Rolf Gössner

Kategorie Politik – Laudatio

Der BigBrotherAward 2018 in der Kategorie Politik geht an die Fraktionen von CDU und Bündnis90/Die Grünen im hessischen Landtag.

Die beiden Regierungsfraktionen erhalten den Negativpreis für ihr geplantes neues Verfassungsschutzgesetz und für die geplante Novellierung des hessischen Polizeigesetzes. Ihre Gesetzesinitiative enthält eine gefährliche Ansammlung gravierender Überwachungsermächtigungen, die tief in Grundrechte eingreifen und den demokratischen Rechtsstaat bedrohen. Die schlimmsten Regelungen im Überblick:

1. Der Inlandsgeheimdienst „Verfassungsschutz" soll auch vorbestrafte V-Leute rekrutieren und kriminell gewordene VerfassungsschutzMitarbeiterInnen weiter einsetzen und abschöpfen können. Das tut er zwar schon heute, wie die Praxis zeigt; neu aber ist, dass dies erstmals gesetzlich abgesichert werden soll und kriminelle V-Leute ganz legal der strafrechtlichen Verfolgung entzogen werden können – anstatt solche V-Leute unverzüglich abzuschalten. Ein rechtsstaatswidriger Freibrief für kriminelles Handeln in staatlicher Mission. Diese Regelung legalisiert praktisch die bisherigen Skandale und mit ihnen die obszönen Verflechtungen des Verfassungsschutzes in rassistische, kriminelle und gewalttätige Neonaziszenen.

2. Erlaubt werden soll auch, Berufsgeheimnisträger wie Ärzte, Anwälte oder Journalisten als V-Leute anzuheuern oder V-Leute in deren beruflichem Umfeld zu platzieren. Damit werden die Verschwiegenheitspflichten und zu schützenden Vertrauensverhältnisse zu ihren Mandanten, Patienten oder Informanten verletzt. Nur Abgeordnete und ihre MitarbeiterInnen sollen vor dieser geheimdienstlichen Instrumentalisierung und Ausforschung ausdrücklich geschützt werden.

3. Selbst Daten über Minderjährige unter 14 Jahren, also von Kindern, sollen in Dateien und Akten des Verfassungsschutzes erfasst und gespeichert werden dürfen. Diese frühzeitige geheimdienstliche Stigmatisierung kann fatale Folgen für die weitere Entwicklung der Betroffenen haben – etwa bei der späteren Berufswahl, Lehrstellen- oder Jobsuche.

4. Der Verfassungsschutz soll ermächtigt werden, personenbezogene Überwachungsdaten an öffentliche Stellen zu übermitteln – und zwar zur „Überprüfung der Verfassungstreue von Personen, die sich um Einstellung in den öffentlichen Dienst bewerben". Das erinnert fatal an die menschenrechtswidrige Berufsverbotspraxis früherer Zeiten. Auch Organisationen und künftigen MitarbeiterInnen staatlich geförderter Demokratie- und Präventionsprojekte, etwa gegen Rechtsextremismus oder Salafismus, drohen anlasslose geheimdienstliche Überprüfungen – womit sie pauschal zu Sicherheitsrisiken erklärt und unter Generalverdacht gestellt werden. Dieses gesetzliche Misstrauensvotum untergräbt Akzeptanz und Vertrauen, die für eine erfolgreiche Arbeit solcher zivilgesellschaftlichen Projekte unerlässlich sind.

5. Spionage-Programme, also sogenannte Staatstrojaner, sollen künftig über gefundene oder aufgekaufte Sicherheitslücken in Computern oder Smartphones Verdächtigter eingeschleust werden, um sie präventiv per Onlinedurchsuchung oder Quellen-Telekommunikationsüberwachung (TKÜ) umfassend ausforschen zu können.

6. Und die Polizei soll künftig u. a. ermächtigt werden, sogenannte „Gefährder" vorsorglich in elektronische Fußfesseln zu legen, um ihren Aufenthalt, ihre Bewegungen und Kontakte über Wochen und Monate lückenlos kontrollieren zu können. Das sind Menschen, die keine Straftaten begangen haben, sondern denen die Polizei aufgrund bestimmter Anhaltspunkte künftige Straftaten zutraut.

Dr. Rolf Gössner bei seiner Laudatio – Foto: F. Kurz, CC BY-SA 4.0

Auf dem Weg in den präventiv-autoritären Sicherheitsstaat

Mit dieser Gesetzesinitiative geht die schwarz-grüne Regierungskoalition in Hessen einen großen Schritt in Richtung präventiv-autoritärer Sicherheitsstaat. Mit besonders prekären Regelungen reiht sie sich damit in die bundesweiten Reformen ein, mit denen u. a. der Staatstrojaner zur Quellen-TKÜ und Online-Durchsuchung sowie die elektronische Fußfessel für „Gefährder" legalisiert werden. So etwa im BKA-Gesetz (2017), in der Strafprozessordnung (2017), in den Geheimdienstgesetzen Baden-Württembergs (2017) und Bayerns (2016). Interessanterweise klagt die grüne Oppositionsfraktion im bayerischen Landtag gegen das dortige Verfassungsschutzgesetz[1] – ausgerechnet gegen ein Gesetz, das sich das hessische Regierungsbündnis unter Mitwirkung der Grünen zum Vorbild genommen hat.

Ursprünglich sollten die Verfassungsschutzgesetze in Bund und Ländern novelliert werden, um überfällige Konsequenzen zu ziehen aus den zahlreichen Missständen, Pannen und Skandalen im Zusammenhang mit der NSU-Mordserie und NSA-Massenüberwachung. Primäre Ziele müssten demnach sein, den Verfassungsschutz und seine Befugnisse wirksam rechtsstaatlich zu zähmen und die Kontrolle über ihn erheblich zu stärken. Doch stattdessen erhalten ausgerechnet diese demokratisch kaum kontrollierbaren Geheimbehörden des Bundes und der Länder – geschichtsvergessen muss

man sagen – wieder unverdienten Auftrieb, werden abermals aufgerüstet und massenüberwachungstauglicher gemacht, anstatt die Bevölkerung endlich vor ihren klandestinen Machenschaften und Skandalen wirksam zu schützen. Das heißt: Der Verfassungsschutz geht gestärkt aus dem Desaster und seiner Skandalgeschichte hervor. Und auch die Polizei wird weiter hochgerüstet.

Was bedeutet das für unmittelbar Betroffene und für uns alle? Zwei Beispiele:

1. Heimlicher Angriff auf Computer und Smartphones mit Staatstrojanern

Der hessische Verfassungsschutz soll unter bestimmten Bedingungen erstmals mit technischen Mitteln heimlich „informationstechnische Systeme" angreifen dürfen – bei „Gefahr im Verzug" zunächst sogar ohne richterliche Anordnung. Das heißt im Klartext: Dieser Inlandsgeheimdienst darf zur verdeckten Informationsgewinnung Computersysteme mit Hilfe von Spionage-Programmen hacken – und zwar mit Hilfe der berüchtigten „Staatstrojaner", die im Land der Hessen auch „Hessentrojaner" heißen.[2] Diese Überwachungssoftware wird heimlich in Computer, Tablets oder Smartphones von Verdächtigten eingeschleust, um diese unter Ausnutzung von Sicherheitslücken zu infiltrieren. So können dann Quellen-Telekommunikationsüberwachungen oder Online-Durchsuchungen durchgeführt werden.

Mit diesen Methoden, die der Abwehr einer „dringenden Gefahr" dienen sollen, bricht der Staat massiv in Privatsphäre und Persönlichkeitsrechte, in Informationelle Selbstbestimmung und Meinungsfreiheit der Betroffenen ein: Denn damit können PC-Mikrofone und Webcams eingeschaltet sowie sämtliche laufenden Kommunikationsinhalte vor ihrer Verschlüsselung überwacht werden – inklusive SMS, Mails, Chats und Messenger-Dienste. Mit Hilfe der Trojaner kann der Geheimdienst auf sämtliche Datenbewegungen, auf alle gespeicherten Festplatten-Inhalte, auf Textdokumente, Gesundheits- und Finanzdaten, auf intimste Informationen, Fotos und Filme zugreifen – letztlich auf das gesamte digitale und vernetzte Leben der Betroffenen. Angesichts der hieraus entstehenden Persönlichkeits-, Kontakt- und Bewegungsprofile ist an den verfassungsrechtlich gebotenen Schutz des Kernbereichs persönlicher Lebensgestaltung praktisch nicht mehr zu denken – ganz abgesehen davon, dass solche Geheimmethoden weder gerichtlich noch parlamentarisch wirksam kontrollierbar sind. Es handelt sich um einen der schwersten staatlichen Grundrechtseingriffe mit totalitärem Potential – um einen Einbruch in alle Lebensbereiche bis hinein in die Gedanken- und Gefühlswelt der Betroffenen.

Diese digitale Waffe unterminiert darüber hinaus das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[3]: Denn der Verfassungsschutz muss Software-Sicherheitslücken ausfindig machen, um einen Staatstrojaner auf dem Gerät installieren und aktivieren zu können. Er wird versuchen, solche Schwachstellen für eigene Zwecke künftig weiter offenzuhalten – anstatt sie sofort schließen zu lassen, um Attacken Dritter abzuwehren, das IT-System insgesamt zu schützen und damit die Allgemeinheit. Stattdessen werden also mutwillig Sicherheitslecks als Einfallstore aufrechterhalten, über die auch andere Geheimdienste, Cyber-Kriminelle, Betrüger, Erpresser und Terroristen gefährliche Angriffe auf private, betriebliche oder staatliche Computersysteme ausführen können oder auf die kritische Infrastruktur insgesamt (etwa von Strom- und Wasserversorgern, des Krankenhaus-, Gesundheits- oder Verkehrswesens).

Dieses unverantwortliche Staatsverhalten öffnet Missbrauch und gefährlichen Cyberattacken Tür und Tor. Abschreckendes Beispiel: der Erpressungs-Trojaner *Wannacry*, der im Mai 2017 neben Privat-PCs auch Automobilkonzerne, Bahnunternehmen und Krankenhäuser lahmlegte und Schäden in Milliardenhöhe verursachte. Die dabei genutzte Sicherheitslücke war dem US-Auslandsgeheimdienst NSA bereits seit Jahren bekannt. Verantwortungsvolle Sicherheitspolitik, die diese Bezeichnung verdient, sieht anders aus. Denn es gehört zum Auftrag des Staates, seine Bürger zu schützen und Sicherheitslücken zu schließen, und nicht, sie mutwillig für eigene Trojaner sperrangelweit offenzuhalten – und damit auch für andere Cyberangreifer.

2. Beispiel: Elektronische Fußfesseln zur Aufenthaltskontrolle von Gefährdern

Die hessische Polizei soll künftig – wie seit 2017 das BKA auf Bundesebene – so genannte „terroristische Gefährder" präventiv in elektronische Fußfesseln legen sowie Meldepflichten, Aufenthaltsbeschränkungen, Hausarrest und Kontaktverbote verhängen können. Nach einer gerichtlichen Anordnung sollen diese Freiheitsbeschränkungen mit einer elektronischen Fußfessel über GPS lückenlos überwacht werden, selbst innerhalb von Wohnungen. Zulässig soll dies dann sein, so heißt es im schwarz-grünen Gesetzentwurf wörtlich, „wenn bestimmte Tatsachen die Annahme rechtfertigen", dass die betreffende Person „innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise" eine Straftat begehen wird, „oder deren individuelles Verhalten eine konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines übersehbaren Zeitraums" eine Straftat begehen wird.

Die elektronische Überwachungsmaßnahme, mit der u. a. terroristische Straftaten verhütet werden sollen, ist auf höchstens drei Monate zu befristen, kann aber um jeweils drei Monate verlängert werden – das heißt im Zweifel: unbeschränkt. Weigern sich Betroffene gegen die Maßnahme, können sie mit richterlicher Entscheidung bis zu zehn Tage lang in Polizeigewahrsam gesteckt werden.

Solche eingriffsintensiven Polizeimaßnahmen, die lückenlose Bewegungsprofile liefern und Rückschlüsse auf die persönliche Lebensführung zulassen, sollen gegen sogenannte Gefährder verhängt werden – also gegen Menschen, die bislang nicht straffällig geworden sind, denen dies aber in Zukunft aufgrund bloßer Indizien und Annahmen oder unterstellter Absichten und Gesinnung polizeilicherseits zugetraut wird. Solche Prognosen für künftiges Verhalten können entweder aus polizeilichen oder geheimdienstlichen Persönlichkeits- und Kontaktprofilen oder auch aus Risikobewertungen per Computeranalyse (z. B. Precrime-Programm „Radar-iTE") resultieren. Doch wie lässt sich dabei verhindern, dass institutioneller Rassismus und Islamophobie zu folgenschweren Einschätzungen führen?

Derart gravierende Grundrechtseingriffe auf mehr oder weniger vage Mutmaßungen zu stützen, dürfte den Verfassungsgrund-

satz der Verhältnismäßigkeit verletzen. Denn rund um die Uhr und in Echtzeit überwachte Aufenthalts- und Kontaktverbote schränken die Betroffenen, die ja als unschuldig zu gelten haben, unmittelbar in ihrer Handlungs- und Bewegungsfreiheit ein und verletzen ihre Privatsphäre und Persönlichkeitsrechte – und letztlich auch ihre Menschenwürde. Solche verhaltenssteuernden und freiheitsberaubenden Präventionsmaßnahmen gleichen letztlich einer vorweggenommenen Verdachtsstrafe – also einer rechtsstaatswidrigen Strafe ohne Tat.

Im Übrigen dürfte die elektronische Fußfessel, die ohnehin relativ leicht manipulierbar und entfernbar ist, im Ernstfall auch ungeeignet zur Verhinderung terroristischer Straftaten sein – besonders wenn es sich um potentielle Täter handelt, die zu allem entschlossen sind: So trug etwa einer der beiden Täter, die 2016 einem katholischen Pfarrer in der Normandie die Kehle durchtrennten, eine elektronische Fußfessel; und auch das Berliner Attentat auf dem Weihnachtsmarkt im Dezember 2016 hätte damit wohl kaum verhindert werden können – wohl aber mit anderen, längst gesetzlich erlaubten Polizeibefugnissen, die aber, wie sich herausgestellt hat, nicht genutzt worden sind.

Zivilgesellschaftliche Proteste und innergrüner Streit um „Hessentrojaner"

Gegen die hessische Gesetzesinitiative regt sich heftiger Protest und Widerstand: Ein breites Bündnis von Demokratieprojekten sowie Bürgerrechts- und Datenschutz-Organisationen unterstützen eine gemeinsame Erklärung, in der sie die geplanten Verschärfungen ablehnen, weil sie Demokratie und Grundrechte schädigen.[4] Während einer Anhörung im Hessischen Landtag hat die überwiegende Mehrzahl der Sachverständigen die Gesetzespläne heftig kritisiert und erhebliche Änderungen angemahnt.[5]

Auch die grüne Basis in Hessen votierte schon Ende 2017 gegen die schwarz-grünen Pläne, speziell gegen die Legalisierung des „Hessentrojaners". Damit verweigerte sie der grünen Landtagsfraktion ihre Unterstützung.[6] Vollkommen zu Recht, lehnen doch die Grünen die Staatstrojaner generell ab und hatten doch die hessischen Grünen im letzten Wahlkampf versprochen, keine Online-Durchsuchung zur Gefahrenabwehr zuzulassen.[7] Doch die Landtagsfraktion bleibt stur und begründet ihr gebrochenes Versprechen mit „terroristischen Bedrohungen", die es nötig machten, die digitale Kommunikation weitgehender als bisher zu überwachen. Das miese Spiel mit der Angst vor Terror zur Beschränkung der Freiheitsrechte, um angeblich mehr Sicherheit zu erlangen, das haben die Grünen bislang eher gemieden und anderen überlassen, wie etwa der CDU/CSU oder auch der Großen Koalition. Die grüne Fraktion in Hessen aber spielt nun selbst beim Überwachungspoker mit, beteiligt sich am sicherheitspolitischen Überbietungswettbewerb und behauptet noch dreist, ihr Gesetzentwurf trage eine „grüne Handschrift".

Mit solchen Geheimdienst- und Polizeigesetzen, wie im schwarz-grün regierten Hessen geplant oder im grün-schwarz regierten Baden-Württemberg teilweise schon umgesetzt, können die Grünen ihr Selbstverständnis als Bürgerrechtspartei allmählich begraben.

Ich bringe die Kritik an der hessischen Gesetzesinitiative noch einmal auf den Punkt:

1. Die künftig gesetzlich abgesicherte Zusammenarbeit mit vorbestraften und kriminell gewordenen V-Leuten widerspricht rechtsstaatlichen Grundsätzen.

2. Die geplante geheimdienstliche Regelüberprüfung künftiger MitarbeiterInnen von Demokratieprojekten bedeutet Gesinnungsschnüffelei und erinnert an unselige Zeiten grundrechtswidriger Berufsverbote.

3. Verhaltenssteuernde und freiheitsberaubende elektronische Fußfesseln verletzen Privatsphäre und Persönlichkeitsrechte – und letztlich auch die Menschenwürde.

4. Und Staatstrojaner bedrohen den Kernbereich privater Lebensführung und gefährden Sicherheit und Vertraulichkeit des IT-Systems.

Das ist „digitale Inquisition", so Heribert Prantl von der Süddeutschen Zeitung. Und er fragt erstaunt, weshalb die allermeisten BürgerInnen sich das gefallen lassen.[8] Und liefert drei Antworten gleich mit: 1. wegen der Politik mit der Angst vor Terror, die die WählerInnen selbst maßlose Freiheitsbeschränkungen schlucken lässt, wenn sie angeblich mehr Sicherheit versprechen; 2. weil die meisten Freiheitsbeschränkungen nicht zu spüren sind, da sie heimlich stattfinden, und 3. weil die BürgerInnen letztlich darauf vertrauten, dass das Bundesverfassungsgericht es wieder richten möge.

Apropos Bundesverfassungsgericht: Es gibt bereits Initiativen für Verfassungsbeschwerden, so u. a. von Digitalcourage, um etwa Staatstrojaner stoppen zu lassen. Und so mündet diese Laudatio in einen öffentlichen Appell, solche Verfassungsbeschwerden kräftig und massenhaft zu unterstützen – als Akt bürgerrechtlicher Notwehr.

Herzlichen Glückwunsch, CDU- und grüne Fraktion im hessischen Landtag, zum BigBrotherAward 2018.

Anmerkungen

1 *Vgl. Süddeutsche Zeitung vom 4.8.2017, http://www.sueddeutsche.de/bayern/innere-sicherheit-landtags-gruene-klagen-gegen-verfassungsschutzgesetz-1.3614760*
2 *Entwickelt werden die Staatstrojaner für die bundesdeutschen Sicherheitsbehörden u. a. von der 2017 in München eingerichteten „Zentralstelle für Informationstechnik im Sicherheitsbereich" (ZITiS).*
3 *BVerfE vom 27.02.2008; vgl. auch BVerf-Urteil 1 BvR 966/09.*
4 *Gemeinsame Erklärung: http://vs.hu-hessen.de*
5 *Gutachten zum hessischen Verfassungsschutz-Gesetzentwurf: https://hessischer-landtag.de/node/2490; Bericht: https://netzpolitik.org/2018/breitseite-gegen-staatstrojaner-in-hessen-verfassungswidrig-und-gefaehrlich/*
6 *https://netzpolitik.org/2017/streit-um-geplantes-hessentrojaner-gesetz-bei-den-gruenen/; https://www.gruene-hessen.de/partei/beschluss/digitale-gefahrenabwehr-statt-digitaler/*
7 *https://www.gruene-hessen.de/landtag/files/2013/01/KP24-NETZPOLITIK-web4.pdf*
8 *Süddeutsche Zeitung vom 27.01.2018*