifel an der Verfassungsmäßigkeit der einzelnen Vorschriften ergeben sich aus folgenden Ausführungen, die maßgeblich auf den Stellungnahmen des Gesetzgebungs- und Beratungsdienstes des Niedersächsischen Landtages beruhen:

1. Zu § 12 Abs. 6 NPOG

> *„Die Polizei kann auf der Grundlage polizeilicher Lageerkenntnisse zur Verhütung von Straftaten von erheblicher Bedeutung mit internationalem Bezug jede im öffentlichen Verkehrsraum angetroffene Person kurzzeitig anhalten, befragen und verlangen, dass mitgeführte Ausweispapiere zur Prüfung ausgehändigt werden, sowie mitgeführte Sachen in Augenschein nehmen."*

Die „Schleierfahndung" ist in Form der verdachts- und ereignisunabhängigen Personenkontrolle nicht mit der Landesverfassung vereinbar und geht ist mit der Rechtsprechung des Bundesverfassungsgerichts zu den automatischen Kennzeichenlesesysteme nicht in Einklang zu bringen. Das liegt zum einen daran, dass die Regelung nicht auf einen konkreten Grenzbezug beschränkt ist, der gesetzlich in einer dem rechtsstaatlichen Bestimmtheitsgebot genügenden Weise gesichert ist, sondern Kontrollen im gesamten öffentlichen Verkehrsraum ermöglicht (vgl. dazu BVerfG, NJW 2019, 827, 839, Rn. 143 ff.). Zum anderen fehlt eine Anordnung zur Dokumentation der Entscheidungsgrundlagen. Da die Entscheidung über die Durchführung der Kontrollen allein im Innern der zuständigen Polizeibehörde auf der Grundlage von „Lageerkenntnissen" getroffen wird, ist eine solche Dokumentation im Hinblick auf die Nachvollziehbarkeit und gerichtliche Überprüfbarkeit der Maßnahme erforderlich (BVerfG, NJW 2019, 827, 840, Rn. 153 ff.).

2. Zu § 17c Abs. 2 Satz 3 NPOG

> *„Soweit es technisch möglich ist, ist sicherzustellen, dass innerhalb der Wohnung der betroffenen Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden."*

Es muss technisch sichergestellt werden können, dass innerhalb der Wohnung der betroffenen Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden. Wenn die heutige Technik dies nicht zulässt, so darf es als Mittel nicht eingesetzt werden (vgl. auch Löffelmann, BayVBl. 2018, 145, 152).
Durch die Regelung wird das Grundrecht auf Unverletzlichkeit der Wohnung aus (Art. 3 Abs. 2 NV i.V.m.) Artikel 13 Abs. 1 GG unter einen im Wortlaut des Grundgesetzes vorgesehenen Vorbehalt technischer Möglichkeiten gestellt. Bereits daher kann § 17c Abs. 2 Satz 3 NPOG keinen verfassungsrechtlichen Bestand haben. Es bleibt zudem offen, ob derzeit die technische Möglichkeit besteht, sicherzustellen, dass innerhalb der Wohnung der betroffenen Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden.

3. Zu § 21 Satz 2, 3 NPOG

„[2]In der richterlichen Entscheidung ist die höchstzulässige Dauer der Freiheitsentziehung zu bestimmen; sie darf

1. *in den Fällen des § 18 Abs. 1 Nr. 2 Buchst. a bei einer bevorstehenden terroristischen Straftat höchstens 14 Tage,*
2. *in den Fällen des § 18 Abs. 1 Nr. 2 Buchst. a bei einer sonstigen bevorstehenden Straftat höchstens zehn Tage und*
3. *in den übrigen Fällen höchstens sechs Tage*

beantragen.

[3] In den Fällen des Satzes 2 Nr. 1 ist eine Verlängerung der Dauer der Freiheitsentziehung durch das Gericht um einmalig höchstens 14 Tage und um weitere einmalig höchstens 7 Tage zulässig.“

Die Freiheitsentziehung ist eine der am stärksten in die Rechte der betroffenen Personen eingreifende Maßnahme und unterliegt der strikten Anwendung des Verhältnismäßigkeitsgrundsatzes (vgl. BVerfGE 128, 326, 372 f.). Da der Eingriff umso intensiver ist, je länger er dauert, gilt dies gerade auch für die zulässige Höchstdauer. Das Bundesverfassungsgericht hatte über die Gewahrsamshöchstdauer zu Gefahrenabwehr-zwecken zwar noch nicht abschließend zu entscheiden. Das Gericht hat aber im Rahmen einer Entscheidung zur Verfassungsmäßigkeit eines Unterbindungsgewahrsams ausgeführt, präventive Freiheitsentziehungen seien nur solange zulässig, wie sie zur Unterbindung der Anlasshandlungen erforderlich und zumutbar seien; daher könnten sie „in aller Regel nur von kurzer Dauer“ sein (BVerfG, B. v. 26. 6. 1997 - 1 BvR 126/91 -, juris Rn. 14; dazu auch Graulich in Lisken/Denninger, Hdb. d. PolR, 6. Aufl. 2018, E Rn. 552).

Vorliegend beträgt die Höchstdauer insgesamt 35 Tage und liegt folglich deutlich über der Zeitspanne von einer „kurzen Dauer“. Insoweit ist zu bedenken, dass eine „kurze Dauer“ keinesfalls länger als ein Monat sein kann. Die Zeitspanne von insgesamt 35 Tagen ist unverhältnismäßig lang und verletzt das Freiheitsgrundrecht - insbesondere, da in dem nämlichen Fällen die Voraussetzungen für eine Untersuchungshaft bei der Präventivhaft nicht vorliegen (es ist vielmehr ein „Minus“ zur Untersuchungshaft). Bei der Untersuchungshaft liegt ein Fall der notwendigen Verteidigung im Sinne des §140 StPO vor, bei der Präventivhaft hingegen wird der Person nicht einmal ein kostenloser Pflichtverteidiger zugeordnet.

Es liegt folglich ein unverhältnismäßiger Eingriff in das Freiheitsgrundrecht vor.

4. Zu § 30 Abs. 4 Satz 1 NPOG

„Über die Erhebung personenbezogener Daten mit besonderen Mitteln oder Methoden oder mittels verdeckt angefertigter Aufzeichnungen nach § 32 Abs. 2 ist die betroffene

Person nach Beendigung der Maßnahme zu unterrichten; dies gilt nicht für Auskunftsverlangen zu einfachen Bestandsdaten (§ 33 c Abs. 2 Satz 1 Nr. 1).“

Die Unterrichtungspflicht wurde hier auf die mit „besonderen“ Mitteln und Methoden erhobenen Daten beschränkt. Diese Beschränkung auf lediglich „besondere“ Mittel ist nicht mit den Artikeln 12 und 13 Abs. 1 und 2 der Richtlinie (EU) 2016/680 (JI-RL) vereinbar.

5. Zu § 32 Abs. 2 NPOG

"Eine verdeckte Anfertigung von Aufzeichnungen ist nur zulässig, wenn die offene Anfertigung dazu führen kann, dass die Straftaten an anderer Stelle, zu anderer Zeit oder in anderer Weise begangen werden.“

Hier ist bereits die Gesetzgebungskompetenz des Landes nicht gegeben. Welcher gefahrenabwehrrechtliche Zweck mit der verdeckten Aufzeichnung erfüllt werden soll, wenn die Straftat statt an anderer Stelle an der beobachteten Stelle begangen wird, erschließt sich nicht. Durch die verdeckte Datenerhebung dürfte ohnehin der mit der Videoüberwachung verbundene Abschreckungseffekt entfallen.
Auch eine Verhütung einer ausgezeichneten Straftat wäre nur mit unmittelbarem Eingriff der Polizei erreicht. Im Fall einer unmittelbaren Wahrnehmung durch die Polizei stellt sich aber die Frage, wozu dann die Aufzeichnung (zur Gefahrenabwehr) gebraucht wird; es reicht jedenfalls die Beobachtung. Warum die Beobachtung verdeckt erfolgen muss, obwohl der Täter dadurch nicht abgeschreckt wird, sondern erst „auf frischer Tat ertappt“ und dann vor Ort an der Straftat gehindert werden kann, ist daher nicht nachvollziehbar.
Eine Aufzeichnung, die allein oder hauptsächlich der Erleichterung der Strafverfolgung (sog. Strafverfolgungsvorsorge) dient, ist einer Regelung durch den Landesgesetzgeber nur zugänglich, soweit der Bundesgesetzgeber von der konkurrierenden Gesetzgebungskompetenz nicht abschließend Gebrauch gemacht hat, vgl. Art. 72 Abs. 1 GG. Unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts zur Telekommunikationsüberwachung (BVerfGE 113, 348, 371 ff.) und des VGH Mannheim zu verdeckten Bildaufzeichnungen außerhalb von Wohnungen (VGH Mannheim, a. a. O., Rn. 41) liegt es nahe, die Regelungen über die verdeckte Personenbeobachtung mittels technischer Mittel in der StPO (vgl. § 100 h StPO) insoweit als abschließend i.S.v. Art. 74 Abs. 1 Nr. 1 GG anzusehen.
Im Übrigen genügt der mit der verdeckten Videoüberwachung verbundene Grundrechtseingriff dem Verhältnismäßigkeitsgrundsatz nicht. Der Eingriff in das Recht auf informationelle Selbstbestimmung aus (Art. 3 Abs. 2 NV i.V.m.) Art. 2 Abs.1 i.V.m. Art. 1 Abs. 1 GG der beobachteten Person ist stark. Im öffentlichen Raum muss möglich sein, sich nicht, auch nicht an potentiell straftatgeneigten Orten, zu bewegen und seiner Individualität Ausdruck zu verleihen, ohne sich dabei stets potentiell beobachtet zu fühlen.

6. Zu § 32 Abs. 3 Nr. 1 NPOG

> *„Die Verwaltungsbehörden und die Polizei dürfen öffentliche Straßen und Plätze sowie andere öffentlich zugängliche Orte mittels Bildübertragung offen beobachten,*
> *1. wenn dort wiederholt Straftaten oder nicht geringfügige Ordnungswidrigkeiten begangen wurden und die Beobachtung zur Verhütung entsprechender Straftaten oder Ordnungswidrigkeiten erforderlich ist,“*

Das Recht auf informationelle Selbstbestimmung (Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG i. V. m. Art. 3 Abs. 1 S. 1 NV) wird wegen der mit dem Eingriff verbundenen Streubreite verletzt, wenn eine Überwachung bereits bei „nicht geringfügige Ordnungswidrigkeiten“ vorgenommen werden darf. Die Verhältnismäßigkeit ist folglich nicht gewahrt.

7. Zu § 32 Abs. 4 Satz 4 NPOG

> *„Die am Körper getragenen Bild- und Tonaufzeichnungsgeräte nach Satz 1 dürfen auch im Bereitschaftsbetrieb Aufzeichnungen anfertigen.“*

Die Vorabaufnahmen („PreRecording“) ist mit der Landesverfassung unvereinbar, weil dadurch auch Unbeteiligte gefilmt werden. Das PreRecording stellt einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung, das Recht am eigenen Bild oder das Recht am gesprochenen Wort dar und wahrt nicht den Verhältnismäßigkeitsgrundsatz.
Die Anfertigung von Vorabaufnahmen soll ohne weitere Voraussetzungen „im Bereitschaftsdienst“ (so Absatz 5 Satz 1 des Entwurfs) zulässig sein. Damit wird aber ein konkreter Eingriffsanlass nicht beschrieben; die Vorabaufnahmen können im Ergebnis jederzeit an jedem Ort erfolgen. Dies wird den Anforderungen des Bundesverfassungsgerichts nicht gerecht. Das Gericht hat für den Einsatz des Automatischen Kennzeichenlesesystems eine Eingriffsschwelle gefordert, die zur Rechtfertigung des Grundrechtseingriffs zumindest einen hinreichend konkreten sowie objektiv bestimmten und begrenzten Anlass voraussetzt (BVerfG, NJW 2019, 827, 833 f., Rn. 90 ff.). Da der Grundrechtseingriff im Fall von Bild- und Tonaufnahmen von Personen, die für 30 Sekunden gespeichert werden dürfen, eher intensiver ist als im Fall der automatischen Aufnahme (und ggf. sofortigen automatischen Löschung) des Autokennzeichens, gelten diese Anforderungen auch für die Vorabaufnahmen.

Problematisch ist zudem die einseitige Kontrolle der Bodycams. Allein die Polizistinnen und Polizisten bestimmen, ab wann aufgezeichnet wird. Außerdem können die Polizisten auch bestimmen, wann die Kameras wieder abgeschaltet werden. Es wird also stets an die subjektive Wahrnehmung und subjektive Einschätzung des betreffenden Polizeibeamten geknüpft sein, wann dieser (persönlich) ein Geschehen als gefährlich oder bedrohlich empfindet und wann dies (noch) nicht der Fall ist. Und dies kann durchaus unterschiedlich von den im Einsatz

befindlichen Polizeibeamten eingeschätzt werden. Ein solches „weiches“, weil zwangsläufig individuell subjektives Kriterium der persönlichen Einschätzung, ist denkbar ungeeignet zur Abgrenzung zwischen einem zulässigen und dem verfassungsrechtlich gerade nicht mehr hinnehmbaren Eingriff in persönliche Schutzrechte der von den Videoaufzeichnungen betroffenen Personen.

Zum anderen ist zu beachten, dass der Zweck der Vorabaufnahmen eher repressiver Natur sein dürfte. Jedenfalls ist die weitere Speicherung der Vorabaufnahmen schon theoretisch nicht mehr dazu geeignet, eine Gefahr abzuwehren, die Anlass für die Aufzeichnung war, oder eine entsprechende Straftat zu verhüten, sondern dient in erster Linie der strafrechtlichen Aufarbeitung des Geschehens (Nachbaur, VBlBW 2018, 97, 98; Schmidt, Diss. 2018, S. 124 ff.). Damit ist auch erneut die Gesetzgebungskompetenz zweifelhaft.

8. Zu § 32 Abs. 5 NPOG

„[1] Die Polizei kann im öffentlichen Verkehrsraum technische Mittel zur Erfassung von Kraftfahrzeugkennzeichen offen einsetzen

1. zur Abwehr einer Gefahr für die öffentliche Sicherheit,

2. auf der Grundlage polizeilicher Lageerkenntnisse zur Verhütung von Straftaten von erheblicher Bedeutung mit internationalem Bezug,

3. an einem in § 13 Abs. 1 Nr. 2 Buchst. a genannten Ort zur Verhütung der dort genannten Straftaten,

4. in unmittelbarer Nähe der in § 13 Abs. 1 Nr. 3 genannten gefährdeten Objekte zu deren Schutz oder zum Schutz der sich dort befindenden Personen, wenn Tatsachen die Annahme rechtfertigen, dass in oder an Objekten dieser Art Straftaten begangen werden sollen, und der Einsatz aufgrund der Gefährdungslage erforderlich ist oder

5. zur Verhütung der in § 14 Abs. 1 Satz 1 genannten Straftaten, wenn Tatsachen die Annahme rechtfertigen, dass solche Straftaten begangen werden sollen.

[2] Dabei dürfen auch Zeit und Ort der Bildaufzeichnung erfasst und eine Bildaufzeichnung des Fahrzeuges angefertigt werden, wenn technisch ausgeschlossen ist, dass Insassen zu sehen sind oder sichtbar gemacht werden können. [3] Das Kennzeichen ist sofort automatisiert mit vorhandenen Dateien abzugleichen, die der Suche nach Personen oder Sachen dienen oder in denen Kennzeichen nach § 37 oder nach anderen Rechtsvorschriften zur Kontrollmeldung ausgeschrieben sind. [4] Ist das Kennzeichen nicht in diesen Dateien enthalten, so sind die nach den Sätzen 1 und 2 erhobenen Daten sofort automatisiert zu löschen. [5] Gespeicherte Daten dürfen außer im Fall einer Ausschreibung zur Kontrollmeldung nicht zu einem Bewegungsbild verbunden werden. [6] Der Einsatz der technischen Mittel ist kenntlich zu machen. [7] Eine verdeckte

Datenerhebung ist nur zulässig, wenn durch eine offene Datenerhebung der Zweck der Maßnahme gefährdet würde.

Die Eingriffstatbestände in Satz 1, Nr. 1 und Nr. 2 sind verfassungswidrig sowie der Umstand, dass die Regelung keine Pflicht zur Dokumentation der Entscheidungsgrundlagen für den jeweiligen Einsatz des automatischen Kennzeichenlesesystems enthält.

Satz 1, Nr. 1 verstößt gegen den Verhältnismäßigkeitsgrundsatz, weil die Kennzeichenkontrolle dadurch nicht, wie es das BVerfG ((Beschl. v. 18.12.2018 - 1 BvR 142/15 -, NJW 2019, 827 [Bayern]; Beschl. v. 18.12.2018 - 1 BvR 2795/09, 1 BvR 3187/10 -, NJW 2019, 842 [Baden-Württemberg und Hessen]) verlangt, auf einen der Verhältnismäßigkeit genügenden Rechtsgüterschutz beschränkt wird (d. h. Leib, Leben oder Freiheit einer Person und der Bestand und die Sicherheit des Bundes und der Länder sowie nicht unerhebliche Sachwerte; vgl. BVerfG, a. a. O.). Die mit der „öffentlichen Sicherheit" nach Satz 1 Nr. 1 in ihrer Gesamtheit geschützte Unverletzlichkeit der Rechtsordnung genügt den Anforderungen an einen hinreichend gewichtigen Rechtsgüterschutz nicht.

Verfassungswidrig ist auch Satz 1 Nr. 2, weil der dortige Einsatz von automatischen Kennzeichenlesesystemen als Mittel der Schleierfahndung nicht auf einen konkreten Grenzbezug beschränkt ist, der gesetzlich in einer dem Bestimmtheitsgebot genügenden Weise gesichert ist. Das Bundesverfassungsgericht hat die automatischen Kennzeichenlesesysteme als Mittel der anlasslosen Schleierfahndung nur für gerechtfertigt gehalten (als Ausgleich für den Wegfall der innereuropäischen Grenzkontrollen; vgl. BVerfG, NJW 2019, 827, 839, Rn. 143 ff.), soweit diese in einem Grenzgebiet bis zu einer Tiefe von 30 km, an öffentlichen Einrichtungen des internationalen Verkehrs und auf Bundesautobahnen und Europastraßen durchgeführt werden. Eine solche, hinreichend bestimmte Regelung des Grenzbezuges fehlt vorliegend.

Satz 1, Nr. 5 lässt einen Ortsbezug bzw. einen Bezug zum Zweck der Kontrollstelle nicht erkennen, sondern bezieht sich lediglich auf die in § 14 Abs. 1 [Satz 1] genannten Straftaten, ohne eine örtliche Beschränkung entsprechend § 14 Abs. 1 dergestalt herzustellen, dass der Einsatz zur Verhütung der genannten Straftaten erforderlich sein muss, die Kennzeichenkontrolle also zur Unterstützung der Kontrollstelle eingesetzt wird.

Auch ist der Verhältnismäßigkeitsgrundsatz in Satz 3 nicht gewahrt. Diese Regelung ermächtigt dazu, die erhobenen Kennzeichen mit „Dateien abzugleichen, die der Suche nach Personen oder Sachen dienen oder in denen Kennzeichen nach § 37 oder nach anderen Rechtsvorschriften zur Kontrollmeldung ausgeschrieben sind". Das Bundesverfassungsgericht beschränkt den Datenabgleich auf die Einbeziehung von solchen Fahndungsbeständen, die für den jeweiligen Zweck der Kennzeichenkontrolle Bedeutung haben können.

Absatz 5 ist zudem unverhältnismäßig, da dieser ein flächendeckenden Einsatz der automatischen Kennzeichenlesesysteme nicht untersagt. Das gilt insbesondere für den Einsatz als Mittel der anlasslosen Schleierfahndung nach Satz 1 Nr. 2.

Verfassungswidrig ist schließlich, dass in Absatz 5 eine Anordnung zur Dokumentation der Entscheidungsgrundlagen fehlt. Da die Entscheidung über die Einrichtung in der Regel allein im Innern der zuständigen Polizeibehörde getroffen wird, ist eine Ermächtigungsgrundlage zum Einsatz von automatischen Kennzeichenlesesystemen nach der Rechtsprechung des Bundesverfassungsgerichts nur dann verhältnismäßig, wenn die Entscheidungsgrundlagen für die Durchführung einer solchen Maßnahme nachvollziehbar und überprüfbar dokumentiert werden, insbesondere im Hinblick auf die - behördlicher Konkretisierung bedürfenden - „Lageerkenntnisse“ und die Auswahl der einbezogenen Fahndungsbestände.

9. Zu § 32 Abs. 7 NPOG

> *„[1] Die Verwaltungsbehörden und die Polizei dürfen im öffentlichen Verkehrsraum zur Verhütung der Überschreitung der zulässigen Höchstgeschwindigkeit von Kraftfahrzeugen nach Maßgabe des Satzes 2 Bildaufzeichnungen offen anfertigen und damit auf einer festgelegten Wegstrecke die Durchschnittsgeschwindigkeit eines Kraftfahrzeugs ermitteln (Abschnittskontrolle). [2] Die Bildaufzeichnungen dürfen nur das Kraftfahrzeugkennzeichen, das Kraftfahrzeug und seine Fahrtrichtung sowie Zeit und Ort erfassen; es ist technisch sicherzustellen, dass Insassen nicht zu sehen sind oder sichtbar gemacht werden können. [3] Bei Kraftfahrzeugen, bei denen nach Feststellung der Durchschnittsgeschwindigkeit keine Überschreitung der zulässigen Höchstgeschwindigkeit vorliegt, sind die nach Satz 2 erhobenen Daten sofort automatisch zu löschen. [4] Die Abschnittskontrolle ist kenntlich zu machen.“*

Hier fehlt bereits die Gesetzgebungskompetenz des Landes. Absatz 7 lässt den Zweck der Datenerhebung nicht hinreichend deutlich werden. Ein präventiver Grund steht hierbei nicht im Vordergrund.
Es handelt sich um eine verbesserte Radarkontrolle um „Raser zu erwischen“. Die Feststellung der Überschreitung der Höchstgeschwindigkeit und deren anschließende Ahndung sind vorrangig und damit ist es eine repressive Maßnahme. Insbesondere da die Abschnittskontrolle das Unfallrisiko erhöht, da es den Verkehr verdichtet und somit am Ende der Kontrolle den Überholzwang erhöht. Somit liegt ein „Verhüten“ von Straftaten nicht vor.
Auch würde ein „Verhüten“ von Straftaten nicht die massenhafte Datenerhebung von Bürgern rechtfertigen. Es handelt sich um Eingriffe mit extrem großer Streubreite, die praktisch jeden treffen können. Es kann ein Gefühl des Überwachtwerdens entstehen.
Das Gewicht dieser Maßnahme wird dadurch erhöht, dass infolge der (wenn auch kurzfristigen) Speicherung der Daten, nämlich KFZ-Kennzeichens, Fahrtrichtung, Ort und Zeit, diese

in vielfältiger Weise ausgewertet, bearbeitet und mit anderen Informationen verknüpft werden können.
Von den Personen, die den Streckenabschnitt befahren, dürfte jedoch nur eine Minderheit gegen die rechtlichen Vorgaben, nämlich die Geschwindigkeitsbegrenzung, verstoßen. Die Section Control Maßnahme erfasst daher überwiegend Personen, die selbst keinen Anlass schaffen, dessentwegen die Überwachung vorgenommen wird.
Die Section Control und die damit einhergehende zumindest kurzfristige Speicherung von Daten von zahlreichen Autofahrern, die sich kein Fehlverhalten zuschulden haben kommen lassen, bewirkt folglich einen Eingriff in das allgemeine Persönlichkeitsrecht von erheblichem Gewicht.
Folglich sind die Anforderungen an die Bestimmtheit und Klarheit an die Rechtsgrundlage sowie die Verhältnismäßigkeit, auf welche sich der staatliche Eingriff stützt, hoch und müssen für den Bürger klar erkennbar sein, was vorliegend nicht der Fall ist.

10. Zu § 33 a Abs. 2 NPOG

„Die Überwachung und Aufzeichnung der Telekommunikation kann in der Weise erfolgen, dass mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird, wenn

1. *technisch sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und*
2. *eine Maßnahme nach Absatz 1 nicht ausreichend ist, um die Überwachung und Aufzeichnung der Telekommunikation in unverschlüsselter Form zu gewährleisten.“*

Der Einsatz eines Trojaners stellt einen tiefgehenden Grundrechtseingriff dar. Daher muss die Software und auch gegebenenfalls die Hardware höchsten Qualitätsanforderungen an die Software-Entwicklung im Allgemeinen und an die IT-Sicherheit im Speziellen genügen.
Vor der Entwicklung und dem eigentlichen Einsatz sind die Anforderungen an das System zu spezifizieren. Es fehlen im Gesetz konkrete Vorgaben zu den vorgeschriebenen Protokollierungspflichten beim Staatstrojanereinsatz.
Es fehlen Anforderungen an Hersteller und kommerzielle Anbieter der Software zur „Quellen-TKÜ“ (und auch zur „Online-Durchsuchung“), die eine Zusammenarbeit bei der technischen Überwachung regeln würden. Anforderungen an Staatstrojaner-Partnerfirmen sollen durch eine Rechtsvorschrift definiert werden. Anbieter von Staats-trojaner-Software müssen insbesondere in Hinblick auf ihre Fachkompetenz und ihre Vertrauenswürdigkeit geprüft werden.

Der Kernbereich der privaten Lebensgestaltung beschreibt die höchstpersönliche Sphäre eines Menschen. Der Schutz dieses Bereichs ist Teil des Schutzes der Menschenwürde und darf nicht mit der Ausrede einer technischen Nicht-Machbarkeit oder gar einer besseren

Praxistauglichkeit eines Trojaners zur Disposition gestellt werden. Das grundsätzliche Erhebungsverbot aus dem Kernbereich darf nicht wegen technischer Unzulänglichkeiten verwässert werden.

Staatstrojaner sollten nur bei besonderer Gefahr für Leib, Leben und Gesundheit eingesetzt werden dürfen.
Es fehlt zudem eine klare Regelung, dass die zur Quellen-TKÜ erforderliche Software so beschaffen sein muss, dass tatsächlich nur Daten des laufenden Telekommunikationsvorgangs erfasst werden können und explizit keine Informationen aus zurückliegenden Gesprächen oder Protokolldaten früherer oder noch nicht versendeter Kommunikation erfolgt.

Insgesamt stellt die Verwendung des Trojaners einen schwerwiegende Grundrechtseingriffe für die Betroffenen dar, der aufgrund präventiver Zwecke nicht gerechtfertigt ist.

11. Zu § 33 d NPOG

„(1) [1] Die Polizei kann mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben über

1. *eine in § 6 oder § 7 genannte Person zur Abwehr einer dringenden Gefahr,*
2. *eine Person, bei der Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat begehen wird, oder*
3. *eine Person, deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird,*

wenn dies zur Abwehr der Gefahr oder zur Verhütung der Straftat unerlässlich ist. [2] Für die technischen Vorkehrungen gilt § 33 a Abs. 3 entsprechend.
(2) Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.“
3) [1] Maßnahmen nach Absatz 1 bedürfen der Anordnung durch das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. [2] Im Antrag der Polizei sind anzugeben:

1. *die betroffene Person, soweit möglich mit Name und Anschrift,*
2. *eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,*
3. *Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes,*
4. *der Sachverhalt und*
5. *eine Begründung.*

[3] Die Anordnung ergeht schriftlich. [4] Sie muss die in Satz 2 Nrn. 1 bis 3 bezeichneten Angaben sowie die wesentlichen Gründe enthalten. [5] Im Übrigen gilt § 33 a Abs. 5 Sätze 5 bis 9 entsprechend.
(4) [1] Bei Gefahr im Verzug kann die Polizei die Anordnung treffen. [2] Absatz 3 Sätze 3 und 4 gilt entsprechend mit der Maßgabe, dass die Anordnung auch eine Begründung der Gefahr im Verzug enthalten muss. [3] Im Übrigen gilt § 33 a Abs. 6 Sätze 3 bis 8 entsprechend.

Die Befugnis im Gesetzesentwurf, Schadsoftware in sämtlichen vorstellbaren informationstechnischen Systemen anzuwenden, ist viel zu weitgehend. Der Bestimmtheitsgrundsatz ist nicht gewahrt.

Darüber hinaus ist die Möglichkeit, die Online-Durchsuchung bereits als Maßnahme der Gefahrenabwehr anzuwenden, aufgrund des hohen Grundrechtseingriffs nicht verfassungskonform.

Die Regelung zur Online-Durchsuchung beinhaltet zudem keinen ausreichenden Schutz für Dritte, die von der Maßnahme mitbetroffen sind. Die Regelung sieht vor, dass auch informationstechnische Systeme von Dritten infiltriert werden dürfen, sofern die Zielperson diese Systeme ebenfalls nutzt. Hierbei kann es neben den Risiken für das informationstechnische System selbst auch zur Offenlegung vieler weiterer schützenswerter Daten und Informationen Dritter kommen, etwa Zugangsdaten, Passwörter, Kommunikation von Berufsgeheimnisträgern sowie Daten aus dem Kernbereich privater Lebensgestaltung.