

Kritik
an den geplanten Änderungen des
Niedersächsischen Polizeigesetzes NPOG



Vorwort

Mit einem Hagel an Kritik und Bedenken und erst nach grundsätzlichen Änderungen aufgrund der strikten Zurechtweisung des niedersächsischen Landesparlaments durch den parlamentarischen Gesetzgebungs- und Beratungsdienst trat am 24.5.2019 das neue Niedersächsische Polizei- und Ordnungsgesetz (NPOG) in Kraft.

Die damalige Landesregierung, bestehend aus SPD und CDU, lobten dieses als modernstes Polizeigesetz, die damaligen Oppositionsparteien wie Bündnis90/Grüne und FDP sparten nicht an Kritik und Bedenken.

Die kraftvollste Opposition fand sich damals allerdings außerparlamentarisch in einem Bündnis zahlreicher gesellschaftlicher Vereine und Gruppen, dem Bündnis #noNPOG.

Nur sechs Jahre später, im Sommer 2025 begann die nun neue aus SPD und Bündnis90/Grünen bestehende Landesregierung mit dem Anlauf einer erneuten und sehr umfangreichen Änderung an dem von uns im folgenden als Niedersächsisches Polizeigesetz bezeichneten NPOG.

Doch die rot-grüne Landesregierung handelte zunächst nur halb-öffentlich und hinter der Öffentlichkeit gegenüber verschlossenen Türen. Wurde das neue Polizeigesetz zwar medial angekündigt, hielt sie den bereits bestehenden Gesetzentwurf vor den Menschen im Land noch bis zum letztmöglich legalen Zeitpunkt geheim. Erst am 17. November 2025 veröffentlichte das Innenministerium unter der als polizeifreundlich bekannten SPD-Innenministerin Behrens den Entwurf, alsobald gefolgt von der über das Knie gebrochenen ersten Lesung im Parlament am 19. November 2025 – nur zwei Tage danach.

Und auch im folgenden glänzte das Ministerium durch beinahe maximale Nichtoffenheit, wollte und will die von den elitär ausgesuchten Verbänden zuvor eingereichten Stellungnahmen nicht veröffentlichen und gab nur widerwillig – aber immerhin! – die Synopse zu den geplanten Änderungen heraus. Die Synopse ist eine Gegenüberstellung vom alten zum neuen Gesetzestext – ohne diese ist die in der Drucksache 19/8942 selbst für rechtlich gebildete Experten nahezu undurchdringbar.

Seither ist es im medial-öffentlichen Raum weitgehend still geblieben, Kritik ist auch nicht von den parlamentarischen Oppositionsparteien zu erwarten, die (namentlich CDU und „AfD“) den Polizeibehörden gerne sogar noch viel weiter gehende Befugnisse einräumen möchten.

Mit Blick auf die „AfD“ vermag man darin die Hoffnung zu erkennen, im Falle einer künftigen Beteiligung an der Landesregierung dann bereits die „richtigen“ Hebel in der Hand zu halten, um ihr eigenes mehr oder weniger verstecktes faschistisches Programm schein-legal durchsetzen zu können und ihnen umliebsame Menschen und Gruppen unterdrücken und mindestens mundtot machen zu können.

Wir vom freiheitsfoo haben große Bedenken vor dem geplanten weiteren bedeutsamen Aufbohren polizeilicher Freiheiten. Ein Zurückschrauben der Befugnisse von Polizei und Geheimdiensten hat es in den letzten Jahrzehnten dagegen so gut nie gegeben. Das kann bei ganz nüchterner Betrachtung so nicht richtig sein und kein gutes Ende nehmen.

Auf den nachfolgenden Seiten versuchen wir Paragraph für Paragraph aufzuzeigen, was die Änderungen im Einzelnen bedeuten und welche Bedenken wir dabei haben.

Unsere Gruppe freiheitsfoo entstand 2013 aus der Ortsgruppe Hannover des Arbeitskreises Vorratsdatenspeicherung, formiert in 2007.

Mit Blick auf unsere jahrzehntelange Erfahrung mit der Einbringung von Sachkritik aus der Zivilgesellschaft in den parlamentarischen Betrieb – sei es in Brüssel, Berlin, Kiel, im Saarland und vor allem in Hannover – wissen wir, dass unsere Beiträge in aller Regel nur auf taube Ohren stoßen und im Großen und Ganzen keinen Niederschlag in die resultierende Gesetzgebungsarbeit finden. Sie dienen den Parlamenten und ihren Parteien – egal welcher couleur – sogar vielmehr als Feigenblatt, die dann stolz darauf hinweisen können, die „Zivilgesellschaft“ doch beteiligt zu haben.

Zugleich spüren wir, dass in diesen Zeiten des Wandels in einer zunehmend von rechten, populistischen bis zu faschistischen Strömungen dominierten medialen Welt die kritischen Stimmen an – derzeit bundesweit grassierenden – Verschärfungen des Polizeirechts umso wichtiger sind.

Und darum dieses Papier. Dem wünschen wir aufmerksame Leserinnen und wirksame Verbreitung.

Unsere Kritik wird den Leserinnen nicht wie aus einem Guß, also in unterschiedlicher Breite und mit unterschiedlichem Stil erscheinen. Sie ist auch lückenhaft und unvollständig. Verschiedene Einzelpersonen haben daran gearbeitet und innerhalb des freiheitsfoos erheben wir nicht den Anspruch, mediale oder optische Professionalität an den Tag zu legen. Für solche Inhomogenitäten bitten wir als Menschen, die aus eigenem Interesse, ohne Bezahlung, in ihrer z.T. nächtlichen Freizeit und ohne parteipolitischen Hintergrund arbeiten, um Nachsicht.

2. März 2026

Inhaltsverzeichnis

Quellen.....	5
Anmerkungen abseits der geplanten konkreten Änderungen.....	6
§2 - Begriffsbestimmungen.....	9
§32 - Datenerhebung durch den Einsatz technischer Mittel bei öffentlichen Veranstaltungen und im öffentlichen Raum.....	10
§32a - Mobile Bild- und Tonaufzeichnungsgeräte.....	14
§32b - Biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen.....	23
§32c - Nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet	25
§32d - Einsatz von unbemannten Fahrzeugsystemen.....	26
§32e - Einsatz technischer Mittel gegen unbemannte Fahrzeugsysteme.....	28
§33 - Schutz des Kernbereichs privater Lebensgestaltung.....	29
§33a - Datenerhebung durch Überwachung der Telekommunikation.....	30
§33b - Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten, Unterbrechung der Telekommunikation.....	31
§33d - Verdeckter Eingriff in informationstechnische Systeme.....	32
§34 - Datenerhebung durch längerfristige Observation.....	33
§35 - Einsatz heimlicher Mittel außerhalb von Wohnungen.....	34
§35a - Einsatz heimlicher Mittel in Wohnungen.....	35
§37 - Ausschreibung zur polizeilichen Beobachtung.....	36
§38 - Weiterverarbeitung personenbezogener Daten, Zweckbindung.....	37
§38a - Kennzeichnung in polizeilichen Informationssystemen.....	38
§39 - Weiterverarbeitung personenbezogener Daten zu anderen Zwecken.....	39
§39a - Weiterverarbeitung personenbezogener Daten zu besonderen Zwecken.....	40
§41 - Datenübermittlung im innerstaatlichen Bereich.....	41
§41a - Datenübermittlung zum Zwecke einer Zuverlässigkeitsüberprüfung.....	42
§43 - Datenübermittlung im Bereich der Europäischen Union und deren Mitgliedstaaten.....	43
§43a - Datenübermittlung der Polizei im internationalen Bereich.....	44
§45a - Automatisierte Datenanalyse.....	45
Impressum.....	47

Quellen

Aktueller Gesetzentwurf:

https://www.landtag-niedersachsen.de/drucksachen/drucksachen_19_10000/08501-09000/19-08942.pdf

Aktuell gültiger Gesetzestext:

<https://voris.wolterskluwer-online.de/browse/document/6397c30a-a372-35db-8e92-694ba015c7c9>

Synopse:

<https://wiki.freiheitsfoo.de/uploads/Main/20251128-Synopse-NPOGnovelle.pdf>

Anmerkungen abseits der geplanten konkreten Änderungen

Den NPOG-Änderungsentwurf nach Nds. LT-DS 19/8942 bezeichnen wir im folgenden als NPOG-ÄE.

Zu Beginn möchten wir einen Blick auf das werfen, was bereits im Zuge der Entstehung des NPOG 2018-2019 kritisiert worden ist und im NPOG-ÄE keine Erwähnung findet. Wir halten es insofern für besonders erwähnenswert:

- Es soll auch zukünftig keine wirklich unabhängige Stelle zur Untersuchung von Polizeigewalt-Verdachtsfällen geben. Dabei ist das aktueller denn je, siehe bspw. hier: <https://taz.de/Kriminologie-ueber-Bochumer-Polizeischuesse/!6130900/>
- Der Niedersachsen-Trojaner („Staatstrojaner“) soll nicht abgeschafft werden. Im Gegenteil soll sein unseliger Einsatzbereich und dessen Zulässigkeit sogar noch ausgebaut werden.
- Auch werden die Elektroschocker-Waffen der Polizei, die Taser nicht abgeschafft. Und das, obwohl es seit Inkrafttreten des NPOG am 24.5.2019 bundesweit alleine sieben Tote durch Polizeitaser gegeben hat: <https://polizeischuesse.cilip.de/taser>

Einen der Toten durch Polizeitaser gab es in Niedersachsen.

Und in diesem konkreten Fall war es sogar so, dass die Polizeidirektion Hannover den Einsatz des Tasers zunächst der Öffentlichkeit gegenüber verschwiegen hat, also eine Vertuschungsabsicht im Raume steht!

Weitere Fragen zum Einsatz der Taserwaffen in Niedersachsen ließ das Nds. Innenministerium als „geheimhaltungsbedürftig“ einstufen und verhinderte damit aktiv eine öffentliche Debatte zur Sache: <https://freiheitsfoo.de/2021/10/09/toedlicher-tasereinsatz-nds-geheimhaltungsbeduerftig/>

Aber selbst davon unabhängig: Die Betrachtung der dokumentierten Fälle von Toten durch Polizei-Elektroschockwaffen zeigt deutlich, dass die Umsetzung der gut gemeinten Einsatzkriterien (kein Einsatz gegen Kinder, Schwangere, Menschen unter Drogeneinfluss) praktisch nicht eingehalten werden können ... und deswegen Menschen zu Tode kommen. Da bleibt nur eins: Taser gehören verboten und nicht ausgeweitet, wie es sich die DPolG in der aufkeimenden Debatte um die NPOG-Novelle so gerne wünscht: <https://www.dpolg.de/aktuelles/news/dpolg-fordert-einfuehrung-des-tasers/>

Und bei dieser Gelegenheit noch weitere Nachfragen an die Landesregierung:

- Warum wurde Polizistinnenkennzeichnung noch immer nicht umgesetzt und so lange verzögert? Die Innenministerin scheint dafür verantwortlich zu sein, bezeichnete sie die Umsetzung des

Koalitionsvertrags doch schon früh als „nicht so wichtig“. <https://wiki.freiheitsfoo.de/pmwiki.php?n=Main.Polizisten-Kennzeichnungspflicht-NDS> Welches Weltbild steckt hinter so einer Haltung?

- Wo bleibt endlich das im Koalitionsvertrag versprochene Transparenzgesetz/Informationsfreiheitsgesetz? Wir haben dazu seit Beginn der Arbeit der aktuellen rot-grünen Landesregierung dazu immer wieder nachgefragt und wurden vertröstet, dessen Bedeutung als zweitrangig herabgewürdigt. Das Bestreben, solch ein bürgerinnenfreundliches und demokratienahes Gesetz zu verankern ist schon mehr als 13 Jahre alt! <https://wiki.freiheitsfoo.de/pmwiki.php?n=Main.Transparenz-Buendnis-Nds>
<https://wiki.freiheitsfoo.de/pmwiki.php?n=Main.Nieders%e4chsische-Transparenzgesetz>
- 2019 hieß es noch bei der Schaffung des NPOG, dass das jetzt das endlich nötige achso moderne neue Polizeigesetz für Niedersachsen sei. Und nun hat sich laut NPOG-ÄE-Begründung erneut "umfangreicher Änderungsbedarf ergeben". Wie das? Die u.a. erwähnte Umsetzung der EU-Datenschutz-Richtlinie 2016/680 wurde damals schon angemahnt und aus Bequemlichkeit oder anderen parteipolitischen Gründen einfach wegnoriert. Damit hat man sich den Reformbedarf in Teilen selber zuzuschreiben, aber das will hier keiner ehrlich zugeben.

Ausdrücklich möchten wir dann noch folgende Frage in den öffentlichen Debattenraum stellen:

Welches Missbrauchspotential birgt das neue NPOG bei etwaiger zukünftiger parlamentarischer Beteiligung rechtsextremer Parteien? Kann mit Blick darauf eine derartige erneute Befugnisausweitung der Polizei verantwortet werden?

Weiter nun mit der Einzelkritik am NPOG-ÄE:

§2 - Begriffsbestimmungen

Hier wird ein vollständig neuer Straftatbestand eingeführt: Die "Vorfeldstraftat" (BVerfG-Neusprech aus BKA-Urteil 9.12.22).

Einfacher zu merken als „CrimeThink“, eine Vokabel, die George Orwell mit seinem „1984“ bereits gesetzt hat.

Die Einführung dieser Straftat in den Straftatkatalog des §2 NPOG öffnet einer willkürlichen Auslegung Tür und Tor.

§32 - Datenerhebung durch den Einsatz technischer Mittel bei öffentlichen Veranstaltungen und im öffentlichen Raum

"Intelligente Videoüberwachung", Verhaltensmustererkennung.

Die so genannte "intelligente Videoüberwachung (VÜ)" wird seitens der Polizeivertreter schon lange gefordert. Die Idee dahinter ist, dass Kameras zunächst grundsätzlich ohne den Einfluss von Polizeimenschen einen Raum oder Fläche überwachen und selbsttätig mittels einer Software zu erkennen versucht, ob dort etwas geschieht, das den Einsatz der Polizei erforderlich macht. In dem Fall meldet sich das System, so dass Polizeibeamtinnen ggf. eingreifen können.

Soweit die Theorie.

Der Sinn und die Effektivität sind jedoch zweifelhaft.

Ein Praxistest solcher Anlagen in Mannheim blieben ohne nachweisbare Evidenz (<https://netzpolitik.org/2025/verhaltensscanner-im-mannheim-hier-wird-die-ueberwachung-getestet-die-so-viele-staedte-wollen/>).

Ein weiteres Negativbeispiel für den Einsatz solcher Technik findet sich in Hamburg, dort eingesetzt am Hansaplatz. Siehe hier: <https://netzpolitik.org/2025/ki-kameras-in-hamburg-schaufenster-in-die-zukunft-der-polizeiarbeit/>

Es gab sogar in Niedersachsen in 2021 ein Versuchsprojekt, wo diese Technik an Straf- oder Untersuchungsgefangenen in Gefängnissen ausgetestet werden sollte. LT-Antrag: https://www.landtag-niedersachsen.de/drucksachen/drucksachen_18_10000/08501-09000/18-08729

Die damalige Landesdatenschutzbeauftragte kritisierte das damals mit scharfen Worten: <https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/einsatz-von-kunstlicher-intelligenz-im-justizvollzug-nur-unter-wahrung-der-personlichkeitsrechte-198588.html> Es wurde damals eine Evaluation des Experiments angekündigt, von der später aber nichts mehr zu hören oder erfahren war.

Die Einführung solcher Technik, mit der die Politiker Handlungsaktivität meinen beweisen zu können führt zu weniger "menschlicher" Aufsicht über VÜ-Bilder. Sie bildet weiter unbewusst ein unbegründetes

Vertrauen in Technik: bzw. im Alltag verlässt man sich auf diese. Die Technik führt zu mehr Videoüberwachung im öffentlichen Raum (ÖR), denn nun meint man ja auch dank der Technik mehr als bisher die von den Kameras erzeugten Bilder im RealTime-Modus ausreichend gut überwachen zu können. Die Gesetzesbegründung ist an Haaren herbeigezogen (i.e.: anhaltende Terrorismus-Bedrohung, gewaltbereiter Extremismus, organisierte Kriminalität (OK)).

Es wird nicht geklärt, woher (auf legale Weise und in ausreichender Realitätsnähe und in größerem Umfang!) Trainingsdaten für das Algorithmen-Training kommen sollen. Diese Frage ist nicht trivial sondern es scheint vielmehr gar nicht möglich unter Beachtung von EU-KI-Regeln. Siehe hierzu: <https://algorithmwatch.org/de/gutachten-datenbank-biometrie-gesichtserkennung/> .

So oder so handelt es sich bei der Videoüberwachung um einen bedeutsamen Eingriff in die Persönlichkeitsrechte aller von den Kameras erfassten Menschen. Der von der Maßnahme erhoffte Erfolg bei der Prävention (nicht Strafverfolgung!) ist dem gegenüber ins Verhältnis zu setzen und dann abzuwägen. Da keine stichhaltigen Erfahrungen oder Studien zur Effektivität "intelligenter Videoüberwachung" vorliegen, kann eine solche Abwägung gar nicht erst stattfinden.

Dass Videoüberwachung (egal ob durch Menschen oder Maschinen) auf die davon betroffenen Menschen jedoch das Potential hat, deren Ausübung grundgesetzlicher Freiheiten (u.a. Versammlungsfreiheit, freie Meinungsäußerung) markant zu beschneiden – das ist unbestritten.

Besonders perfide und bislang ganz undiskutiert: Diese Form der dauerhaft die Menschen beobachtenden Überwachungskameras dürfen auch an Drohnen angebracht werden.

Hier (wie auch für andere Novellen-Teile) an den Haaren herbeigezogene und floskelhafte Notwendigkeitsbegründung: "Aufgrund der anhaltend hohen Bedrohungslage durch Terrorismus, gewaltbereiten Extremismus und organisierte Kriminalität bedarf es neuer gesetzlicher Grundlagen für den Einsatz moderner technischer Einsatzmittel." Ad 1 fehlt es an Grundlage und ad 2 siehe bspw. hier die fehlende Evidenz/Signifikanz: <https://taz.de/Lagebild-Organisierte-Kriminalitaet/!6126212> (ganze 65 Ermittlungsverfahren zur OK der nds. Polizei in 2024).

Die Gesetzesbegründung setzt ein falsches Signal:

"Die intelligente Videoüberwachung ist jedoch deutlich effektiver, da typische menschliche Ermüdungserscheinungen bei dauerhafter Überwachungstätigkeit durch intelligente Videoüberwachung minimiert werden. Um Ermüdungserscheinungen zu minimieren, ist erforderlich, dass das vorhandene Personal in möglichst kurzen Zeiträumen ausgetauscht wird. Durch den Einsatz der neuen Technik wird das

vorhandene Personal hingegen dadurch entlastet, dass dieses nur noch in bestimmten „Alarmfällen“ tätig werden muss.“

Bedeutet: Man rückt die Beamt*innen ab von den Monitoren und will sich mehr oder weniger ganz auf die Technik und deren (hoffentlich) funktionierende "Intelligenz" verlassen, erkennt möglicherweise abstruse von der KI nicht auswertbare Gefahrensituationen nicht mehr rechtzeitig. In anderen Worten: Die Installation von Videoüberwachung verspricht (nach Meinung der dafür verantwortlichen Stellen) einen Zugewinn an Sicherheit – die Verbesserung der persönlichen "Sicherheitsempfindens" wäre jedenfalls kein verfassungsrechtlich zulässiger Erlaubnisgrund für Videoüberwachung. Tatsächlich handelt es sich dabei aber um ein falsches Versprechen. Im Gegenteil mögen sich die Menschen dadurch sogar effektiveres Erscheinen von Polizei oder anderen Helfern im tatsächlichen Falle einer gefährlichen Situation erwarten, die dann aber gar nicht erfolgt.

Und an dieser Stelle muss noch auf einen weiteren Punkt hingewiesen werden, nämlich die "false-positive-Meldungen" der KI, die die Überwachungsbilder überwacht. "False-positive" meint, dass die KI alarmierend auf einen möglicherweise gefährlichen Vorgang hinweist, der sich dann aber als harmloser entpuppt. Je öfters solche Falschalarme gegeben werden, umso weniger ernst nehmen die Polizisten die Technik, was ebenfalls zum gegenteiligen als den beabsichtigten Effekt führen kann.

Wie fehleranfällig die Technik sein kann beweist allein das Südkreuz-Versuchsprojekt an einem Berliner Bahnhof. Dort ging es zwar um biometrische Überprüfung und Erkennung der von den Kameras erfassten Menschen (siehe in unserem Kontext auch den §32b NPOG-ÄE), aber das Prinzip der Nicht-Fehlerfreiheit der "KI"-Technik und deren durchaus sehr negativ ausfallend könnenden Folgen für die von der Überwachung betroffenen Menschen sind die gleichen. Siehe dazu die Kritik des CCC zum Südkreuz-Experiment: <https://www.ccc.de/en/updates/2018/debakel-am-suedkreuz>

Man behauptet in der Begründung, es gäbe keine "erhöhte Eingriffsintensität" gegenüber "konventioneller" VÜ. Das ist Unsinn: Menschen müssen/können befürchten (zusätzlich zu bisherigen Bedenken bei VÜ), dass bei "intelligenter VÜ" (überhaupt ein unsinniges Wortgebilde, fast schon Neusprech) durch individuell ungewöhnliche oder eigenartige Verhaltensweisen völlig unnötigerweise in den Fokus der "VÜ-Intelligenz" zu geraten und somit auch in den Fokus der Polizei. Das führt effektiv zu selbstaufgelegten Freiheitseinschränkungen, zur Schere im Kopf, zur Beeinträchtigung der persönlichen Entfaltung und des freien Lebens und zur Diskriminierung von Gruppen, die nicht in das Bild "normaler" Menschen im Sinne des Trainingsmaterials passen.

Bemerkenswertes zum Schluss: Sogar die GdP (!) fordert hier eine Einschränkung der Regelungen zur "intelligenten VÜ" bzw. eine genauere Begrenzung der zu erfassenden Verhaltensmuster. Das kümmert das MI indes wenig.

§32a - Mobile Bild- und Tonaufzeichnungsgeräte

Die Regelungen zu Körperkameras (Bodycams) erhalten hiermit einen eigenen Paragraphen. Die vorher weniger umfänglichen Regelungen waren bislang im §32 untergebracht.

Es geht um die Ausweitung des Einsatzes von Bodycams (mit 30s Vorlaufaufzeichnung. u.u. Einsatz auch in Wohnungen, evtl. automatisches Einschalten bei Pistolen-Zückung, das aber freibleibend.)

Sämtliche Probleme und Kritik aus 2019 zur Thematik Bodycams bleiben wortlos unberücksichtigt. (z.B. Auskunft- und Aushändigungsrechte zu den Aufzeichnungen für die von den Aufzeichnungen Betroffenen. Wer wacht über die Daten, hat also die Macht darüber? Forderung neutraler Datensicherungs-Stelle. Wer darf wann/wie/warum löschen? etc.)

Der Einsatz der Bodycams ist eine Soll-Bestimmung, kann von Betroffenen also nicht verlangt werden und aggressive Polizist:innen können bei ihnen unangenehmen Szenen die Kamera einfach aus lassen

Der Einsatz in Wohnungen soll "zum Schutz von Polizist*innen" dienen - wie macht eine Bodycam das?

Dem Einsatz in Wohnungen kann (unter Bedingungen, tralala) widersprochen werden, aber offenbar erst, wenn die Cams schon laufen, oder? Das betrachten wir als praxisferne Vorstellung.

Wir möchten an dieser Stelle ausdrücklich auf unsere bereits umfangreiche Kritik an Bodycams aus 2018 (dort im Dokument ab Seite 14) hinweisen

(<https://wiki.freiheitsfoo.de/uploads/Main/20180728Stellungahme-freiheitsfoo-NPOG-anon.pdf>), die unter anderem unsere Kritik aus der Stellungnahme an den Landtag Schleswig-Holstein aus 2016 anknüpft (<https://wiki.freiheitsfoo.de/uploads/Main/20160427Stellungnahme-Bodycams-SchleswigHolstein-anon.pdf>).

Hier die Auszüge daraus, es handelt sich dabei um ganz grundsätzliche und nach wie vor gültige Kritik an der Ausrüstung der Polizei mit Bodycams:



Die bisherigen Einsätze solcher Kamerasysteme in anderen Bundesländern haben - anders als von den Bodycam-Befürwortern fälschlicherweise immer wieder öffentlich behauptet - überhaupt keinen Nachweis eines sinnvollen Einsatzes dieser Systeme erbracht.

Dass beispielsweise die Rahmenbedingungen des Pilotprojektes in Hessen derart unprofessionell gelegt worden sind, dass überhaupt keine Aussage über die Effekte von Bodycams getroffen werden kann, weil (unter anderem) die Polizeikräfte des Pilotprojektes im Vorfeld eine besondere Ausbildung in Sachen Deeskalation erhalten haben und sich somit ein Vergleich mit anderen Polizeistreifen nicht ziehen lassen kann, haben wir in unserer Stellungnahme an den schleswig-holsteinischen Landtag ausführlich dokumentiert.

Daraus möchten wir in Kürze lediglich unsere Kernhaltung und deren Begründung zitieren:

„Wir lehnen den Einsatz von „Bodycams“ („Körperkameras“), also i.A. kleinen, an der Uniform der Polizeibeamten und -beamtinnen befestigten Kameras mit Aufzeichnungsfunktion grundsätzlich ab – erst recht dann, wenn diese Technik allgemein und anlasslos vorgehalten und eingesetzt werden können soll.

Wir begründen unsere Haltung in der Hauptsache wie folgt:

I.) Der Einsatz von Bodycams greift – unabhängig von der Frage, ob die Kameras in Betrieb sind oder nicht – tief in die Persönlichkeitsrechte derjenigen Menschen ein, die den damit ausgerüsteten Polizeibeamten begegnen.

II.) Bodycams führen zu einer Erhöhung des allgemeinen Überwachungsdrucks, der auf allen Menschen lastet, die sich im öffentlichen Raum bewegen.

III.) Bodycams erzeugen eine zusätzliche Distanz zwischen den Menschen bzw. Bürgern des Landes und den Polizeibeamten, denen sie begegnen. Das führt zu einer Entfremdung, zu mehr Misstrauen, zu weniger „Miteinander“ und zu einer allgemeinen Verringerung der Akzeptanz der Polizei und deren Handeln.

IV.) Die Einführung von Bodycams stellt nichts anderes als eine weitere Eskalationsstufe im „Überwachungs-Rüstungs-Wettlauf“ zwischen staatlichen Autoritäten einerseits und den Menschen bzw. Bürgern auf der anderen Seite dar.

V.) Eine Einführung von Bodycams wäre nichts anderes als die Manifestierung einer weiteren Facette des Obrigkeitsstaates, seine Bürger bei staatlichen Handlungen jederzeit und allumfassend zu kontrollieren. Unsere Vorstellung eines gesellschaftlichen, friedlichen Zusammenlebens ist eine andere und wir lehnen uns

dabei an eine Äußerung des Hannoveraner NS-Widerstandskämpfers Otto Brenner an: "Nicht Ruhe, nicht Unterwürfigkeit gegenüber der Obrigkeit ist die erste Bürgerpflicht, sondern Kritik und ständige demokratische Wachsamkeit." Der Einsatz von Bodycams wirkt repressiv und mag aus der Sicht der Befürworter zu "mehr Kooperationsbereitschaft gegenüber den Polizeibeamten" führen, wie es seitens der hessischen Polizei gebetsmühlenartig vorgetragen wird. Das mittels Videoüberwachungs-Repression erzwungene Duckmäusertum bewirkt tatsächlich allerdings genau so wenig "Kooperationsbereitschaft" wie "Akzeptanz". Beide so sehnlichst gewünschten Effekte beruhen nämlich auf Freiwilligkeit und einem Handeln auf gemeinsamer Augenhöhe."

Und auch:

"Viele praktische Fragen beim Einsatz von Polizei-Bodycams bleiben offen oder werden gar nicht erst gestellt:

- Wie kann eine den Anforderungen des technischen Datenschutzes genügende Kennzeichnung der mit Bodycams ausgerüsteten Polizeibeamten aussehen?
freiheitsfoo-Stellungnahme zum NPOG-E Seite 15 von 36
- Ist eine den Kennzeichnungsregeln genügende Praxis überhaupt denk- und umsetzbar, die allen Passanten – egal aus welcher Richtung und in welchem Tempo sich den Bodycam-Polizisten nähernd – eine rechtzeitige Wahrnehmung der potentiellen Videoüberwachung und die dazugehörigen Chance zum Ausweichen – denn das ist der rechtliche Hintergrund der Videoüberwachungskennzeichnung! – ermöglichen kann?
- Wie fühlen sich diejenigen Polizeibeamte, die eine entsprechende Kennzeichnung mit sich tragen müssen und wie verändert diese Maßnahme ihr Handeln und ihren Arbeitsalltag?
- Wie und wo werden die Daten gespeichert?
- Werden die Daten auf den Informationsspeichern verschlüsselt abgelegt und wenn ja, handelt es sich um eine ausreichend gesicherte und zugleich praktikable und sinnvolle Form von Datenverschlüsselung?

- Wie sind die Zugriffsregeln auf die Daten definiert: Darf oder soll z.B. der die Bodycam tragende Polizeibeamte ein Recht oder die Möglichkeit zur Entscheidung darüber besitzen, welche Bilder und Aufzeichnungen weitergegeben und polizeilich genutzt werden können und welche nicht?
- Wie kann gewährleistet werden, dass alle von Polizei-Bodycams aufgezeichneten Menschen ihr Recht aufs eigene Bild, also ihr Recht auf informationelle Selbstbestimmung wahrnehmen können? Mittels welcher Prozedur, auf welchem Wege und mit welchem Aufwand kann ein videografiertes Passant seine Bilddaten abrufen oder einfordern?
- Wie soll gewährleistet werden, dass etwa für Polizeibeamte "ungünstige" Aufzeichnungen nicht von diesen selber oder von deren Vorgesetzten gelöscht oder nicht weitergegeben werden?
- Inwiefern greifen die Bodycam-Aufnahmen in die Persönlichkeits- oder Arbeitsrechte von Polizeibeamten ein, die sich bspw. gegenseitig filmen?
- Erhalten die Polizeibeamten die Wahlfreiheit bei der Entscheidung, ob sie ihren Dienst lieber mit oder ohne Bodycam durchführen möchten? Mit Blick auf die Ausgangslage und die vorgebliche Begründung für den Einsatz der Bodycams wäre diese Wahlfreiheit doch wohl eine Selbstverständlichkeit!
- Wie meint man den Missbrauch oder die Manipulation von Bodycam-Aufzeichnungen verhindern zu können?"

Ergänzend dieser Stellungnahme (...) aber noch folgendes, konkret auf den NPOG-E bezogenes an Detailkritik:

a.) Die Bibliothek des Niedersächsischen Landtags hat ein aktuelles Buch zum Thema BodyCams in ihrem Bestand:

Jens Zander: "Body-Cams im Polizeieinsatz", Verlag für Polizeiwissenschaft, Frankfurt am Main 2016 (Landtags-Bibliothek-Signatur 2016.0454)

Wir empfehlen allen Mitgliedern des Ausschusses die Lektüre dieser überschaubar dicken Schrift und zitieren hier zum einen aus dem Teil zur Untersuchung der Wissenschaftlichkeit der hessischen Studie und aus dem Fazit des Verfassers, der selber Polizeibeamter ist: Jens Zander zur Validität der so vielfach und repetierend veröffentlichten Erfolgsmeldungen des Hessischen Pilotprojekts in Frankfurt:

”Dass der Abschlussbericht bislang nicht direkt veröffentlicht wurde, sondern dass stattdessen positive Pressemeldungen des Hessischen Innenministeriums über das erfolgreiche Pilotprojekt dominieren, sollte hinsichtlich der Objektivität aufhorchen lassen. (...) Der Verdacht einer bewusst möglichst positiven Darstellung ohne Interesse an einer wirklichen Evaluation drängt sich auf. (...) Wie eingangs erwähnt, ist das Pilotprojekt [der Polizei Hessen] nicht zuletzt aufgrund des Einsatzes von nur drei Kameras in Alt-Sachsenhausen methodisch nicht in der Lage, gesicherte Erkenntnisse zu erlangen. Das Projekt auf dem Niveau 2 [im möglichen Niveaubereich 1 bis 5] der MSMS eignet sich auch nach Hinzuziehung weiterer Daten weder als Nachweis für oder gegen die Wirksamkeit der Body-Cam.”

Jens Zanders Schlußbemerkung in seinem Buch (Hervorhebung durch uns):

”Eingangs wurde erwähnt, dass es sich bei Body-Cams um wahre Wundermittel zu handeln scheint. Nach umfangreicher Beschäftigung mit Body-Cams im Polizeieinsatz komme ich zu dem Schluss, dass diese anfangs erwähnte begeisterten Erwartungen gedämpft werden müssen. Body-Cams entpuppen sich nicht als Wundermittel, sondern als technische Neuerung, die vergleichsweise wenig und dürftig erforscht ist. Bei näherer Betrachtung der Güte der vorhandenen Studien weicht die anfängliche Euphorie eher Ernüchterung. Zwar deuten sich einige Effekte an, die aber eher unspektakulär sind, zumal bei keiner Forschung die Übertragbarkeit auf Deutschland gewährleistet und der Langzeiteffekt berücksichtigt werden kann. Im Zuge der Einführung der Body-Cam kann gleichfalls beobachtet werden, was andere Autoren vor Jahren schon zu herkömmlicher Videoüberwachung angemerkt haben. Töpfer schrieb dazu passend vor acht Jahren:

„Wesentliche[s] Element der Anziehungskraft von Videoüberwachung sind die Faszination für neue Technik und der naive Glaube an die einfache Lösung komplexer sozialer Probleme []. Genährt werden solch technologische Allmachts- und Machbarkeitsfantasien durch die oberflächlichen Hochglanz-Versprechen von Entwicklern und Herstellern und ihren Marketingabteilungen und Lobbyisten.“
(Töpfer 2007: S. 38) Diese Einschätzung lässt sich abschließend treffend auf

Body-Cams im Polizeieinsatz übertragen. Bistlang scheint die Diskussion über die Einführung von Body-Cams in Deutschland eher vom Glauben an deren Wirksamkeit geprägt zu sein, als von wissenschaftlichen Erkenntnissen."

b.) Wie in der mündlichen Anhörung ihres Ausschusses zum zuvor unter Rot-Grün geplanten NGefAG vom 17.11.2016 deutlich geworden ist, ist die Einrichtung einer neutralen Stelle zur Sammlung und Auswertung der BodyCam-Aufzeichnungen eine der Mindestanforderungen, um die Polizeibeamte nicht der Gefahr auszusetzen, dass diese willkürlich oder gar auf den eigenen Vorteil zielend BodyCam-Aufzeichnungen der Öffentlichkeit, den Strafverfolgungsbehörden oder den Betroffenen Aufzeichnungen löschen oder nur diejenigen weiterreichen würden, die ihnen selber nicht zum Nachteil gereichen können. Ebenso wie die Verpflichtung zur Einrichtung einer solchen Stelle fehlen sämtliche Vorgaben zu Regelung der Fragen, wann und auf wessen Entscheidung hin die BodyCam-Aufzeichnung aktiviert wird, wie die Daten behandelt und gegen Missbrauch und Manipulation gesichert werden und ob von der Aufzeichnung Betroffene ein Recht auf Herausgabe der Daten haben und wie sie dieses umsetzen können. Zu alledem schweigt sich der NPOG-Gesetzentwurf sträflich aus, was die Befürchtung nährt, dass die Einhaltung derart wichtiger Randbedingungen nicht ernst genommen und nicht umgesetzt werden wird.

c.) In der Begründung für das im Absatz 5 als zulässig deklarierte 30sekündige PreRecording von Bild und Ton der BodyCams heißt es in der Begründung zum NPOG-E:

"Die Pre-Recording-Funktion führt bei den Betroffenen zu einem Grundrechtseingriff. Angesichts der sehr kurzen Aufnahmezeit von 30 Sekunden, der unwiderruflichen Löschung durch spurlose Überschreibung, wenn die Bodycam nicht aktiviert wird, handelt es sich um einen flüchtigen, oberflächlichen Eingriff, der verfassungsrechtlich unbedenklich erscheint."

Das sehen wir anders: Einen "flüchtigen und oberflächlichen Grundrechtseingriff" können wir nicht erkennen, ob es solche überhaupt geben kann, wäre eine andere zu diskutierende Frage.

Alleine das 30 Sekunden lange PreRecording des gesprochenen Wortes aus dem Umfeld des BodyCam-Trägers könnte mit nicht allzugroßer Übertreibung als permanenter Lauschangriff im öffentlichen Raum bezeichnet werden. Wie auch immer: Verfassungsrechtlich unbedenklich ist das genau nicht, sondern zumindest verfassungsrechtlich diskutabel. Eine entsprechende Diskussion dazu wurde im parlamentarischen Betrieb dazu (wie auch zu allen anderen Grundsatz- und Randbedingungsfrage) jedoch ausgeblendet oder sogar aktiv unterbunden. Als Grundlage für diese Behauptung verweisen wir auf unsere verstörenden Erfahrungen mit dem ad hoc aus dem Boden gestampften BodyCam-Pilotprojekt im Dezember 2016, die eine wissenschaftliche Begleitung und Analyse des Nutzens der polizeilichen BodyCams unmöglich

machte – ganz anders als in der Innenausschuss-Anhörung vom November 2016 von vielen Ausschuss-Mitgliedern immer wieder zur Beruhigung versichert worden ist.

d.) Erstaunlich finden wir, dass keiner der gewerkschaftlichen Interessenvertreter von Polizeibeamten bislang die Frage angesprochen hat, inwiefern die die BodyCam einsetzenden Polizeibeamte selber unter dieser Technik ggf. zu leiden haben – sei es aufgrund des damit neu hinzukommenden subjektiven Überwachungsdrucks, sei es aufgrund der ggf. mit der Einführung erfolgenden "Aufrüstung" auf der Seite der von der Polizei-Videoaufzeichnung Betroffenen ("Gegenfilmen"). Und auch die Fragen des betrieblichen Daten- und Persönlichkeitsschutzes der Polizeibeamten kamen bislang leider weder im Innenausschuss, noch im Plenum, noch in der Gesetzesbegründung überhaupt zur Sprache.

e.) Wir möchten den Vorschlag von Prof. Nils Zurawski von der Universität Hamburg aus der Innenausschuss-Sitzung vom November 2016 in Erinnerung rufen und unterstützen, die Einführung einer BodyCam-Einsatzbefugnis unbedingt mit einer Ausstiegsklausel zu versehen. Das zumindest wäre eine etwas vertrauensbildende Maßnahme.

Aufgrund der bisherigen negativen Erfahrungen mit Pilotprojekten zu BodyCam-Einsätzen in Deutschland (Unwissenschaftlichkeit, Grundlage zur Ausdehnung dieses Mittels unabhängig vom Ergebnis der Pilotversuche) lehnen wir grundsätzlich jegliche Allgemeinbefugnis zum Einsatz von BodyCams ab und fordern die Streichung dieses Absatzes.

Weiter zu den Bodycams:

In der Begründung zum neuen §32a heißt es: "Zudem liegt ein möglichst umfassender Einsatz der Bodycam auch im Interesse der jeweils betroffenen Personen, da deren Nutzung der nachträglichen Aufklärung eines gegebenenfalls unübersichtlichen Einsatzgeschehens dienlich sein kann." Dann müssten diese Personen aber auch Einsichtsrechte in die Aufzeichnungen erhalten. Dazu wird aber nichts geregelt, also gibt es diese Auskunftsrechte auch nicht. Insofern ist das Argument schlicht hinfällig.

Weiter aus der Begründung:

"Nach Satz 2 Nr. 2 sollen Bild- und Tonaufzeichnungen auch auf Verlangen der betroffenen Person ausgelöst werden. Den von polizeilichen Maßnahmen betroffenen Personen wird so die Möglichkeit eingeräumt, selbst eine Nachprüfbarkeit des weiteren polizeilichen Handelns herbeizuführen. Da Bild- und Tonaufzeichnungen nicht nur in das Recht auf informationelle Selbstbestimmung der das Verlangen äuernden betroffenen Person eingreifen, sondern auch Dritte sowie die Einsatzkräfte betroffen werden, beschränkt Satz 2 Nr. 2 das Recht, Bild- und

Tonaufnahmen zu verlangen, auf polizeiliche Maßnahmen, die durch die Anwendung von unmittelbarem Zwang durchgesetzt werden können, in denen es also zur Anwendung von physischer Gewalt kommen kann.”

Dass Betroffene selber verlangen werden, die Bodycams einzuschalten ist wohl nur schönredende Theorie: Wer weiß von diesen Rechten geschweige denn ist in so einer angespannten Situation in der Lage, dieses Recht geltend zu machen? Zudem der Polizei mit dem zweiten Satz des Zitats auch noch Ausnahmerechte von der Pflicht, die Bodycam auf Zuruf einzuschalten eingeräumt werden. Auch ”wenn eine andere berechnigte Person die Aufzeichnung nicht akzeptiert” darf die Polizei das Bodycam-Einschalten auf Zuruf unterlassen. Also bitte: Wer soll/kann denn solcherlei komplexe Erwägungen in der Hektik eines Polizeieinsatzes vernünftig abwägen und handeln? Damit überfordert man die Polizeimenschen, deren Urteil befürchtenswerterweise zu Ungunsten der Betroffenen ausfallen wird.

Nochmals aus der Begründung:

”Der Einsatz von körpernah getragenen Aufnahmegeräten (Bodycams) hat sich seit ihrer Einführung durch Pilotprojekt im Jahre 2016 bewährt.”

Diese steile These verlangt eine Begründung oder wissenschaftliche und neutrale Untermauerung, die es aber leider nicht gibt und deswegen in der Begründung auch nicht erwähnt wird. (Siehe auch die Zitate aus den bisherigen Stellungnahmen oben). Es gibt keinen Beleg für die präventive Wirkung von Bodycams. (Und nur dann wäre der Einsatz rechtlich zulässig!) Das ändert sich auch nicht, wenn es in der Begründung später gebetsmühlenartig heißt:

”Bei der Dokumentation des Geschehens handelt es sich zudem lediglich um eine Begleiterscheinung des Einsatzes, wobei der primäre Zweck der mobilen Bild- und Tonaufzeichnungsgeräte in der präventiven Deeskalation liegt.”

Das ist unbewiesen und zudem zweifelhaft, auf keinen Fall aber grundsätzlich so.

Eine Kenntlichmachung der Bodycam-Videoüberwachung lehnt das MI mit der Begründung ”des geringen Eingriffsgewichts” ab. Das ist eine sehr selbstgefällige Bewertung der Eingriffsintensität polizeilicher Videoüberwachung, insbesondere dann, wenn es um deren Durchführung in privaten Wohnungen geht!

Zur ”durchwachsenen” Historie der Einführung von Bodycams in Niedersachsen:

- <https://freiheitsfoo.de/2017/11/25/bodycam-diskurs-scheitern-nds/>

- <https://freiheitsfoo.de/2021/01/04/kritik-einfuehrung-polizeibodycam-hannover/>

§32b - Biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen

Hier handelt es sich um eine gänzlich neue Regelung mit einem neuen Paragraphen dazu.

Es geht um den Einsatz biometrischer „Echtzeit-Fernidentifizierungssysteme“ im öffentlichen Raum.

Die Niedersächsische Landesregierung möchte mittels dieses neuen Paragraphen den Umfang der Videoüberwachung im öffentlichen Raum substantiell ausweiten. Mit Hilfe von "moderner Bildanalysesoftware auf Basis von KI" (O-Ton aus der Begründung) soll es der Polizei gestattet werden, die Bilder der Polizeikameras im öffentlichen Raum derart informationstechnisch zu verarbeiten, dass in den Bildern und Aufzeichnungen nach Verdächtigen oder Gesuchten gefahndet werden kann. Die Landesregierung erwartet sich davon ein "zusätzliches Erkenntnismittel", liefert aber keine.

Vieles von der in §32 NPOG-ÄE von uns formulierter Kritik greift hier genau so und wir wiederholen sie hier deswegen nicht. Darüber hinaus:

Der Einsatz und die Funktionalität dieser Technik lässt sich gar nicht in Harmonie mit EU-Recht bringen, siehe dazu das schon oben erwähnte Trainingsdatenerhebungsproblem. [Noch Baustelle - nthd]

Ganz unklar bleibt, welche Daten(-banken) da überhaupt abgeglichen werden. Damit öffnet man der Polizei Tür und Tor für den Einbezug sämtlicher irgendwie nur verfügbarer Datenquellen.

Die KI-Verordnung ("AI Act") der EU (<http://data.europa.eu/eli/reg/2024/1689>) verbietet zwar generell die Echtzeit-Datenauswertung zu Identifikationszwecken, räumt aber weitreichende Ausnahmen ein (siehe Artikel 5(1)h bzw. Anhang II), von Drogenhandel über schwere Körperverletzung und Sabotage bis Terrorismus.

Die Identifikation von Personen macht diese Technik im Gegensatz zur Mustererkennung aus §32 zu einem verdeckten Fahndungswerkzeug, auch über längere Beobachtungszeiträume: Bewegungsprofile - inklusive Rückschlüsse auf sensitive Persönlichkeitsmerkmale - können vollständig unbemerkt aus der Ferne angelegt werden. Die Folgen auch hier: Überwachungsdruck und Chilling-Effekt. Hierfür ist im übrigen der Echtzeitaspekt garnicht das Hauptproblem, auch wenn die KI-Verordnung das durch die starke Trennung suggeriert (<https://verfassungsblog.de/ein-anfang-mehr-nicht/>).

Technische Erfahrungen konnte die Niedersächsische Polizei bereits 2024 dank Amtshilfe aus Sachsen mit dem dort entwickelten System "PerIS" sammeln: <https://www.nd-aktuell.de/artikel/1182824.verdeckte-observationstechnik-gesichtserkennung-auch-in-niedersachsen.html>

Ganz unklar bleibt, welche Daten(-banken) da überhaupt abgeglichen werden. Damit öffnet man der Polizei Tür und Tor für den Einbezug sämtlicher irgendwie nur verfügbarer Datenquellen.

In der Begründung selber wird darauf hingewiesen, dass die Technik zu "Fehlinterpretationen" neigt. Welche Konsequenzen bzw. welchen geringen Mehrwert diese Technik dann im Alltagseinsatz haben kann hat das Pilotprojekt am Berliner Südkreuz-Bahnhof deutlich offenbart. Warum man diese Erfahrungen hier ausblendet ist nicht nachvollziehbar. Offenbar haben die verantwortlichen Politiker nichts aus der Vergangenheit gelernt und meinen, soziale Probleme immer noch mit (nur) mehr Technik, insbesondere mehr Überwachungsdruck ausmerzen zu können.

§32c – Nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

Auch hier ein ebenfalls ganz neuer Paragraph mit komplett neuem Inhalt bzw. neuen Befugnissen. Es geht um die "retrograde biometrische Fernidentifizierung im öffentlichen Raum."

Rechtsgrundlage zur Fahndung/Identitätsfeststellung im öffentlichen Raum mittels Videoüberwachung in Echtzeit und retrograd (also auch zeitlich rückwirkend) durch Zugriff auf VÜ-Aufzeichnungen inkl. Einsatz von "KI" und inkl. polizeilichen Nutzungsrecht aller "öffentlich zugänglichen personenbezogenen Daten aus dem Internet".

Während sich §32b mit der Suche nach Polizeibekannten Personen befasst, geht es hier also um die Gegenrichtung: Herausfinden der Identität bisher unbekannter Personen mithilfe von Aufzeichnungen aus Überwachungssystemen.

Damit erlaubt man der Polizei u.a., sämtliche im Netz verfügbaren Bilder, Fotos und Audioaufnahmen von Menschen sich anzueignen und für die eigenen Zwecke wie hier zu nutzen. Die Polizei würde damit tun, was Unternehmen wie PimEyes und Clearview AI zurecht als extrem invasiv und als eindeutiger Verstoß gegen die DSGVO ausgelegt wurde (<https://noyb.eu/de/criminal-complaint-against-facial-recognition-company-clearview-ai>).

Dass ein solches Erlaubnis ein tiefgreifender Einschnitt in die Freiheit der Menschen bedeutet muss kaum erläutert werden, oder? Wer kann heute noch überschauen geschweige denn beeinflussen, ob und in welchem Umfang andere Menschen z.B mithilfe ihrer Smartphones Bilder, Videos und Tonaufnahmen von einem selber machen? Addiert man dann das Bewusstsein, dass die Polizei Zugriff auf dieser Daten nehmen darf kann das zu massivsten Selbsteinschränkungen der Menschen in der Ausübung ihrer Freiheiten und zu einer stark verkümmerten Fähigkeit führen, sich selbst zu verwirklichen bzw. eine eigene Persönlichkeit überhaupt erst herausbilden zu können.

Letzteres gilt vor allem für Kinder, Jugendliche und Heranwachsende. Deren Entwicklung kann durch die Erlaubnis für die Polizei, alle biometrischen verwertbaren Daten über Menschen nutzen zu können bedeutsam behindert werden.

§32d - Einsatz von unbemannten Fahrzeugsystemen

Ganz neu und bislang ungeregt: Einsatz von Drohnen durch die Polizei.

Anders als bisher wird der Einsatz von Polizeidrohnen jetzt umfangreich geregelt. Bislang waren die (u.a. bei Einsätzen rund um Fußballspiele) ohne ausreichende Kennzeichnung und damit rechtswidrig unterwegs. Ob und wie eine für alle von der Überwachung Betroffenen nun zukünftig "kenntlich gemacht" wird, wie es der neue §32d(2) vorsieht bleibt abzuwarten und ggf. gerichtlich zu überprüfen.

Bemerkens- und kritikwert ist dabei die sich bei der Polizei eingeschlichene Praxis, dass die Drohnen in dem eben genannten Zusammenhängen auch schon dann zur Video- (und Audio-?)Überwachung der Fußballfans eingesetzt wurde, wenn eine Grundlage/Zulässigkeit nach §32(1) noch gar nicht gegeben war. Begründet wird dies in aller Regel damit, dass doch "nur" Übersichtsbilder übermittelt werden und regulär (zunächst) keine Aufzeichnung der Bilder stattfindet. Beides überzeugt rechtlich nicht, wie auch Gerichte schon mehrfach bestätigt haben. Inwiefern die Auflösung der Bilder nicht auch Identifizierungen von einzelnen Menschen ermöglicht ist diskutabel. Undiskutabel dagegen, dass Menschen sich von einer Polizeidrohne in der freien Ausübung ihrer Grundrechte beschränken lassen, ganz unabhängig davon, in welcher Form und mit welcher Bildqualität diese Bilder von den Menschengruppen aufnimmt oder überträgt.

Noch bedeutsamer aber:

In Absatz 1 erlaubt die Novelle der Polizei nun den Einsatz für zahlreiche Anwendungsfälle und nur in einem Fall, nämlich in Bezug auf §32 (Einsatz technischer Mittel bei öffentlichen Veranstaltungen und im öffentlichen Raum inklusive Verhaltensmustererkennung mittels KI), soll die Drohne "offen" agieren müssen. In allen anderen Fällen darf der Drohneneinsatz als nicht offen, d.h. verdeckt bzw. im Geheimen stattfinden. Diese anderen zulässigen Fälle von Drohneneinsätzen sind:

- §32e NPOG-ÄE: Einsatz gegen andere unbemannte Fahrzeuge zu Lande, Wasser oder in der Luft
- §33a NPOG-ÄE: Einsatz zur Überwachung und Abhörung von Telekommunikation
- §33b NPOG-ÄE: Einsatz zur Lokalisierung von Handys, Computern u.a. sowie zur Unterbrechung von Telekommunikation
- §33d NPOG-ÄE: Einsatz zur Einbringung, Installation und zum Betrieb von Staatstrojanern
- §35 NPOG-ÄE: Einsatz zur heimlichen Überwachung und Belauschung von Menschen außerhalb ihrer Wohnungen

- §35a NPOG-ÄE: Einsatz zur heimlichen Überwachung und Belauschung von Menschen innerhalb ihrer Wohnungen

Man beachte: Es muss sich hierbei nicht nur um Drohnen im Sinne der derzeit benutzten Umgangssprache, also um fliegende, ferngesteuerte Quadro- oder Multikopter handeln. Auch denkbar und erlaubt sind hiernach der Einsatz von (Miniatur-)Fahrzeugen, Booten oder als sich fortbewegende Tiere getarnte Überwachungstechnik.

§32e - Einsatz technischer Mittel gegen unbemannte Fahrzeugsysteme

Einsatz technischer Mittel gegen andere Drohnen

§33 - Schutz des Kernbereichs privater Lebensgestaltung

Hier geht es um den "Schutz des Kernbereichs privater Lebensgestaltung" und mit der Hinzufügung eines Nebensatzes meint die derzeitige Landesregierung, die Chance bzw. die Wertigkeit, einen Polizeispitzel auch in Zukunft weiter nutzen zu können wiegen grundsätzlich schwerer als der Schutz dieses Kernbereiches privater Lebensgestaltung eines anderen Menschen.

So zugespitzt (aber so steht es im Gesetzentwurf drin) dürfte das in dieser Allgemeinheit in Karlsruhe keinen Bestand haben.

§33a - Datenerhebung durch Überwachung der Telekommunikation

Hier geht es um den heimlichen Eingriff in IT-Systeme, um den Niedersachsentrojaner (Staatstrojaner).

Der Paragraph bleibt unverändert.

Der Trojanereinsatz durch den Staat rüttelt am Grundrecht auf Vertraulichkeit und Integrität unserer Computer und Smartphones und ist an sich seit den Diskussionen ab 2018 höchst umstritten. Auch die Grünen haben sich seinerzeit vehement dagegen ausgesprochen und scheinen nun eingeknickt zu sein.

§33b - Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten, Unterbrechung der Telekommunikation

Identifizierung und Lokalisierung von Mobilgeräten, Unterbrechung der Telekommunikation

Hier setzt der Gesetzgeber einen Beschluss des BGH aus dem Februar 2018 um. Man könnte fragen, warum das nicht schon im NPOG in 2019 eingefügt worden ist.

§33d - Verdeckter Eingriff in informationstechnische Systeme

Auch hier geht es – wie beim §33a – um den heimlichen Eingriff in IT-Systeme, um den Niedersachsentrojaner (Staatstrojaner), der Paragraph bleibt unverändert.

Der Trojanereinsatz durch den Staat rüttelt am Grundrecht auf Vertraulichkeit und Integrität unserer Computer und Smartphones und ist an sich seit den Diskussionen ab 2018 höchst umstritten. Auch die Grünen haben sich seinerzeit vehement dagegen ausgesprochen und scheinen nun eingeknickt zu sein.

§34 - Datenerhebung durch längerfristige Observation

Zulässigkeit langfristiger verdeckter Observation nun auch (unter bestimmten Bedingungen) im Zusammenhang mit "Vorfeldstraftaten".

Hier hat das BVerfG mit einem Urteil aus dem Dezember 2022 klar gemacht, dass die bisherige Regelung im NPOG rechtswidrig war. Etwas, was in der Diskussion damals in 2019 seitens der damaligen Landesregierung aus SPD und CDU noch vehement bestritten worden ist.

Doch von Reue oder Einsicht keine Spur. Noch weniger von Lerneffekten.

§35 - Einsatz heimlicher Mittel außerhalb von Wohnungen

Dieser Paragraph wie auch der nachfolgende §35a bleiben durch den NPOG-ÄE zwar inhaltlich unangetastet, aber Polizeidrohnen sollen nach §32d NPOG-ÄE auch hierfür eingesetzt werden dürfen.

Polizeidrohnen sollen künftig also auch dazu eingesetzt werden dürfen, um im öffentlichen Raum heimlich Menschen zu filmen, zu belauschen und zu überwachen. Zwar bedarf dieses einer vorherigen richterlichen Genehmigung (Ausnahme: "Gefahr im Verzug"), dennoch ist der Umfang der Zulässigkeit von Drohnen für diese Maßnahme im Lichte der technischen Entwicklungen (u.a. Miniaturisierung von Drohnen) von heute aus überhaupt nicht absehbar und sollte daher verboten bleiben oder bedarf mindestens einer ausführlichen öffentlichen Diskussion.

Noch genauer betrachtet möchten wir darauf hinweisen, dass es sich nicht nur um eine Erlaubnisgarantie für fliegende Drohnen handelt, denn ganz allgemein ist im §32d NPOG-ÄE von "unbemannten Fahrzeugsystemen" die Rede, also mitunter auch potentiell von anderen fliegenden oder fahrenden, krabbelnden, kriechenden, schwimmenden oder tauchenden Miniaturgeräten mit eingebauter Überwachungstechnik. Derlei wird weltweit in immensen Umfang und mit hohem Innovationsdruck entwickelt und stellt in diesem Kontext der pauschalen Erlaubniserteilung an die Polizei eine große Gefahr für die Demokratie dar.

§35a - Einsatz heimlicher Mittel in Wohnungen

Man überlege sich einmal, welche denkbaren und in der öffentlichen Diskussion bislang noch überhaupt nicht erörterten Spielräume sich den Polizeibehörden damit eröffnen, denn der Einsatz von Polizeidrohnen soll auch für diese heimliche Maßnahme erlaubt sein.

Hier melden wir die gleichen Bedenken an wie auch soeben schon zum §35.

§37 - Ausschreibung zur polizeilichen Beobachtung

Zulässigkeit polizeilicher Ausschreibung (Fahndung) nach Menschen nun auch (unter bestimmten Bedingungen) im Zusammenhang mit "Vorfeldstraftaten". Auch hier muss wie in §34 schon beschrieben nachgebessert und Verfassungswidrigkeiten (scheinbar) beseitigt werden.

§38 - Weiterverarbeitung personenbezogener Daten, Zweckbindung

Zulässigkeit der Nutzung von Daten zu anderen Zwecken als zu denen, zu denen die Daten eigentlich erhoben wurden.

§38a - Kennzeichnung in polizeilichen Informationssystemen

Kennzeichnung in polizeilichen Informationssystemen

Hier (u.a.!) hat das LfD NDS Kritik geübt und empfohlen, die Kennzeichnung um den Zweck der Datenverarbeitung zu ergänzen. Das Innenministerium in Hannover streut sich dagegen, begründet seine Verweigerungshaltung aber nicht wirklich. Es wird nicht deutlich, was gegen diese Ergänzung wirklich spricht.

§39 – Weiterverarbeitung personenbezogener Daten zu anderen Zwecken

Weiterverarbeitung personenbezogener Daten zu anderen Zwecken

Das LfD Niedersachsen hat hierzu protestiert und lehnt die Regelung, wonach strenge Vorgaben der Zweckbindung und der Grundsatz hypothetischer Datenneuerhebung in bestimmten Fällen nicht gelten, ab. Das Innenministerium will dem nicht nachgeben.

§39a - Weiterverarbeitung personenbezogener Daten zu besonderen Zwecken

Gar nicht neu: Wie interpretiert die Polizei Niedersachsen den Begriff der "Anonymisierung von Daten"? Kann Sie in Praxis belegen, dass es sich dabei nicht tatsächlich nur um pseudonymisierte Datensätze handelt? Im neu formulierten 39a geht es um das Recht der Polizei, personenbezogene Daten ohne vorherige Anonymisierung "zu Forschungszwecken" an "Dritte" übermitteln. Das mit der Vorgabe, dass dort die Anonymisierung zu erfolgen habe. Das LfD kritisiert das völlig zurecht. Das Innenministerium meint, das sei doch gar kein Problem ... Und wer überwacht die Anonymisierung (die in Praxis übrigens leichter gesagt als getan ist) bei den "Dritten"? Und wer alles darf dieser "Dritte" sein? Wer will tatsächlich und effektiv entsprechenden Datenabfluss oder Datenmissbrauch an diesen Stellen verhindern können?

§41 - Datenübermittlung im innerstaatlichen Bereich

Innerstaatliche Datenweitergabe an Behörden und Private sind hiernach unter nur noch minimalen Beschränkungen und nahezu kompletter Aufgabe der Zweckbindung erlaubt. Damit wird ein Eckpfeiler des Datenschutzes zertrümmert.

Details:

§ 41 (2) [neu]: Datenweitergabe möglich zur Erfüllung von Aufgaben der sendenden Stelle, zur *"Abwehr erheblicher Nachteile für das Gemeinwohl"* oder *"zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer Person"*. Welche Rechte einer Person? Irgendwelche? Wäre die Gefahr einer Beleidigung ausreichend?

§ 41 (3) [neu]: Daten sollen neuerdings auch an Firmen und Dritte weitergegeben werden können, u.a. reicht es dazu, wenn diese ein *„berechtigtes Interesse“* anmelden und betroffene Menschen vorher nicht widersprochen haben. Das ist praktisch ein Freifahrtsschein zur Datenweitergabe unter beliebigen Begründungen und unter kompletter Vernichtung der Zweckbindung.

§41a - Datenübermittlung zum Zwecke einer Zuverlässigkeitsüberprüfung

Neues Recht der Polizei, personenbezogene Daten an öffentliche und nicht-öffentliche Stellen im Rahmen von "Zuverlässigkeitsüberprüfungen" auszuhändigen.

Die Regelungen, wie diese Stellen dann mit den sensiblen Auskünften über Menschen umgehen, sind unsicher nicht deutlich genug eingegrenzt.

Auch zweifelhaft sind die gesetzlichen Vorgaben, wer und wie die davon betroffenen Menschen über den Vorgang informiert werden. Es gibt begründete Sorge, dass diese Beauskunftung in Einzelfällen ganz unterbleibt oder - in anderen Fällen - zur Stigmatisierung der Menschen z.B. bei Ihrem Arbeitgeber führen kann.

Das LfD kritisiert zudem, dass bei der Übermittlung der Auskünfte an "öffentliche Stellen" diese nicht darauf beschränkt sein müssen, ob es ein Sicherheitsrisiko im Zusammenhang mit einer Person geben kann oder nicht. Dass also weit mehr Detaildaten über diesen Menschen ausgeliefert werden, als eigentlich nötig.

§43 - Datenübermittlung im Bereich der Europäischen Union und deren Mitgliedstaaten

Das Recht hierzu ist nicht neu, aber nicht minder kritikwürdig, insbesondere mit Blick auf die Rechtsrücke und neuautoritäre Ausrichtung von/in anderen EU-Mitgliedsstaaten:

Zulässig ist hiernach die Weitergabe personenbezogener Daten an andere EU-Mitgliedsstaaten und entsprechend gleichgestellte andere Schengen-assoziierten Staaten”.

Denn erlaubt ist ein solch heikler Datentransfer darf sogar schon „zur Abwehr einer Gefahr durch den Empfänger oder zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer Person“ erfolgen.

Man denke nur an Länder wie Ungarn, die Slowakei oder an Polen und Fälle wie die von Maja T., um zu erkennen, dass diese Regelungen ja bis zu lebensgefährlich für die betroffenen Menschen sein und so pauschal nicht richtig sein können.

§43a - Datenübermittlung der Polizei im internationalen Bereich

Dies sind mindestens genau so heikle Regelungen zu Datentransfers über Menschen in weitere Staaten über die eben genannten Staaten.

Erlaubt sein soll die Übermittlung von niedersächsischen gesammelten Polizeidaten über Menschen immer dann, wenn dies *„zur Erfüllung polizeilicher Aufgaben oder zur Abwehr einer erheblichen Gefahr durch die empfangende Stelle erforderlich ist.“*

Das ist schon reichlich pauschal und man fragt sich, wer denn tatsächlich überprüfen kann, ob das so ist oder nur seitens des Datenempfängers vorgegeben wird, um an die Daten zu gelangen.

Dazu gehört nun der Blick auf die Liste der Länder/Staaten, denen dieses Recht auf Polizeidaten zugesprochen wird: Es sind dies alle restlichen Länder der Welt. Inklusive USA, Russland, China, Türkei und Iran – um nur wenige Beispiele aktuell autoritär geführter Länder aufzuführen.

§45a - Automatisierte Datenanalyse

Hier wurde ein ganz neuer Paragraph geschaffen.

Es geht um sog. Palantir-Befugnisse. Die Innenministerin hat zwar Produkte der Firma Palantir abgelehnt, nicht aber die Technik dahinter und hier kommen schonmal alle Befugnisse, falls Palantir-Software selbst (oder ein "europäisches" Substitut) dann überraschenderweise doch angeschafft werden sollte.

Das LfD kritisiert am 45a (wohl u.a.), Vorgangs- und Falldaten für die automatisierte Analyse auszuschließen, weil darin auch personenbezogene Daten Unbeteiligter (Zeugen etc.) enthalten sind. Das Innenministerium interpretiert das BVerfG nach eigenem Gustus so, dass das gar nicht nötig sei. Es ergebe sich daraus *"kein konkretes Verbot"* ...

In der Begründung zum 45a heißt es, dass (in Abs.2) festgelegt werde, *dass ein solches Analysetool nur "um ein technisches Hilfsmittel" handle, dass die Arbeitsweise der Polizei nicht grundsätzlich verändere.*

Wer glaubt, dass man per ordere de mufti so etwas bürokratisch definieren oder festkrallen könne, der hat die Welt nicht verstanden. Selbstverständlich würde ein solches Analysetool in den Händen der Polizei deren Arbeit im Wesen stark verändern und das würde auch der Absatz 2 nicht verhindern.

Angemerkt sei hier auch noch, dass in der Begründung ausdrücklich darauf hingewiesen wird, dass auch Daten *"aus Internetquellen"* einbezogen werden können, zusätzlich dann auch noch *"Daten aus staatlichen Registern, wie Melderegistern, dem zentralen Verkehrsinformationssystem ZEVIS oder dem Nationalen Waffenregister"*. Auf diese Datenbanken soll die Analyse-ID selbständig zugreifen können. Es ist nicht vorstellbar, dass eine solche Software derart integer und gehärtet auf den Polizeitisch kommt, dass künftige Datenskandale mit höchst sensiblen Menshendaten verhindert werden können.

In der Begründung zu Absatz 3 des §45a wird es dann "lustig": Denn dort wird der Polizei verordnet *"technisch-organisatorische Maßnahmen"* im Kontext des Einsatzes der Analyse-Software zu treffen, *"um die Bildung und Verwendung diskriminierender Algorithmen zu vermeiden und die Nachvollziehbarkeit des verwendeten Verfahrens sicherzustellen"*.

Nein, das ist kein Scherz. Vielmehr muss es sich hierbei um entweder Ignoranz oder Dummheit handeln. Denn weder die Polizei noch die Programmierer eines KI-Frames können das leisten.

Algorithmen sind niemals diskriminierend, das ist großer Quatsch.

Neigt eine "KI" dazu, rassistische oder andere menschenverachtende Tendenzen auszubilden liegt das an dem Datenfutter, das ihr im Training vorgelegt worden ist. Und niemand, kein Mensch zumindest ist in der Lage, die Urteilsfindung einer KI im Detail *"nachzuvollziehen"*.

Dieser Begründungsteil der NPOG-Reform ist der Offenbarungseid der Unfähigkeit der Gesetzesverfasser, der Unkontrollierbarkeit und fehlenden Nachvollziehfähigkeit von "KI"-Anlagen.

Impressum

freiheitsfoo

www.freiheitsfoo.de

März 2026

Unsere Stellungnahme haben wir ohne irgendeine Zuhilfenahme von „KI“ erstellt.

Was ist das freiheitsfoo?

1.) Was ist freiheitsfoo?

- Das freiheitsfoo ist eine ausdrücklich offene Gruppe von Menschen.
- Bei freiheitsfoo geht es um Inhalte (siehe Punkt 2), aber auch mindestens genauso darum, wie wir miteinander umgehen und uns organisieren.
- freiheitsfoo ist ein Experiment.

2.) Worum es beim freiheitsfoo geht

- Menschen- und Freiheitsrechte für andere und für uns hinterfragen, einfordern und leben.
- Darunter besonders die Rechte auf Privatsphäre, informationelle Selbstbestimmung, Anonymität und Intimsphäre im Digitalen.
- Räume und Gelegenheiten schaffen und pflegen, in/bei denen Menschen sich möglichst frei zu eigenen, selbstbestimmten Persönlichkeiten entwickeln und entfalten können.
- Eine offene und transparente Plattform für ein solches Engagement sein.

Auszug aus dem freiheitsfoo-Selbstverständnis (<https://freiheitsfoo.de/freiheitsfoo/>).