Terrorismus bekämpfen – Grundrechte wahren!

European United Left • Nordic Green Left
EUROPEAN PARLIAMENTARY GROUP
GUE/NGL
www.guengl.eu

Impressum

Herausgegeben von der Delegation DIE LINKE. im Europaparlament, Konföderale Fraktion der Vereinten Europäischen Linken / Nordische Grüne Linke GUE / NGL

Besonderer Dank gilt allen Autor*innen und Mitstreiter*innen die uns bei der Erstellung der vorliegenden Studie unterstützt haben.

Redaktion: Dr. Cornelia Ernst, Lorenz Krämer, Anja Eichhorn

Bildnachweise:
Seite 1: flickr.com, LawrenceHolmes., CC BY 2.0
Seite 6: www.pixabay.com, CC0 Public Domain
Seite 9: pixabay.com, ar130405
Seite 13: www.pixabay.com, CC0 Public Domain
Seite 16: flickr.com, k_tjaaa, CC BY 2.0
Seite 20: wikimedia.org, Romaine, CC0 1.0 Universal
Seite 24: flickr.com, k_tjaaa, CC BY 2.0
Seite 27: wikimedia.org, jxandreani, CC BY 2.0
Seite 30: flickr.com, novofotoo, CC BY 2.0
Seite 39: DIE LINKE. im EP
Seite 40: flickr.com, LawrenceHolmes., CC BY 2.0

Fertigstellung und Publikation am 20. April 2017

www.guengl.eu
www.dielinke-europa.eu

European United Left • Nordic Green Left
EUROPEAN PARLIAMENTARY GROUP
GUE/NGL
www.guengl.eu

Die Autor*innen

Terrorismus bekämpfen, Grundrechte wahren
Dr. Cornelia Ernst, MdEP
… ist seit 2009 Mitglied des Europäischen Parlaments. Sie ist Mitglied im Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres sowie im Ausschuss für Industrie, Forschung und Energie. Die sächsische Co-Sprecherin der Delegation DIE LINKE. im Europaparlament hat sich als Expertin für individuelle Freiheitsrechte in der EU einen Namen gemacht. Im Innenausschuss setzt sie sich für Datenschutz, gegen Überwachung und für eine Asylpolitik ein, die Menschen willkommen heißt und nicht bekämpft.

Lorenz Krämer
… ist seit 2009 parlamentarischer Mitarbeiter von Cornelia Ernst in Brüssel. Er setzt sich hauptsächlich mit den Themen Datenschutz, Überwachung und Netzpolitik auseinander und berät Cornelia in diesen Fragen.

Massenüberwachung – läuft!
Martina Renner, MdB
… ist seit 2013 Mitglied des Deutschen Bundestages für die Fraktion DIE LINKE. Hier ist sie Obfrau der LINKEN. im NSA-Untersuchungsausschuss und ordentliches Mitglied im Innenausschuss. Darüber hinaus ist Martina Renner Sprecherin für antifaschistische Politik.

Auf dem Weg zu einem EU-Bevölkerungsregister
Matthias Monroy
… ist Wissensarbeiter, Aktivist und Mitglied der Redaktion der Zeitschrift Bürgerrechte & Polizei / CILIP. In Teilzeit Mitarbeiter des MdB Andrej Hunko. Publiziert in linken Zeitungen, Zeitschriften und Online-Medien, bei Telepolis, Netzpolitik und in Freien Radios. Alle Texte und Interviews unter digit.so36.net, auf englisch digit.site36.net,
auf Twitter @matthimon.

The surveillance armada
Estelle Massé
… ist Senior Policy Analyst im Brüsseler Büro von accessnow. Ihre Hauptthemen sind Datenschutz und Privatsphäre, Überwachung, Netzneutralität und Handel.

European counter-terrorism measures: the blind leading the blind
Olivier Winants
… ist Fraktionsmitarbeiter der Konföderalen Fraktion der Vereinigten Europäischen Linken / Nordischen Grünen Linke (GUE / NGL) und dort für die Themen Datenschutz, Überwachung, Straf- und Zivilrechtskooperation zuständig.

Der Einsatz von Überwachungsinstrumenten im Freistaat Sachsen
Klaus Bartl, MdL
… ist seit 1990 Abgeordneter im Sächsischen Landtag der Fraktion DIE LINKE. Der Jurist und Rechtsanwalt ist zudem stellvertretender Fraktionsvorsitzender der Fraktion DIE LINKE. und für seine Fraktion als Verfassungs- und rechtspolitischer Sprecher tätig. Darüber hinaus ist Klaus Bartl Vorsitzender des Verfassungs- und Rechtsausschusses im Sächsischen Landtag.

Probleme der Rechtsstaatlichkeit im Antiterrorkampf
Frank Tempel, MdB
… ist seit 2009 Mitglied des Deutschen Bundestages für die Fraktion DIE LINKE. im Bundestag. Dort ist er Mitglied und stellvertretender Vorsitzender im Innenausschuss des Bundestages sowie Drogenpolitischer Sprecher seiner Fraktion. Zudem ist Frank Tempel Leiter des Arbeitskreises V für Demokratie, Recht und Gesellschaftsentwicklung.

Frankreich im andauernden Notstand
Marie-Christine Vergiat, MdEP
… ist seit 2009 für die französische Front de gauche Mitglied der Konföderalen Fraktion der Vereinigten Europäischen Linken / Nordischen Grünen Linke (GUE / NGL). Sie ist Mitglied im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres und im Unterausschuss für Menschenrechte. Außerdem ist Marie-Christine Vergiat Mitglied in der Delegation für die Beziehungen zum Panafrikanischen Parlament.

Inhalt

Vorwort 5

Massenüberwachung – läuft! 7
Martina Renner, MdB

Auf dem Weg zu einem EU-Bevölkerungsregister 10
Matthias Monroy

The surveillance armada 14
Estelle Massé

European counter-terrorism measures: the blind leading the blind 17
Olivier Winants

Der Einsatz von Überwachungsinstrumenten im Freistaat Sachsen 21
Klaus Bartl, MdL

Probleme der Rechtsstaatlichkeit im Antiterrorkampf 25
Frank Tempel, MdB

Frankreich im andauernden Notstand 28
Marie-Christine Vergiat, MdEP

Terrorismus bekämpfen, Grundrechte wahren 31
Dr. Cornelia Ernst, MdEP und Lorenz Krämer

Ansprechpartner*innen 38

Vorwort

Mittlerweile bestimmen die Bilder von Anschlägen, toten oder verletzten Menschen, ob in St. Petersburg oder Stockholm, Damaskus oder Mossul die täglichen Nachrichten über eine Welt, die aus den Fugen zu geraten scheint. Das hat einerseits das Gefühl vieler Menschen verstärkt, dass sicher Geglaubtes gar nicht so sicher ist und andererseits zu Abstumpfungen geführt, die zwischen Opfern erster und zweiter Klasse unterscheiden. Es ist wie eine Spirale: Immer die gleichen Reaktionen, immer die gleichen Folgehandlungen der Regierenden, kaum etwas verändert sich. Dass die Attentäter von Brüssel bereits aus den Anschlägen in Paris bekannt waren, wird gern vergessen. Stattdessen werden Millionen Gelder verschwendet für die Präsenz von Militär an Grenzen, vor Parlamenten und anderen öffentlichen Gebäuden, ohne damit auch nur das Geringste zu bewegen. Die wirklichen Strukturen des Terrorismus werden unter hektischen Reaktionen vernebelt, ihre Mystifizierung dadurch eher verstärkt.

Die Quellen des Terrorismus bleiben unangetastet, will man es sich doch mit profitablen Geschäftspartner*innen nicht verscherzen. Die fehlende ehrliche Evaluation von Anti-Terror-Maßnahmen hat Konservativen und Rechtspopulisten bislang in die Hände gespielt, so dass dieser höchst profitable Wirtschaftszweig nie um seine Berechtigung bangen musste. Dazu gehört auch die völlig unklare Bestimmung, was unter terroristischen Handlungen zu verstehen ist. Die auch in der neuen Terrorismusrichtlinie verwendete Definition erlaubt es, u. U. auch Proteste zu kriminalisieren, was nicht nur Grundrechte gefährdet, sondern auch den Erfolg einer wirksamen Bekämpfung des Terrorismus. Deshalb fordern wir eine unabhängige, seriöse Evaluation aller Maßnahmen und Instrumente zur Terrorismusbekämpfung. Auf dieser Grundlage gilt es dann zu prüfen, wie wir auf europäischer wie mitgliedsstaatlicher Ebene zu einer effizienten und nachhaltigen Bekämpfung von Terrorismus kommen können. Opfer und deren Angehörige verlangen nicht nur Aufklärung und Konsequenzen, sondern auch klare Antworten und wirksame Gegenkonzepte. Dazu gehört auch die Ehrlichkeit, dass es kein Allheilmittel gegen Terrorismus gibt, dessen Bekämpfung Aufgabe der gesamten Gesellschaft ist. Das schließt auch eine aufgeklärte und selbstermächtigte Zivilgesellschaft ein. Einzelne Repressionsmaßnahmen ersetzen das nicht.

Deshalb muss sich auch die Linke in den Mitgliedsstaaten wie auf europäischer Ebene mit ihren Vorstellungen und Konzepten einschalten. Wir können diesen Diskurs, der auf die Zukunft unserer Länder Einfluss hat, nicht Konservativen und Rechten überlassen, zumal dessen Ergebnisse den Charakter unserer Gesellschaft künftig noch stärker prägen werden.

Mit diesem E-Book soll dafür ein Beitrag geleistet werden. Wir brauchen in der Linken Europas eine offene Debatte über Terrorismus und sicherheitspolitische Positionen. Dazu haben wir Erfahrungen, die wir auf europäischer, aber auch mitgliedsstaatlicher und regionaler Ebene sammeln konnten, zusammengetragen und konzeptionelle Politikansätze zur Diskussion bereitgestellt.

Ich bedanke mich bei allen mitschreibenden Autor*innen und und hoffe auf eine spannende und sachbezogene Debatte.

Dr. Cornelia Ernst,
DIE LINKE im Europaparlament

Massenüberwachung – läuft!

Martina Renner, MdB

Eigentlich hätte der Prüfbericht der Bundesdatenschutzbeauftragten zur Kooperation des deutschen Auslandsgeheimdienstes mit seinem US-Pendant NSA gar nicht öffentlich werden sollen. Nur im Geheimen hätte darüber gesprochen werden sollen, dass beide gemeinsam in der Außenstelle Bad Aibling des Bundesnachrichtendienstes seit 2005 nichts Anderes als Massenüberwachung betreiben. Gemeinsam zapft man Satelliten und Kabel in Deutschland und weltweit an und erhebt, speichert, leitet aus und verarbeitet milliardenfach Kommunikationsverkehrsdaten und millionenfach Inhaltsdaten. Dass dies oftmals unter Rechtsbruch und Lüge gegenüber dem Parlament erfolgte, stört in Deutschland einige Abgeordnete, einen Teil der Öffentlichkeit und kritischen Presse. Der gesetzlose Dienst geht aber vorerst gestärkt aus dem Skandal hervor.

Im November 2016 verabschiedete das Parlament ein novelliertes Gesetz, mit dem die Befugnisse des BND klar Richtung anlasslose Massenüberwachung im In- und Ausland ausgeweitet wurden. Renommierte Verfassungsrechtler wie der ehemalige Präsident des Bundesverfassungsgerichts, Prof. Papier, aber auch Bürgerrechtsorganisationen wie amnesty international, engagierte Journalist_innen wie z. B. Reporter ohne Grenzen und das Institut für Menschenrechte kritisierten den Gesetzentwurf scharf. Ohne Erfolg. Herrschende Sicherheitspolitik bricht bewusst Grundrechte auf Meinungsfreiheit und Schutz der Privatsphäre.

Es ist inzwischen das Jahr drei nach Snowden. Tausende schauen sich das Schicksal des Whistleblowers als Spielfilm im Kino an. Niemand bezweifelt ernsthaft mehr, dass er im Recht war mit seinen Taten und Mahnungen. Keiner zweifelt mehr ernsthaft an, dass das, was auf den Dokumenten der NSA als „Global Reach"-Ansatz beschrieben wird, technische und operative Realität der Geheimdienste im Verbund mit der NSA ist. Der BND nennt es verschämt Erfassung von „Routineverkehren". Der Begriff kann kaum beschreiben wie grundlegend die Zäsur der Kommunikationsüberwachung Anfang der 2000er Jahre war. Mit dem Eintritt in das Internetzeitalter vollzog sich ein Paradigmenwechsel im deutschen Auslandsnachrichtendienst. Bis dahin horchte man Telefon- und Faxverbindungen ab.

Mit dem digitalen Zeitalter und nach den schrecklichen Terrorereignissen vom 11. September 2001 begann ein neues Zeitalter der Datenerfassung. Jetzt ging es darum möglichst viel zu erfassen, durchzuscannen, die Daten zu vernetzen, Profile zu bilden, Prognosen zu treffen. Sinnbildlich für diesen neuen Erfassungs- und Auswertungsansatz steht die auch in den Snowden-Dokumenten beschriebene Soft- und Hardware XKeyscore, die auch bei den deutschen Auslands- und Inlandsgeheimdiensten zum Einsatz kam. Im Tausch liefern sie Daten aus Abgriffen an Satelliten zu Krisen- und Kriegsregionen oder am Datenknoten der Deutschen Telekom in Frankfurt.

Um Datenschutzregelungen im BND-Gesetz zu umgehen, erfand der BND die ‚Weltraumtheorie': Für Daten, die von der Satellitenerfassungsstation in Bad Aibling erfasst wurden, sollten die Regelungen nicht gelten, weil die Daten im Weltraum, außerhalb des Geltungsbereichs des BND-Gesetzes, erfasst würden. Von der Telekom erzwang man den Kabelzugriff für die NSA erst durch einen Blankobrief aus dem Bundeskanzleramt, mit dem das ehemalige Staatsunternehmen genötigt wurde, die Ausleitung der Daten an den BND technisch umzusetzen. Als die Telekom später auf G10-Anordnungen bestand – also das übliche Verfahren zur Überwachung von Telekommunikation in Deutschland, nutzte man die Anordnungen z. B. zur Überwachung vermeintlicher Terroristen vom Sudan bis Tschetschenien als Türöffner um an das eigentliche Ziel zu kommen: die Routineverkehre insbesondere zwischen europäischen Staaten.

Ähnliche Operationen fanden mit der CIA in Hilden bei Düsseldorf statt. Dort wurde die deutsche Tochter des US-amerikanischen Telekommunikationsunternehmen MCI Worldcom getäuscht, um ans Kabel zu gelangen. Unter Legende einer privaten Firma installierte man ein Gerät, das vermeintlich der Aufdeckung von Leistungserschleichung diente und machte sich noch nicht mal die Mühe, eine G10-Anordnung vorzutäuschen. Ähnlich verfuhr man in der Zusammenarbeit mit dem britischen Auslandsgeheimdienst GCHQ. Dessen Fähigkeit zur Erfassung, Komprimierung und Auswertung von Metadaten (bekannt auch als das in den Snowden-Dokumenten beschriebene Programm Tempora) faszinierte die deut-

schen Geheimdienstler derart, dass man als Gegenzug die Briten ebenfalls an Kabelverbindungen in Frankfurt lassen wollte. Diese Operationen waren dem Kontrollgremium des bundesdeutschen Parlaments vollkommen unbekannt.

Unklar ist auch, welche Informationen in den für die Fach-, Rechts-, und Dienstaufsicht zuständigen Ministerien, dem Bundeskanzleramt und dem Innenministerium, vorlagen. Wenn überhaupt, wusste man dort nur in Grundzügen, was die Abteilung „Technische Aufklärung" im BND so trieb. Grundlage für das Versagen der Aufsicht war auch eine als „Drehtür-System" bezeichnete Personalpolitik in den zuständigen Referaten der Aufsicht. Dort, im Bundeskanzleramt, saßen und sitzen viele ehemalige BND-Beschäftigte. In der BND-Abteilung „Technische Aufklärung" wiederum herrschte ein militärisches Regime, das zwei Prinzipien folgt: „Klappe halten" und „Der Zweck heiligt die Mittel", dem überwiegend Soldaten der Bundeswehr in enger Verbundenheit mit den USA willig folgten.

Aktuell beschäftigen sich sowohl öffentliche Debatte als auch parlamentarische Aufklärung maßgeblich mit den eingesetzten Suchbegriffen von NSA und BND – den Selektoren. Die Problematik der für den Einsatz von Selektoren notwendigen milliardenfach anlasslos erhobenen Grunddaten tritt dabei hinter den offenkundig skandalösen Einzelprofilen zurück, mit denen die Daten durchforstet wurden. Jenseits des Auftragsprofils des BND und der angeblich gemeinsamen Ziele des Antiterrorkampfes nahm man Parlamente, Regierungsbehörden, wissenschaftliche Einrichtungen und Hilfsorganisationen internationaler wie nationaler Bedeutung aus mit der Bundesrepublik eng verbunden Staaten der EU und der NATO in den Fokus.

Etwa 13 Millionen Suchbegriffe übergab die NSA im Rahmen der Zusammenarbeit an den BND. Dieser – unfähig auch nur einen Bruchteil der Überwachungsziele zu verstehen – durchsuchte damit seine Datenbanken und half der NSA bei politischer wie wirtschaftlicher Spionage von Konkurrenzen unter Industriekonzernen wie Airbus und Boeing oder in Fragen der Weltmarktkonkurrenz von Landwirtschaft bis Elektroindustrie. So kann auch nicht überraschen, dass der BND monatlich 1,3 Milliarden Metadaten erhob und überwiegend an die NSA gab. Richtig aufregen kann sich über den Umstand der politischen Instrumentalisierung so wirklich niemand in der politischen Sphäre. Das Credo ist: das machen doch alle. Das Verhalten der Dienste ist offenbar genau so gewollt und man nimmt das Abhören von Regierungskommunikation eher sportlich. Das Wort der Kanzlerin „Abhören unter Freunden geht gar nicht" aus dem Sommer 2013 hat beim BND nicht wirklich zur Einsicht geführt, sondern lediglich zum schnellen und nicht nachvollziehbaren Beseitigen der Beweise.

Eigentlich hat es richtig gescheppert. Die Bundesdatenschutzbeauftragte stellte eine Vielzahl von Rechtsverstößen allein bei der Kooperation von NSA und BND in Bad Aibling fest und rügte den BND in 17 Fällen. Ein weiterer einmaliger Vorgang: die G10-Kommission versuchte den BND zu verklagten und musste feststellen, dass ein Gremium, das quasi einem Richter bei der Bewilligung von Kommunikationsüberwachung durch Strafverfolgungsbehörden gleichgestellt ist, nicht zur Kontrolle berechtigt sei soll. Das Betreiberkonsortium des größten Internetknotens De-Cix klagt gegen den BND. Aber statt die Befugnisse des BND zu begrenzen und Grundrechtseingriffe streng einzugrenzen, bekommt der BND mit der Novelle des für seine Arbeit grundlegenden Gesetzes quasi mit der NSA oder dem GCHQ vergleichbare Kompetenzen. Dazu kommt, dass der BND jetzt auch hoch hinauswill. Er verlangt nach eigenen Satelliten, die ihm die Bundesregierung bzw. die Steuerzahler spendieren sollen. Und es geht noch weiter: Der BND soll 150 Millionen Euro Steuergelder bekommen, um damit im Namen der Sicherheit massive Unsicherheit zu schaffen. Während die Bundesregierung die Bedeutung von IT-Sicherheit erkennt und dazu Strategien entwickelt, soll der Geheimdienst nach Sicherheitslücken suchen, diese auf Schwarzmärkten kaufen und anwenden. Jede Sicherheitslücke, die nicht geschlossen wird, bleibt aber für viele andere nutzbar: für fremde Geheimdienste, für Wirtschaftsspionage und für andere Kriminelle. Sicherer wird unsere digitale Welt mit einer solchen Strategie jedoch nicht.

Auch der Inlandsgeheimdienst rüstet auf. Die Überwachung sozialer Netzwerke wird massiv ausgebaut in der irrigen Annahme, dass Kommunikationsinhalte dort nicht grundrechtsgeschützt seien. Aber niemand ist bei Facebook, Twitter oder Instagram unterwegs, damit die Geheimdienste Informationen zu Kontaktpersonen, politischen Einstellungen, Aufenthaltsorten etc. speichert. Über mehrere Ebenen werden soziale und auch familiäre Beziehungen der Betroffenen insgeheim durchleuchtet. Gesichtserkennung, Videoüberwachung, das Hacken von Computern und Handys sind Realität. Inzwischen werden die erschnüffelten Daten quer durch Europa und auch mit den USA geteilt. Eine Kontrolle, um welche Daten es konkret geht und wer darauf zugreifen kann, gibt es nicht. Stattdessen werden Strafverfolger und Schlapphüte miteinander vernetzt, obwohl dies in Deutschland aus guten Gründen verboten ist. Und wenn keine Kontrolle stattfindet, gibt es natürlich auch keine Aufklärung. Die Bürger_innen werden allein gelassen mit dem Gefühl, ausgespäht und überwacht zu werden – von wem und wofür auch immer. Demokratie sieht anders aus!

Auf dem Weg zu einem EU-Bevölkerungsregister

Matthias Monroy

Im April will die EU-Kommission ihren Fahrplan für „verknüpfte Datentöpfe“ vorlegen. Eine Infografik zeigt erstmals das Ausmaß der umfangreichen Datensammlung im Bereich Justiz und Inneres.

Vor einem Jahr hat die Europäische Kommission eine „hochrangige Sachverständigengruppe[1] für IT-Systeme und Interoperabilität“ eingesetzt, um „bestehende Wissenslücken und Mängel in Informationssystemen auf Unionsebene“ zu untersuchen. Sie besteht aus der EU-Agentur für das Management der IT-Großsysteme (eu-LISA), der Grenzagentur Frontex, dem Europäischen Polizeiamt Europol, dem Unterstützungsbüro für Asylfragen (EASO) und der EU-Grundrechteagentur. Ebenfalls beteiligt ist der EU-Koordinator für die Terrorismusbekämpfung Gilles de Kerchove. Auch die Behörden des gesamten Schengen-Raums entsenden VertreterInnen und Sachverständige. Den Vorsitz der Gruppe übernimmt die Europäische Kommission.

Der Abschlussbericht der „hochrangigen Sachverständigengruppe“ war eigentlich für Juni 2017 angekündigt, nun ist die Veröffentlichung auf April vorverlegt. Bis dahin sollen sich drei Unterarbeitsgruppen mit den bestehenden, den zukünftigen Datenbanken sowie deren Interoperabilität befassen. Im Dezember hat die Kommission einen Zwischenbericht[2] vorgelegt. Das Papier enthält richtungsweisende Vorschläge für ein EU-weites „integriertes biometrisches Identitätsmanagement für Reisen, Migration und Sicherheit“. Jede der einzelnen Maßnahmen birgt laut dem Dokument größere Herausforderungen in der technischen und operationellen Umsetzung. Schließlich müssten auch rechtliche Fragen und die Berücksichtigung des Datenschutzes geklärt werden.

Einheitliche Suchmaske zur gleichzeitigen Abfrage mehrerer Informationssysteme

Werden Personen beim Grenzübertritt oder im Rahmen einer Polizeikontrolle überprüft, sollen zukünftig sämtliche größere Polizeidatenbanken abgefragt werden. Dies beträfe das Schengener Informationssystem (SIS), das Visa-Informationssystem (VIS), die Fingerabdruckdatenbank EURODAC, das Europäische Strafregister (ECRIS), das Europolsystem sowie die Interpol-Datenbank für als verloren oder gestohlen gemeldete Ausweisdokumente. Schon jetzt ist geplant, die derzeit in der Entwicklung befindlichen neuen EU-Reiseregister ebenfalls in die einheitliche Suchmaske einzubinden. Hierzu gehören das „Ein-/Ausreisesystem“ (EES)[3] und ein Register zur Anmeldung geplanter Reisen (ETIAS)[4].

eu-LISA, die EU-Agentur, die im Jahr 2012 für den Betrieb der großen EU-Datenbanken eingerichtet wurde, soll nun eine Machbarkeitsstudie für die einheitliche Suchmaske beauftragen. Die Ergebnisse könnten in einem Pilotprojekt getestet werden. Die „Expertengruppe“ schlägt hierfür zunächst die Datenbanken SIS und VIS vor. Zusammen mit eu-LISA sollen auch Europol und Interpol prüfen, unter welchen Voraussetzungen die dort geführten Informationssysteme eingebunden werden könnten. Europol betreibt hierfür bereits ein Pilotprojekt unter dem Namen „Querying Europol Systems“ (QUEST), das nächstes Jahr in einigen Mitgliedstaaten beginnen soll.

Um auch das Strafregister ECRIS über eine einheitliche Suchmaske abzufragen, müsste das dezentral geführte System auf EU-Ebene angesiedelt werden. Derzeit wird die ECRIS-Verordnung neu formuliert[5], außer den Kriminalakten und Urteilen von EU-Staatsangehörigen sollen auch Daten

[1] https://netzpolitik.org/2016/eu-innenkommissar-fordert-abfrage-mehrerer-polizeidatenbanken-mit-einem-einzigen-klick/

[2] http://www.statewatch.org/news/2016/dec/eu-com-hlg-interoperability-report.pdf

[3] https://netzpolitik.org/2014/riesige-eu-vorratsdatenspeicherung-aller-ein-und-ausreisen-aufbau-lohnt-sich-laut-innenministerium-nur-bei-nutzung-durch-polizei-und-geheimdienste/

[4] https://netzpolitik.org/2016/passagierdaten-und-reiseregister-genuegen-nicht-eu-plant-weitere-datenbank-zur-einreisegenehmigung/

[5] https://netzpolitik.org/2016/eu-plant-ausbau-vernetzter-datenbanken-von-justiz-und-polizei/

zu Drittstaatenangehörigen erfasst werden. Im Zuge der Diskussionen um die Neufassung der Verordnung sprechen sich viele Mitgliedstaaten für die Zentralisierung von ECRIS aus.

Zusammenführen aller biometrischen Datenbanken

In den vier Datenbanken SIS, VIS, EURODAC und ECRIS speichern die EU-Mitgliedstaaten derzeit Fingerabdrücke und/oder Gesichtsbilder. Das dezentral verabredete „Prüm-Verfahren" erleichtert den Zugriff auf national geführte Fingerabdruck- und DNA-Datenbanken. Auch das geplante zentral geführte EES soll biometrische Daten verarbeiten und fünf Jahre lang aufbewahren. Würden diese Systeme über die einheitliche Suchmaske abgefragt, ergäbe sich daraus laut der „Sachverständigengruppe" eine herausragende Innovation. Mit der übergreifenden Suche nach Fingerabdrücken und Gesichtsbildern könnten beispielsweise Personen, die sich mit unterschiedlichen Identitäten registrieren, aufgespürt werden.

Allerdings stehen rechtliche Bedenken im Weg, denn jede Datenbank dient einem bestimmten Zweck. Würde dieser erweitert, muss jede einzelne Verordnung geändert werden. Die Gruppe schlägt deshalb vor, die Treffermeldungen zu anonymisieren. Würde etwa eine Person in EURODAC abgefragt, könnte das System melden, dass auch im EES biometrische Daten zu der Person vorliegen. Anschließend könnte dort eine weitere Abfrage erfolgen. Ein entsprechendes Pilotprojekt wird bereits von einigen EU-Mitgliedstaaten sowie Europol unter dem Namen „Automatischer Daten Austausch Prozess" (ADEP)[6] betrieben.

Mit dem Zusammenführen der biometrischen Datenbanken will sich die Europäische Kommission einige Jahre Zeit lassen. Vorgeschlagen wird, hierfür die Plattform des zu errichtenden EES zu nutzen. eu-LISA und Europol werden mit der Prüfung beauftragt, inwiefern zunächst die Datenbanken SIS, VIS und EURODAC sowie Informationssysteme bei Europol in das EES integriert werden könnten. Schließlich werden auch die Prüm-Partner[7] aufgefordert, Möglichkeiten der Einbindung des Prüm-Verbundes zu prüfen. Denkbar sei zudem, weitere nationale Biometrie-Datenbanken auf EU-Ebene anzusiedeln. Kleinere Mitgliedstaaten würden sich laut der „Sachverständigengruppe" enorme Kosten ersparen, wenn sie auf EU-Infrastruktur zurückgreifen anstatt eigene Systeme zu entwickeln und zu beschaffen.

[6] http://dipbt.bundestag.de/doc/btd/18/083/1808323.pdf

[7] https://de.wikipedia.org/wiki/Pr%C3%BCmer_Vertrag

Gemeinsames Personenarchiv

Die beiden derzeit errichteten Reiseregister EES und ETIAS sollen eine gemeinsame Personendatenbank führen. Wer sich also zum Grenzübertritt anmeldet, erzeugt einen alphanumerischen Datensatz, der bei der späteren Ein- und Ausreise mit weiteren Informationen angereichert wird. Hierzu gehören auch „Hintergrundinformationen" zur Reise oder die bei der Eingabe genutzte IP-Adresse.

Das Personenarchiv könnte um andere Systeme erweitert werden. eu-LISA wird aufgefordert zu prüfen, inwiefern beispielsweise Daten aus dem SIS, dem VIS oder EURODAC genutzt werden könnten. Selbst die Integration von Europol-Daten sei möglich. Auf diese Weise würde die „Fragmentierung" der europäischen Datenbankarchitektur behoben. Dabei gehe das neue System sparsam mit Daten um, wenn gleiche Personendatensätze nur noch an einer Stelle abgelegt sind. Denkbar sei deshalb sogar das „Verschieben" („relocating") aller Daten aus vorhandenen Informationssystemen in das gemeinsame Personenarchiv. Weil ein solches (grenz-)polizeiliches Bevölkerungsregister immense Auswirkungen auf den Datenschutz hätte, werden der EU-Datenschutzbeauftragte und die Grundrechteagentur um Einschätzungen gebeten.

Eigentlich war das Reiseregister EES lediglich für Angehörige von Drittstaaten geplant. Nach den von 2015 konnte sich Frankreich mit dem Vorschlag durchsetzen, auch Grenzübertritte von EU-Angehörigen zu protokollieren. Die „Sachverständigengruppe" soll nun prüfen, welche rechtlichen Anpassungen für eine solche Erweiterung erforderlich sind.

Datenqualität und einheitliche Formate

Außer der Neuordnung von existierenden und geplanten Informationssystemen befasst sich die „Sachverständigengruppe" mit zwei Querschnittsthemen. Bemängelt wird die häufig unzureichende Qualität der Daten, die aus den Mitgliedstaaten angeliefert werden. Dies betrifft etwa die Schreibweise oder ausgelassene Datenfelder. Dadurch ergäben sich Lücken bei der „Identifizierung von irregulären Migranten oder von Terroristen". Auch gerieten unschuldige Personen durch falsche Eingaben ins Visier der Behörden. Mitunter werden die Datensätze aufgrund mangelnder oder einander ausschließender Angaben von den EU-Informationssystemen gar nicht angenommen. Hier soll eine Überprüfung der Daten bereits bei ihrer Eingabe von Grenzbehörden, Konsulaten oder Ausländerämtern in die nationalen Systeme abhelfen.

Unter Leitung des Bundeskriminalamtes[8] arbeiten Europol, Interpol und einige Mitgliedstaaten seit 2007 an einem „Universellen Nachrichtenformat" („Universal Message Format", UMF) für einen „verbesserten automatisierten Informationsfluss". Das UMF soll zum Standard für sämtliche Daten zu Personen und Sachen in den europäischen Informationssystemen werden. Die „Expertengruppe" schlägt deshalb vor, das UMF auch für die geplanten Datenbanken ETIAS und EES zu nutzen.

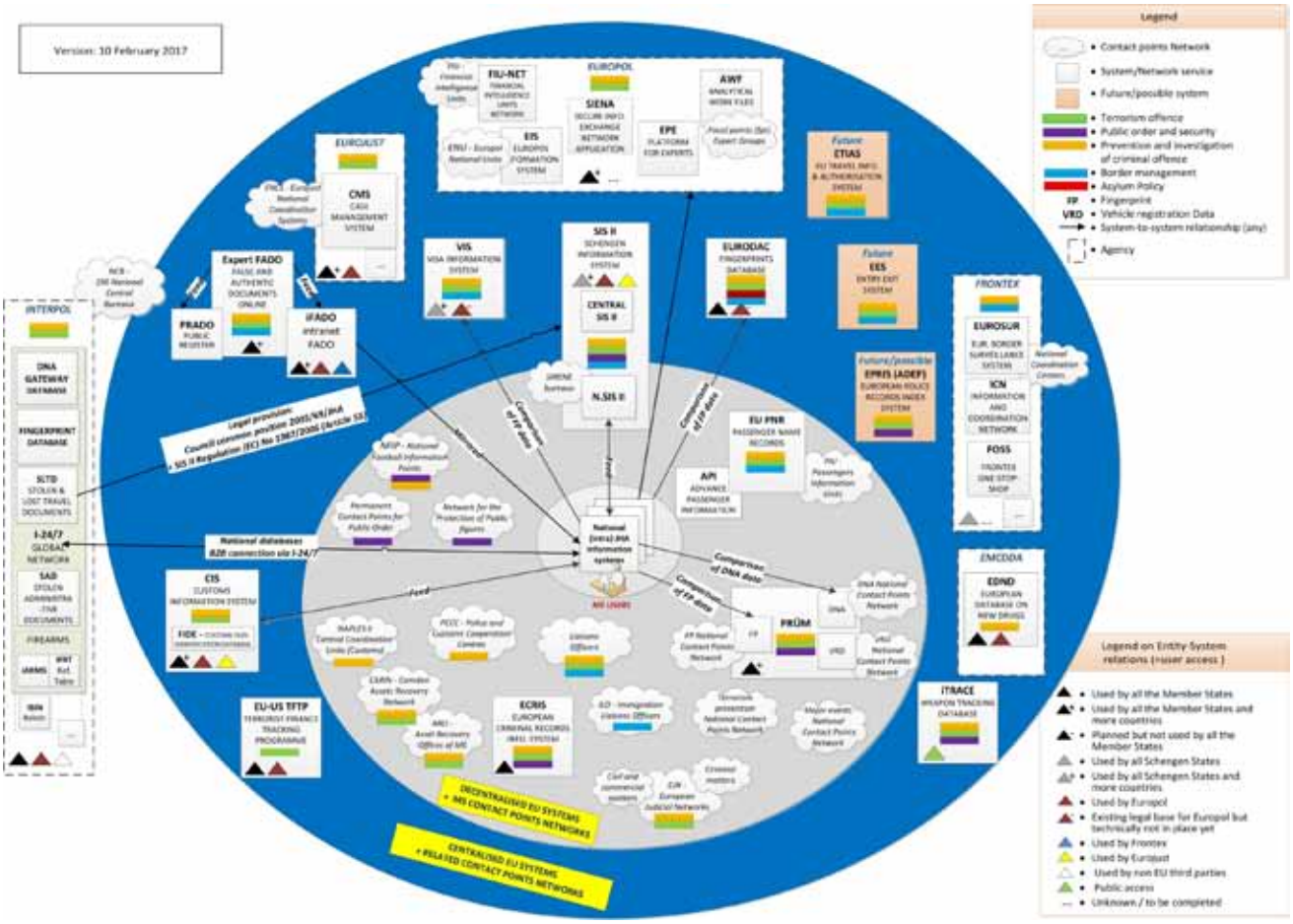
Infografik zeigt erstmals Ausmaß der Datensammlung im Bereich Justiz und Inneres

Das Verschmelzen der fünf wichtigsten Datentöpfe ist nicht das einzige Thema der „hochrangigen Sachverständigengruppe". Sie soll sämtliche bestehenden Informationssysteme begutachten und auf ihren Nutzen prüfen. Anschließend werden operative und rechtliche Schwächen benannt. Bei dezentralen Systemen stehen die Behörden beispielsweise vor dem Problem, dass in den Mitgliedstaaten oft unterschiedliche Software verwendet wird. Die „Sachverständigengruppe" prüft in diesen Fällen, ob die Systeme auch zentralisiert werden könnten.

Eine Infografik[9] der Europäischen Union zeigt nun erstmals das Ausmaß der umfangreichen Datensammlung im Bereich Justiz und Inneres. Sie zeigt Datenbanken der Polizei, des Zolls und von EU-Agenturen wie Europol oder Frontex und soll den Delegationen aus den Mitgliedstaaten der Europäischen Union beim Verstehen der Datenlandschaft behilflich sein.

[8] https://netzpolitik.org/2016/verknuepfung-europaeischer-datentoepfe-bka-und-europol-proben-technische-umsetzung/

[9] http://data.consilium.europa.eu/doc/document/ST-6253-2017-INIT/en/pdf



Stop
Terror

The surveillance armada

Estelle Massé

It has become an embarrassing yet predictable announcement after each terrorist attack to hear: "Most of the attackers were known to authorities". But despite the availability of this information, the immediate solution usually put forward by government officials is to increase the realm of their authorities' surveillance powers, to develop mass surveillance capabilities in order to be able to spy on anyone at anytime. We had the data, but we need more.

Fear can be powerful and blinding. Certain politicians know how to exploit that fear to advance measures that would not have been easily accepted by people under others circumstances. SIM card registration, data retention, facial recognition cameras, biometric collection, online surveillance and more are some of the measures presented as solutions to fight terrorism. These measures create significant interferences with people's right to privacy and free expression without empirical data showing their efficiency in enhancing security. Nevertheless, these measures are being implemented.The deployment of CCTV in London was a response to the IRA attacks in the 90s. The adoption of an EU law on data retention of phone records was a response to the London and Madrid bombings in 2006. Most recently, the passage of an EU law to track flying passengers was a response to the Paris and Brussels attacks. The surveillance armada keeps on growing, but attacks keep happening.

Everyone of us is under surveillance. Edward Snowden showed us the extent of the US surveillance, in cooperation with the five, nine or eleven eyes. Almost every government spy on their citizens, and in the European Union the spying has only been increasing since the Snowden revelations. The initial outrage of EU leaders on the NSA spying activities is long gone. As Europe faced a high number of violent terrorist attacks, most governments fell back into the "collect it all" narrative. Germany, France, the UK, Denmark, Belgium have all increased surveillance measures on the population. Whether you are walking down the street, speaking on the phone or browsing online, you are being watched.

Increasing the surveillance armada has been made easier with technology. To control our communications, governments are gaining access to tech companies data, whether these are willing or not, aware or not. From skype calls to Facebook chats, from emails to browsing history, most government authorities can collect it all, and access it all. The development of the internet of things, connected devices represent "key pieces of evidences" for law enforcement authorities. In the United States, several murder cases are ongoing where police is trying to retrieve data from smart home devices to confirm stories. Similarly, a man from Ohio was charged with insurance fraud after his pacemaker data revealed that he lied to the authorities. Other companies from the military and security industry are capitalising on people's fear to sell equipment to governments that will further increase their surveillance capacities. A research from the Dutch investigative paper The Correspondent shows how this industry, in charge of making us safe, "is primarily taking good care of itself".

Today's tools, whether built for security purposes or not, represent an endless potential for government surveillance. But are we safer in return? We currently have no evidence of it. What is the impact on our lives? The negative effect of mass surveillance on people's life, from self-censorship to discrimination, have been largely documented. Measures adopted by government to surveill anyone on the basis of zero suspicion in the hope to make us all safer have been found disproportionate by several courts, including the EU Court of Justice who overturned the data retention directive.

Despite the lack of evidence on the efficiency of mass surveillance and its proven interference with human rights, authorities often question the reaction of people refusing to cave in to this security theater. After all, if you have nothing to hide, you have nothing to fear. This argument is used repeatedly by anyone trying to justify snooping into your personal life. As Daniel J. Solve explains in his book Nothing to Hide, "the issue with the nothing to hide argument is that it suggest that privacy is about hiding bad things." Privacy is not about hiding, it is about protecting your information, like when you use curtains for your house, an envelop for your mail or a password for your accounts. You

are not hiding information, you are protecting your intimacy and personal information. The "nothing to hide" argument is essentially a way for the authority to turn everyone into potential suspect on the basis of no evidence.

So where do we go from here? States and authorities should have the necessary powers to detect and prevent terrorist attacks. This, however, should not lead to a scenario where everyone become a suspect and to unlawful measures reducing civil liberties are adopted. Mass surveillance is therefore not the solution. To reduce the surveillance armada, a first step would be to require tech companies to adopt privacy by design and by default standards to limit their collection and storage of user data. At the moment, most governments in the EU tell us that gathering more data might somehow make us safer. We would consider the security argument serious, if only, member states would commit to share possible information about suspect they get through the analysis of this data, but this is not the case. You might ask yourself, what are we doing exactly? Well, collecting data about millions of people, surveilling them, ignoring the impact on human rights rights and hoping for the best. Even in EU Passenger Name Record Directive, the sharing of information about suspect betweens EU states is not mandatory. This means that, if one day this data collection measure whose efficiency has never been demonstrated, would somehow help prevent an attack, the relevant authorities might never get that information. But people will probably hear afterwards that "most of the attackers were known to authorities".

Freiheit statt Angst 2013, Berlin

European counter-terrorism measures: the blind leading the blind

Olivier Winants

We know the horrible legacy that the fear and blind repression spiral has left our world after 9/11: Guantanamo Bay, Abu Ghraib and the terrible torture prisons in Poland, Romania, Macedonia. Furthermore, a host of 'USA Patriot Act'-inspired measures that entailed unprecedented mass spying on its own population. All e-mails, mobile phone usage and browsing habits of the whole European population are recorded. The Court of Justice in Luxembourg annulled for that reason, in April 2014, the European data retention directive which allowed for mass espionage.

There is a mountain of academic, legal and professional lecture that questions the necessity and proportionality of such blanket data collection in the fight against terrorism. First, there has never been conclusively demonstrated to what extent these measures are really designed to guarantee our safety. European human rights treaties, however, make it clear that any measure which constitutes a serious violation of our rights, such as privacy, must prove that the measure is necessary to achieve the intended purpose and that less intrusive measures are not available. The European legislator has never provided that evidence.

Furthermore, the European Privacy Commissioners have long questioned these grotesque measures, mainly because they do more harm to our rights than they would protect it. None of these „privacy watchdogs' found conclusive evidence that an EU PNR measures, for example, would actually effectively help in fighting terrorism despite what the governments proclaim loudly. The aforementioned judgment of the Court of Justice found it cannot be that every citizen was treated as a suspect, which it correctly saw as a blatant violation of the presumption of innocence.

Several terrorist attacks (Toulouse, Boston, the assassination of Theo van Gogh, Jewish cultural center in Brussels, Charlie Hebdo ...) all had one thing in common: the perpetrators were known or were on „watch lists" of police and state security forces. The personal data were available. Thus, it is not a matter of collecting more information. Moreover, today there are many police and judicial measures already allowing to monitor specific suspects such as wiretapping of telephone or Internet, search and seizure, and shadowing. The successful police action in Verviers in 2015 was built on the existing operational measures, without it ever needing to use massive databases.

Why symbolic populist politics are dangerous for the erosion of human rights

There are several stories of anti-terrorist ‚blacklisting' measures, such as freezing the bank account, house arrest, or the imposition of a travel ban which have directly followed from counter-terrorism legislation codifying mass bulk data collection, another word for mass surveillance. These blanket measures have horrific and devastating effects, such as families who are doomed to live on charity or gifts from local residents, or people who are not allowed to attend the funeral of a parent or child in another country because of their name being blacklisted.

It is crucial to understand that in most of these cases there is never any formal evidence that these people have any actual links with terrorist networks. Often people are put on a blacklist by automated systems which correlate different sets of personal data into algorithmic predictions about potential dangerous behavior, without any actual criminal act being carried out. And equally often the ‚hits' in the systems pop up based solely on their name, or their ethnic or religious group which also gives legal objections concerning discrimination.

The real danger is even deeper, as it became painfully clear in the UK after the Snowden leaks. Then Prime Minister Cameron used the law on counter-terrorism in an attempt to silence the world-renowned newspaper The Guardian, which had published articles by Edward Snowden revealing the mass spying by the British government in the GCHQ scandal. Bitter is the irony: the same Cameron bluntly promises after the attack in Paris to tackle terrorism even harder in the name of free speech.

Other poignant examples of the dangerous of blanket mass surveillance legislation, sold to us as counter-terrorism measures: people arrested for mocking authorities in Facebook posts, or handcuffed be carried to the police station for reporting on social media that they want to take part in a public protest.

What we need: an in-depth evaluation of existing measures and a renewed commitment to uphold fundamental rights within counter-terrorism measures

In its recent report 'Dangerously disproportionate', Amnesty International rings the alarm about the erosion of the rule of law in European countries due to the dangerous amount of human rights-erosive legislation:

„Ultimately, however, the threat to the life of a nation – to social cohesion, to the functioning of Democratic Institutions, to respect for human rights and the rule of law – does not come from the isolated acts of a violent criminal fringe, However They wish to destroy much May thesis Institutions and undergraduate thesis principles mine – but from Governments and societies That are prepared to abandon their Own values in confronting them."

The developments Amnesty International so clearly exposes in its report are extremely worrying. The principles of our rule of law democracies – separation of powers, judicial supervision, the body of human rights –are becoming expertly demolished by the traditional parties and replaced by far-reaching powers united in the hands of the government.

With the threat of far-right parties on the rise, this is adding a layer of danger: they already have the legal tools at hand to execute their fascist-bordering policies. It is morbid to think that that we are closer to a pre-war Europe than the Europe which adopted the European Convention of Human Rights. And where this concentration of government power in the past was mainly organized by the extreme right and fascist parties, today it is defended without hesitation by the traditional center parties.

What we need is a complete paradigm shift: we have oppose any political discourse that preaches the false dichotomy between human rights and security. That there is a need for an effective protection of citizens' safety from terrorist attacks is beyond question, as well as the right and duty of a government to take urgent action when faced with imminent danger. But not against any price. These measures still need to strengthen the essence of a democratic constitutional state, not weaken it.

Today we need a courageous policy that departs from symbolic populist short-term politics and makes a strong case for targeted counter-terrorism measures that are based on the rule of law, respect and uphold human rights and that are actually monitored and evaluated for their effectiveness.

The European Parliament adopted in 2011 a detailed report[1] calling for an in-depth evaluation of the entire EU counter-terrorism policy. To this date, more than 200 (!!) counter-terrorism measures have been adopted at European level and we still lack any independent evaluation of whether these measures actually work!

As the European Parliament correctly demanded:

"Stresses that a proper evaluation of ten years of counter-terrorism policies should focus on examining whether the measures taken to prevent and combat terrorism in the EU have been evidence-based (and not based on assumptions), needs-driven, coherent and part of a comprehensive EU counter-terrorism strategy , based on an in-depth and complete appraisal, to be carried out in line with Article 70 of the TFEU, with the Commission reporting back to a Joint Parliamentary Meeting of the European Parliament and national parliamentary committees responsible for overseeing counter-terrorism activities within six months of the study being commissioned, drawing upon reports to be requested from relevant organisations and agencies such as Europol, Eurojust, the Fundamental Rights Agency, the European Data Protection Supervisor, the Council of Europe and the United Nations"

The European Commission, who is the initiator of counter-terrorism legislation, has consistently failed to uphold its 'constitutional' duty to check any human rights-infringing measures for its necessity and proportionality as required by article 52 of the Charter of Fundamental Rights, which is binding primary law. It's not just a cosy bonus evaluation that could be considered useful. No, it is an absolutely constitutional duty by the legislator, and it has consistently denied to provide clear impact assessments, on the necessity, proportionality and effects of these matters on civil liberties. Even worse, in the recent counterterrorism directive, it has not even provided any impact assessment at all!

The alternative: a more humane, human-rights driven, inclusive approach combined with targeted, rule-of-law based measures.

[1] http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2011-0286&language=EN

In all the recent attacks the suspects were known and sometimes even located by the intelligence services of at least two Member States. What has terribly gone wrong was the communication between the intelligence services themselves and the police cooperation across borders. It was not a lack of personal data, nor a lack of existing legal enforcement measures.

The new anti-terrorism measures of the last two years increasingly bet on collecting yet more personal data, but none of these measures would have prevented these attacks because they do not touch upon the operational problems and flaws within and between investigative services themselves. We need more human resources to properly train and staff our police forces.

We also need the political courage to evaluate the existing anti-terrorist measures in order to clearly understand which ones are working and which are not, and from there on to give form to a targeted and effective security policy with minimum impact on civil liberties and human rights, and based on clear factual proof.

Very importantly, we need a human preventive and inclusive approach to prevent radicalization and exclusion. We need a preventive policy that starts from the streets, through investing in street workers, social inclusion policies and the promotion of socio-economic cohesion, and so build a real anti-discrimination culture. To quote the words of the Belgian mayor Bart Somers at a conference on ‚foreign fighters' in Mechelen: only through inclusion can we avoid radicalization.

Vor der Brüsseler Börse haben die Menschen Blumen im Gedenken an die Opfer vom 22. März 2015 niedergelegt.

Der Einsatz von Überwachungsinstrumenten im Freistaat Sachsen

Klaus Bartl, MdL

Wenn es um die Aushöhlung verfassungsmäßig verbriefter Grund- und Freiheitsrechte im Namen einer vermeintlichen Sicherheit vor Kriminalität, Terrorismus oder sonstigen, meist vor allem „gefühlten" Bedrohungen geht, kann der Freistaat Sachsen für sich eine unrühmliche Vorreiterrolle in Anspruch nehmen. So war beispielsweise das bundesweit bahnbrechende Pilotprojekt zur „Videoüberwachung von Kriminalitätsschwerpunkten" 1996 in Leipzig, genauer im Bereich des dortigen Hauptbahnhofs angesiedelt worden. Seitdem überwacht eine Vielzahl von Kameras die Innenstadt und den als Hochburg der autonomen Szene verschrienen Stadtteil Connewitz. Mit welchem Nutzen steht in den Sternen.

Auch in anderen deutschen Großstädten gehört die Kameraüberwachung des öffentlichen Raumes mittlerweile zum Alltag, obwohl die Wirksamkeit dieses Instruments der Kriminalitätsbekämpfung bislang durch keine wissenschaftliche Studie tatsächlich belegt werden konnte. Vielmehr geht die Wissenschaft davon aus, dass durch die Videoüberwachung Kriminalität an andere, nicht überwachte Orte verdrängt und ein gefährliches Gefühl der Scheinsicherheit erzeugt wird. Von den erheblichen Eingriffen in das Recht auf informationelle Selbstbestimmung und andere für die Funktionieren einer Demokratie essentiellen Grund- und Freiheitsrechten einmal ganz abgesehen.

Aber nicht nur am Boden wird in Sachsen überwacht und gefilmt, was das Zeug hält: 2008 führte Sachsen wiederum als erstes Bundesland ein Pilotprojekt polizeilicher Überwachungsdrohnen ein. Auch diese sind zwischenzeitlich bundesweit im Einsatz. Anders als in allen anderen Bundesländern, in denen sie nur bei besonders schweren Straftaten wie Mord zum Einsatz kommen, werden sie in Sachsen aber unter anderem auch zur Überwachung von Demonstrationen oder im Umfeld von risikobehafteten Fußballspielen eingesetzt.

Welche Demonstrationen die seit 1990 von der konservativen CDU geführte Landesregierung dabei besonders im Auge oder besser im Kameraobjektiv hat, macht ein Überwachungsskandal deutlich, der 2011 Sachsen in die bundesweiten Schlagzeilen brachte: Spätestens seit dem Jahr 2000 war der geschichtsrevisionistische, sogenannte „Trauermarsch" in Erinnerung an die Bombardierung des vermeintlich „unschuldigen" Dresdens am 13. Februar 1945 eine Großveranstaltung der radikalen deutschen und europäischen Rechten. Bis zu 6500 Neofaschisten nahmen alljährlich an ihm teil. 2010 gelang einem breiten antifaschistischen Bündnis erstmals die Verhinderung dieses Schaulaufens der deutschen und internationalen Rechten durch Gegendemonstrationen und Mitteln des zivilen Ungehorsams wie z. B. Sitzblockaden.

Dies, und nicht die jahrelange Instrumentalisierung des Gedenkens durch die radikale Rechte, war der konservativen Staatsregierung offenbar ein Dorn im Auge. Nicht anders ist es zu erklären, dass im Folgejahr schon im Vorfeld des 13. Februars staatliche Repressionen ungeahnten Ausmaßes einsetzten – nicht etwa gegen Rechts, sondern gegen die antifaschistischen Gegendemonstrationen. Im Zuge der Ermittlungen gegen eine ominöse, als „kriminelle Vereinigung" eingeschätzte „Antifa-Sportgruppe" – ein Phänomen, das sich später als Hirngespinst der Ermittlungsbehörden erweisen sollte – wurden unter anderem im Zuge einer sogenannten Funkzellenabfrage Verkehrsdaten mehrerer zehntausender Mobilfunkanschlüsse teilweise über Tage hinweg, im ganzen Stadtgebiet Dresdens überwacht. Diese Ermittlungen schlugen nach Bekanntwerden in ganz Deutschland hohe Wellen und wurden als „Dresdner Handygate" öffentlich breit skandalisiert.

Bei einer Funkzellenabfrage übermitteln die Telekommunikationsanbieter den Ermittlungsbehörden bekanntlich Daten, die im Einzugsgebiet eines Sendemast bzw. einer „Funkzelle" anfallen. So können Kommunikationsdaten („Verkehrsdaten") u. a. mit Ort, Uhrzeit und Datum der getätigten Anrufs sowie Rufnummern des Anrufers und des Angerufenen ermittelt werden. In seinem Urteil zur Vorratsdatenspeicherung vom 2.3.2010 hält das Bundesverfassungsgericht die weit reichenden datenschutzrechtlichen Implikationen dieses Verfahrens anschaulich fest:

„Die Aussagekraft dieser Daten ist weitreichend (…) Adressaten (…), Daten, Uhrzeit und Ort erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen derjenigen, deren Verbindungsdaten ausgewertet werden. (…) je nach Nutzung der Telekommunikation und künftig in zunehmender Dichte kann eine solche Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers ermöglichen"

Um einen Missbrauch dieser Ermittlungsmethode in solch Orewell´schen Ausmaßen zu verhindern, hat der Bundesgesetzgeber für ihren Einsatz eigentlich einen engen Rahmen abgesteckt. Nach § 100g Abs. 1 Satz 1 der Strafprozessordnung ist ihr Einsatz in der Regel nur gegen genau bestimmbare Personen zulässig, die im Verdacht stehen eine Straftat von erheblicher Bedeutung begangen zu haben. Nur wenn die Telefonnummer des Verdächtigen nicht bekannt ist, kann auch eine nicht-individualisierte Abfrage in Betracht gezogen werden. Der Einsatz der Funkzellenabfrage muss dann aber räumlich und zeitlich begrenzt und andere Ermittlungsansätze müssen aussichtslos bzw. zumindest wesentlich erschwert sein. Sie darf sich auch in diesem Fall nur gegen den Beschuldigten richten, wenn dessen Aufenthaltsort ungefähr bestimmbar ist. Ein Einsatz der Funkzellenabfrage, der einer Rasterfahndung gleichkommt, ist vom Gesetzgeber jedenfalls nicht vorgesehen. Im Gegenteil: Die Persönlichkeitsrechte Dritter sind beim Einsatz in Form einer Verhältnismäßigkeitsprüfung in Betracht zu ziehen und, wenn die Funkzellenabfrage nicht ohne deren erheblichen Verletzung eingesetzt werden kann, ist eigentlich auf deren Einsatz zu verzichten.

Eigentlich. Doch der Bundesgesetzgeber hatte die Rechnung ohne die inzwischen sprichwörtliche „Sächsische Demokratie" gemacht. In Dresden wurden im Februar 2011 die Kommunikationsdaten zehntausender Unverdächtiger im ganzen Stadtgebiet und teilweise über Tag hinweg ausgespäht. Weder war hierbei eine räumliche und zeitliche Eingrenzung, noch eine Verhältnismäßigkeitsprüfung zwischen den Ermittlungen gegen die vermeintliche „kriminelle Vereinigung" bzw. wegen des Vorwurf der erheblichen Straftat des Landfriedensbruch und eben den verfassungsmäßig geschützten Grund- und Freiheitsrechten der zehntausenden Unbeteiligten erkennbar. Das Dresdner „Handygate" ist ein Lehrstück dafür, welche die Demokratie gefährdende Eigendynamik Überwachungsmaßnahmen auch in einem demokratischen Rechtsstaat annehmen können und wie leicht die rechtlichen Schutzmechanismen, die die Rechte der Bürger schützen sollen, der Logik der Ermittlungsbehörden und dem politischen Willen der Machthaber geopfert werden.

Noch nicht einmal die von der Rechtsprechung angeregte nachträgliche Information der von den Überwachungsmaßnahmen Betroffenen wurde von den sächsischen Ermittlungsbehörden vorgenommen. Als der sächsische Datenschutzbeauftragte Andreas Schurig dies und allgemein das rechtlich fragwürdige Vorgehen von Justiz, Ermittlungsbehörden und Staatsregierung im September 2011 in einem Bericht zur „Handygate"-Affäre kritisierte, sah er sich massiven öffentlichen Angriffen von deren Vertretern ausgesetzt. Ihm wurde medial die Kompetenz und die Zuständigkeit abgesprochen, sich zu diesem Sachverhalt zu äußern. Er würde gegen die Prinzipien der Gewaltenteilung und der Unabhängigkeit der Justiz verstoßen. Es wurde sogar unverhohlen die Änderung besonders kritischer Passagen in dem Bericht des Datenschutzbeauftragten gefordert.

Dieses Beispiel zeigt deutlich die Uneinsichtigkeit, mit der hohe Vertreter von Staatsregierung, Justiz und Ermittlungsbehörden auf ihren offenkundigen Rechtsbruch im Fall der Dresdner Funkzellenabfrage reagieren. Auch die juristische Aufarbeitung des Skandals folgt diesem Muster: Zwar beurteilte das Landgericht Dresden 2013 in zweiter Instanz die Funkzellenabfrage als unrechtmäßig. Bei genauerer Betrachtung des Urteils wird jedoch deutlich, dass das Dresdner Gericht sich vor allem auf formelle Mängel bei der Begründung der Maßnahme stützt, sie inhaltlich hingegen für rechtlich vertretbar hält. Sprich: Auch das Landgericht will kein Problem bei der extensiven und damit unverhältnismäßigen Überwachung erkennen, die in Grundrechte zehntausender, auch gänzlich Unbeteiligter massiv eingreift. Sächsische Land- und Bundestagsabgeordnete von LINKEN und GRÜNEN sind daher vor das Bundesverfassungsgericht in Karlsruhe gegangen, wobei dessen abschließendes Urteil noch aussteht.

Die Funkzellenabfrage hat sich ungeachtet dessen zu einer Ermittlungsmethode entwickelt, die – nicht nur in Sachsen, sondern bundesweit - mit zunehmender Tendenz eingesetzt wird. Auch in diesem Fall bestätigt sich der Grundsatz: Was an Überwachungsinstrumenten in Sachsen erprobt und zuerst eingesetzt wird, ist ein paar Jahre später in ganz Deutschland etabliert.

Auch in einem aktuellen Fall scheint sich diese These zu bestätigen: Nach dem gescheiterten Anschlagsversuch des in Chemnitz lebenden Syrers Jaber Albakr im Oktober 2016 und dem Anschlag auf den Weihnachtsmarkt an der Gedächtniskirche im Dezember 2016 ist in Deutschland wieder einmal die Debatte um die Verschärfung von Überwachungsmaßnahmen im Zuge der Terrorabwehr entbrannt. Zu Beginn des Jahres 2017 hat der sächsische Innenminister Markus Ulbig, als einer der Ersten seines Metiers, seinen Willen be-

kräftigt, die schon seit einigen Jahren mögliche automatische elektronische KfZ-Kennzeichenerfassung auszuweiten und zu intensivieren. So soll, zusätzlich zu den bereits im Einsatz befindlichen sechs mobilen KfZ-Scannern, ein stationäres Gerät an der Autobahn A17 bei Pirna aufgestellt werden, das die Daten aller vorbeifahrender Kraftfahrzeuge verdachtsunabhängig erfassen soll. Weiterhin sollen diese Daten anders als bisher auch gespeichert werden und zusätzlich mit einer Software zur Gesichtserkennung der Fahrer bearbeitet werden können. Sogar die Erstellung von Bewegungsprofilen ist laut Medienberichten im sächsischen Innenressort im Gespräch.

Dass der dschihadistische Terrorismus dabei weniger Ursache, denn vielmehr scheinbar willkommener Anlass für die Ausweitung der Überwachung ist, zeigt der Fakt, dass die Intensivierung der Kennzeichenerfassung bereits nach der sächsischen Landtagswahl 2014 in den Koalitionsvertrag von CDU und SPD geschrieben wurde, die seitdem gemeinsam die Staatsregierung stellen. Diese Instrumentalisierung des Terrors und des – zu Recht oder Unrecht – gesunkenen Sicherheitsempfindens weiter Teile der Bevölkerung verkennt, welche Gefahren der Demokratie und dem Rechtsstaat aus eben diesen Überwachungsinstrumenten entstehen. Gerade Sachsen zeigt, wie schnell solche Instrumente auch in einem demokratischen Rechtsstaat gegen den staatlichen Machthabern politisch unliebsame Personen und, sozusagen als „Kollateralschaden“, auch gegen gänzlich Unbeteiligte unter Umgehung aller grundrechtlichen Schranken eingesetzt werden können. Sind solche Instrumente erst einmal vorhanden, die aufgrund des technischen Fortschritts eine Leistungsfähigkeit besitzen, wie Orwell sie in seinen kühnsten Phantasien sich nicht hätte ausdenken können, ist es bis zum „gläsernen Bürger“ nur noch ein kleiner Schritt. Mit dem „gläsernen“, seiner Grund- und Freiheitsrechte beraubten Bürger wäre aber auch die Demokratie und der Rechtsstaat am Ende, die die Apologeten der Überwachung, deren Avantgarde in den letzten Jahrzehnten häufig in Sachsen beheimatet war, im Name der Sicherheit vorgeben, verteidigen zu wollen.

Demonstration: Freiheit statt Angst 2013

Probleme der Rechtsstaatlichkeit im Antiterrorkampf

Frank Tempel, MdB

Der zentrale Begriff des Antiterrorkampfes der Sicherheitsbehörden ist der des „Gefährders". Fast ausschließlich wird er im Zusammenhang mit dem islamistischen Terror benutzt. Bei rechtsterroristischen Phänomenen taucht er nie auf.

Zunächst einmal lässt sich feststellen, dass der Begriff „Gefährder" nicht gesetzlich definiert ist. Es handelt sich also um eine weitgehend willkürliche Entscheidung, wann jemand als Gefährder eingestuft wird und wann nicht. Polizei und Geheimdienste nutzen ihn indes als Arbeitsbegriff bei der Bekämpfung terroristischer Gefahren sowie im Versammlungsrecht. Der Begriff erfüllt vor allem zwei Funktionen: Erstens sollen mit ihm Personen kenntlich gemacht werden, die anhand personenbezogener Merkmale oder Verhaltensweisen als Gefährder gelten, um diese in entsprechenden polizeilichen Verbunddateien sichtbar zu machen. Zweitens können aus der Einstufung als Gefährder gegen die entsprechende Person „präventive" und repressive Maßnahmen vorgenommen werden. In diesem Kontext ist der jüngste Vorstoß der Bayrischen Landesregierung zu verstehen, welche Gefährder für unbegrenzte Zeit in Haft nehmen lassen will.

Was ist nun ein Gefährder nach Ansicht von Bund und Ländern? Die gemeinsame Definition der Polizeien beider Ebenen lautet: *„Als Gefährder wird (…) eine Person bezeichnet, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie politisch motivierte Straftaten von erheblicher Bedeutung (…) begehen wird."* Voraussetzung ist also nicht das Vorliegen konkreter Anhaltspunkte für Straftaten, das ohnehin strafrechtliche Ermittlungen wie etwa bei der Vorbereitung einer schweren staatsgefährdenden Gewalttat nach sich ziehen dürfte.

Um wie viele Gefährder reden wir überhaupt? Die Zahlen aus dem islamistischen Spektrum sind in den letzten Jahren kontinuierlich gestiegen: Im November 2006 waren 72 Personen gespeichert. Im Dezember 2015 lag die Anzahl bereits bei 442. Die Hälfte der Gefährder hält sich zurzeit außerhalb Deutschlands auf. Bei etwas mehr als die Hälfte der Gefährder handelt es sich um deutsche Staatsangehörige. So weit bekannt, werden im Bereich des islamistischen Terrorismus verschiedene „Funktionstypen" definiert, die innerhalb der djihadistischen Netzwerke unterschiedliche Funktionen (als Leitungskader, Techniker, Agitatoren, Aktivisten, etc.) einnehmen.

Richtig ist, dass der Staat die Pflicht hat, seine Bürgerinnen und Bürger vor Gewalttaten zu schützen. Hierzu braucht er die nötigen Instrumente, um die entsprechenden Personen, die eine Gefahr darstellen, aufzuspüren und gegebenenfalls zu stoppen. Leitfrage ist aber, inwiefern das Datenregime und die damit verbundenen Eingriffe in das allgemeine Persönlichkeitsrecht verhältnismäßig und geeignet sind, um den Gefahren von Terrorismus zu begegnen. Hieran habe ich beträchtliche Zweifel.

Mittlerweile gibt es eine Vielzahl an Verbunddateien, in denen Personen aufgrund verschiedener kriminologischer Merkmale gespeichert werden. Sofern Daten aus einer Maßnahme für eine andere Angelegenheit genutzt werden sollen, hat das Bundesverfassungsgericht hierfür Leitlinien aufgestellt. Durch diese Leitlinien soll verhindert werden, dass die Polizei Erkenntnisse aus Ermittlungen zu schwerwiegenden Tatvorwürfen benutzt, um wesentlich kleinere Delikte in einem ganz anderen Bereich zu verfolgen. Beispielsweise hat das Bundesverfassungsgericht vollkommen ausgeschlossen, dass Erkenntnisse aus einer optischen Wohnraumüberwachung oder einer Online-Durchsuchung, die nur im Rahmen der Gefahrenabwehr durchgeführt werden darf, in einem anderen strafrechtlichen Ermittlungsverfahren weitergenutzt werden dürfen. Allerdings hat das Gericht den Sicherheitsbehörden einige Schlupflöcher gelassen: Als Spurenansatz darf die Polizei die im Rahmen einer schwerwiegenden Straftat gesammelten Erkenntnisse insofern nutzen, als dass sie die Erkenntnisse nicht ignorieren muss. So kann beispielsweise dann die Übermittlung von Daten möglich sein, um vergleichende Rechtsgüter zu schützen.

Diese Schlupflöcher werden von der Bundesregierung nun weidlich genutzt. Die Bundesregierung nimmt nicht etwa eine grundrechtsfreundliche Novellierung der Speicher- und Datenaustauschpraxen vor, sondern schrammt mit Vollgas immer weiter an den verfassungsrechtlichen Leitplanken entlang. So setzt die Bundesregierung konsequent den

Schutz individueller Rechtsgüter wie etwa den Schutz von Leib, Leben und Freiheit mit abstrakten Rechtsgütern wie dem Schutz des Staates gleich. Das führt dazu, dass schon die Durchsetzung aufenthaltsrechtlicher Maßnahmen als Schutzgut gezählt wird, um eine Datenübermittlung zwischen den Verbunddateien zu rechtfertigen.

Neben dem Ausbau des Datenregimes setzt die Bundesregierung einseitig auf eine Strafrechtsverschärfung. Hierbei verletzt die Bundesregierung das Prinzip der Verhältnismäßigkeit. So stehen das Reisen und der Versuch des Reisens in terroristischer Absicht bereits unter Strafe. Mit diesem Tatbestand legitimieren Polizei und Geheimdienste weitreichende Überwachungsmaßnahmen wie zum Beispiel die heimliche Telekommunikationsüberwachung, die Online-Durchsuchung und das Abhören der Wohnung.

Außerdem soll mit einem neuen Tatbestand der Terrorismusfinanzierung der Forderung der Financial Action Task Force (FATF) Rechnung getragen werden, ein bei der OSZE angesiedelten Gremiums. Allerdings ist bereits nach jetzigem Strafrecht das Geldsammeln und Geldspenden zur Vorbereitung einer staatsgefährdenden Gewalttat strafbar (§ 89a Abs. 4 Nr. 2). Als Auffangtatbestand ist zudem die Terrorfinanzierung als Unterstützung einer terroristischen Vereinigung von §§ 129a Abs. 5, 129b StGB – auch unabhängig von einer Erheblichkeit oder konkreten Gewalttat – erfasst. Über diesen Tatbestand kann zudem das Reisen in terroristischer Absicht begegnen werden. Auch der Versuch des Reisens kann als Beihilfe einer terroristischen Vereinigung schon heute strafrechtlich belangt werden, schließlich dürften sich bis zum Versuch der Ausreise die betroffenen Personen durch die Kontaktaufnahme mit den entsprechenden Organisationen strafbar gemacht haben.

Auch weitere Maßnahmen wie die elektronische Aufenthaltsüberwachung („elektronisch Fußfessel“) haben wir als LINKE stets abgelehnt, da sie ein eklatanter Eingriff in die informationelle Selbstbestimmung und in die Privatsphäre der Betroffenen bedeutet. Entweder eine Person bietet so klare Anhaltspunkte für die baldige Begehung einer Straftat, dass sie ohnehin rund um die Uhr überwacht werden muss oder eine Person erhält „lediglich“ eine Fußfessel, dann kann sie mit dieser am Fuß jedoch ebenfalls erheblichen Schaden anrichten. Der strafbewehrte Verstoß gegen Aufenthaltsverbote, der durch die Fußfessel dann noch festgestellt werden kann, wird hingegen nicht bei der Bewertung der Verhältnismäßigkeit ins Gewicht fallen. Im Übrigen hätte eine Fußfessel wohl auch den Anschlag von Anis Amri nicht verhindert, dessen Fall nun als Begründung für die Fußfessel herhalten muss. Die Sicherheitsbehörden hielten einen Anschlag durch Amri für wenig wahrscheinlich – es handelt sich also um eine eklatante Fehleinschätzung der Behörden, trotz entsprechender Hinweise anderer Geheimdienste.
Neben der Verhältnismäßigkeit stellt sich selbstredend die Frage nach der Geeignetheit der strafrechtlichen Verschärfungen und der Eingriffe in die Privatsphäre durch die Überwachungsmaßnahmen: Inwiefern sind die Methoden hilfreich, um dem legitimen Ziel, den Zufluss djihadistischer Kämpferinnen und Kämpfer in den Irak, Syrien und in andere Konfliktregionen zu unterbinden, auch tatsächlich gerecht wird? Der bereits sehr weite Regelungszugriff des geltenden deutschen Terrorismusstrafrechts spricht dafür, dass das eigentliche Problem nicht im Bestehen vermeintlicher Strafbarkeitslücken liegt, sondern vielmehr in den praktischen Schwierigkeiten der Identifikation gewaltbereiter Terroristen und dem Nachweis der Absicht, zum Zweck der Begehung, Vorbereitung oder Unterstützung terroristischer Taten ins Ausland reisen zu wollen. Diesem Problem kann man mit noch schärferen strafrechtlichen Regelungen nicht begegnen. Symbolische Gesetzgebung verhindert keine Anschläge, beschädigt aber den Rechtsstaat. Es kann allenfalls mit mehr und qualifiziertem Sicherheitspersonal und besserer internationaler Zusammenarbeit angegangen werden – und langfristig primär durch Prävention im Sozial- und Jugendbereich.

Das Bataclan in Paris, Frankreich

Frankreich im andauernden Notstand

Marie-Christine Vergiat, MdEP

Der Notstand wurde in Frankreich am 14. November 2015 ausgerufen, dem Tag nach den Anschlägen von Paris. Seitdem wurde er regelmäßig verlängert, ohne dass seine Wirksamkeit je bewiesen worden wäre. Vor allem ging es darum, die Öffentlichkeit zu beruhigen, hatten die Attentate doch nur wenige Wochen vor der Pariser Klimakonferenz stattgefunden.

Die Attentate vom 13. November 2015 forderten 130 Todesopfer, davon 90 im mythenhaften Saal des Bataclan. Es waren vor allem junge Menschen, die zum Konzert der amerikanischen Rockgruppe "Eagles of Death Metal" dorthin gekommen waren. Während der darauf folgenden Stunden und Tage war ein großer Teil der Franzosen wie gelähmt, um so mehr als dass diese Attentate einige Monate nach denjenigen des Januar desselben Jahres verübt wurden, die 17 Menschen das Leben kosteten, 12 davon bei der Belagerung des Satirejournals "Charlie Hebdo".

Für die französischen Behörden galt es folglich, schnell und bestimmt zu handeln. Anders als im Januar, wo eine Art quasi-religiöser nationaler Einklang zelebriert wurde, mit dem Höhepunkt bei der Demonstration vom 11. Januar, an der Staats- und Regierungschefs der ganzen Welt teilnahmen, kam es im November eher zu einer Art gegenseitigem Überbieten, von dem sich auch der Präsident der Republik nicht ausnahm. Vor dem Congrès, der außerordentlichen Versammlung der beiden Kammern des französischen Senats aus Assemblée nationale und Sénat, verkündete er, "den Krieg gegen den Terrorismus", "einen Krieg einer anderen Art gegen einen neuen Feind, der einen Verfassungsrahmen erfordert, mit dem sich durch die Krise steuern lässt" führen zu wollen. "Ein Werkzeug, geeignet um darauf für eine bestimmte Zeit Maßnahmen zu gründen, ohne auf den Belagerungszustand zurückgreifen zu müssen", "ohne die öffentlichen Freiheiten zu gefährden", wagte er hinzu zu fügen. Es ist ihm Rahmen dieses Diskurses, dass er den Entzug der Staatsbürgerschaft für Urheber von Terrorakten forderte.

Der Notstand wurde für 12 Tage durch ein präsidentielles Dekret eingerichtet, das bei einer Krisensitzung des Kabinetts in der Nacht vom 13. auf den 14. November angenommen worden war. Seitdem wurde er zunächst mit einem Gesetz vom 20. November 2015 um 3 Monate verlängert, und danach wieder in mehreren Schritten, derzeit bis Juli 2017. François Hollande musste freilich die Idee aufgeben, den Notstand in die Verfassung zu schreiben, genauso wie die Idee mit dem Entzug der Staatsbürgerschaft. Letztere hatte einen Aufschrei verursacht, einschließlich in den Reihen der Sozialisten, selbst innerhalb der Regierung.

Frankreich hat leider eine lange Tradition von Ausnahmegesetzen. Der Rahmen für den Notstand war 1955 entworfen worden, um auf die ersten Attentate algerischer Unabhängigkeitskämpfer, damit den Beginn des Algerienkrieges, zu reagieren. Er wurde damals mehrmals eingesetzt, immer im selben Zusammenhang. Bei drei weiteren Malen wurde er in den Überseegebieten eingesetzt, für relativ kurze Zeiträume zwischen einem Tag und einigen Monaten in den Jahren 1985,1986 und 1987. In allen diesen Fällen lag vor, was die Juristen "Zeiten von Aufständen" nennen. Jüngst wurde der Notstand im November 2005 in der Ile-de-France und einigen weiteren Städten umgesetzt, wobei die Anwendung, es ging um die Krawalle von Jugendlichen in den Banlieues, deutlich fragwürdiger war. Er dauerte weniger als 2 Monate. Der damalige Präsident der Republik, Jacques Chirac, beendete den Notzustand am 3. Januar 2006 mit der Feststellung, dass das Instrument ungeeignet sei.

Der Notzustand von 2015 wurde unter völlig anderen Voraussetzungen eingerichtet, ist es doch das erste mal, dass er im Zusammenhang mit dem Kampf gegen Terrorismus eingesetzt wird. Gleichwohl war in der Vergangenheit Frankreich schon öfter Ziel von Anschlägen geworden, bei Anschlagswellen die das gesamte europäische Territorium betrafen.

Er gibt den Verwaltungsbehörden außerordentliche Mittel an die Hand, die vom gemeinen Recht abweichen und außerhalb der richterlichen Kontrolle stehen, oder diese nur im Nachhinein erlauben.

Das Gesetz vom 20. November 2015 hat nicht nur eine erstes Mal die Dauer des Notstands verlängert, sondern auch tiefgreifende Änderungen in das Gesetz von 1955 eingefügt,

um “die Effektivität seiner Vorgaben zu verstärken”. Mit Ausnahme der Pressefreiheit, die glücklicherweise von den französischen Abgeordneten gerettet wurde, wurden die Einschränkungen der Grundrechte weitgehen beibehalten: verschärfter Hausarrest, Hausdurchsuchungen bei Tag und Nacht, Zugriff auf Daten, Auflösung von Versammlungen… Schlimmer noch, das neue Gesetz erlaubt es, dass seinen Maßnahmen, die in die Freiheiten eingreifen, auch Personen unterworfen werden können, von denen man “ernstzunehmende Gründe hat anzunehmen, dass das Verhalten eine Gefahr für die Sicherheit darstellt”. Das zielt nicht nur auf Personen mit strafbaren Aktivitäten, sondern auf Personen, die in den Augen der Polizei verdächtig sind, solche zu begehen. Dies ist Präventivjustiz, ausgeübt durch die Polizei, auf der Grundlage von Verdächtigungen.

Darüber hinaus muss unterstrichen werden, dass seit den Attentaten von 1986 in Frankreich mehr als 30 Gesetzestexte zum Kampf gegen Terrorismus angenommen wurden, von denen jeder seinen Anteil an Ausnahmeregelungen und Freiheitsbeschränkungen mitgebracht hat, während eine Vielzahl von Beobachtern, und insbesondere von Richtern, die Einschätzung vertreten hat, dass den französischen Behörden alle Werkzeuge zur Verfügung stünden, um auf diesem Gebiet zu agieren ohne den Notzustand ausrufen zu müssen.

Das besonders intrusive Geheimdienstgesetz vom 24. Juli 2015 ist eines der jüngsten Beispiele. Sein ausgewiesenes Ziel war es, die den französischen Geheimdiensten zur Verfügung stehenden Mittel zu verstärken, um “langjährige illegale Vorgänge, die von keinem rechtlichen Rahmen gedeckt waren, zu legalisieren”, mit der Begründung, dass es besser sei, wenn besagte Dienste in einem “legalen” Rahmen agieren könnten. Das ganze ist ein Betrug am Rechtsstaat. Das Gesetz erlaubt demnach eine massenhafte Sammlung von Daten, vor allem von Internet- und Telefonverbindungen, praktisch ohne Kontrolle. Wenn man sich erinnert, wie die NSA-Affäre angeprangert wurde, dann kann man sich nur wundern, wenn man sieht wie die französischen Behörden Maßnahmen mit denselben Zielen legalisieren.

Seitdem hat noch das großenteils vor den Novemberattentaten entworfene Gesetz vom 3. Juni 2016, dem Namen nach zur Verstärkung des Kampfes gegen organisierte Kriminalität, den Terrorismus und seine Finanzierung, die Strafprozessordnung reformiert, “um diese an außergewöhnliche Situationen anzupassen”. Dieser Text wurde als notwendig vorgestellt, um eine Reihe von Maßnahmen, die im Rahmen des Notstands beschlossen worden waren, in das gemeine Recht zu überführen. Unter anderem sieht es eine 30 jährige Sicherheitshaft vor, die nicht reduziert werden kann, ohne jedwede Möglichkeit zur Haftersparnis, sowie einen Straftatbestand für regelmäßiges Besuchen terroristischer Websites, der 2 Jahre Freiheitsentzug nach sich ziehen kann. Die französische Gesetzgebung auf dem Gebiet der Terrorbekämpfung ist damit selbst ohne den Notstand die repressivste in Europa geworden.

Heute sind also die wesentlichen Maßnahmen des Ausnahmezustandes im normalen Recht umgesetzt worden und machen damit jede weitere Verlängerung gänzlich nutzlos. Selbst die Abgeordneten, die ihn nochmals bis zum Juli 2017 verlängert hatten, haben dies erkannt und geurteilt, dass dieser zu nichts mehr großartig gut wäre, nur findet sich so kurz vor den anstehenden Wahlen niemand, um die Sache in die Hand zu nehmen und den Notstand aufzuhalten.

Der Notstand ist nur ein Vorwand, eine Maske, die die freiheitsbedrohenden Auswüchse legitimiert, die in Frankreich immer schlimmer werden. Selbst in dem Zeitraum, als er am meisten legitim schien, ist die Bilanz bezeichnend für den Grad an Relevanz und Angemessenheit: von den 3000 Hausdurchsuchungen, die zwischen dem 13. November 2015 und dem 8. Januar 2016 stattgefunden haben, ist nur eine einzige in einer Untersuchung in Verbindung mit Terrorismus gemündet.

Dem Gegenüber stehen die zahlreichen willkürlichen Verhaftungen und Hausarreste insbesondere von Klimaaktivisten während des COP 21 Treffens. Das gleiche dann wieder bei den Protesten gegen das geplante “Arbeits”-Gesetz im Frühjahr 2016 und dann noch einmal im Zusammenhang mit dem Kampf gegen die irreguläre Einwanderung.

Muslime, und Menschen, die insbesondere aufgrund ihres Familiennamens für solche gehalten werden, haben ganz besonders für diese diskriminierende Unterdrückung herhalten müssen. Die Maßnahmen haben sich insbesondere auf ärmere Stadtteile gerichtet, wo es ohnehin schon starke Gefühle von Abgehängtsein gab, und haben sich dort zu den bereits erfahrenen Diskriminierungen hinzu addiert, woraus sich in einer höllischen Spirale die Islamophobie nährt. Zudem ist der Ausnahmezustand ungeeignet für den Kampf, den er vorgibt zu führen, denn die “Dschihadisten” entziehen sich jeder Raum-Zeit-Logik: Sie wollen nicht diesen oder jenen Teil Frankreichs kontrollieren. Dagegen benutzen sie alles, was diskriminiert, um ihre Propaganda und ihre Rekrutierung zu füttern. Es ist deshalb Kontraproduktiv, den Notstand beizubehalten. In Wirklichkeit zielt er nur darauf ab, die Franzosen in Sicherheit zu wiegen, wenn man bedenkt dass die Ausnahmeregelungen, die er erlaubt, genauso freiheitsbedrohend wie ineffizient sind.

Ausnahmeregelungen müssen von ihrer Natur her Ausnahmen sein, aber im Zusammenhang mit dem Kampf gegen den Terrorismus scheint die Vernunft an Land zu verlieren. Emotionen, oder besser, das Benutzen von Emotionen erlaubt all diese Auswüchse. Alles scheint richtig Angesichts einer unmittelbaren und ungreifbaren Bedrohung, die jederzeit zuschlagen kann. Man gewöhnt schrittweise die Bevölkerung an ein Ausnahmeregime, an allgegenwärtige Polizeipräsenz bis hin zu schwerem Militär.

Es ist immer schwieriger geworden gehört zu werden, wenn man die Prinzipien eines Rechtsstaats in Erinnerung ruft, nach denen Freiheitsbeschränkungen zwar möglich sind, aber nur wenn sie vorläufig sind, dem angestrebten Ziel angemessen, durch bestehende Gegebenheiten begründet und von absoluter Notwendigkeit. Nur wenige Abgeordnete haben es gewagt, sich dem Notstand zu widersetzen, seiner Verlängerung und den Einschränkungen der Freiheit, die damit kommen.

Trotzdem, diese Prinzipien aufzugeben ist gleichbedeutend damit, denjenigen Recht zu geben, die man vorgibt zu bekämpfen und sich daran zu hindern, sie wirklich zurückzudrängen, während wir doch “auf den Terror mit mehr Demokratie, mehr Offenheit und Toleranz antworten” müssten, wie es der norwegische Premierminister nach den Attentaten 2011 so gut gesagt hat.

Radome des Bundesnachrichtendienstes in Bad Aibling (Schutzhülle, Radarkuppel)

Terrorismus bekämpfen, Grundrechte wahren!

Zu sicherheitspolitischen Positionen der LINKEN. im Europaparlament

Dr. Cornelia Ernst, MdEP und Lorenz Krämer

1. Das Spiel mit der Angst muss aufhören!

Die letzten Jahre haben viele Menschen verstört. Die Anschläge in Brüssel, Istanbul, Nizza, Ansbach, Berlin und jüngst in St. Petersburg und Stockholm haben starke Emotionen ausgelöst. Den Opfern und ihren Angehörigen gilt unsere ehrliche Verbundenheit und Solidarität. Die Anschläge fallen in eine Zeit großer Verunsicherung, in der viel Bestehendes in Frage gestellt wird, bisher weithin akzeptierte Werte wie Gemeinsinn und Mitgefühl ins Wanken geraten sind. Ein Gefühl von Machtlosigkeit und die Furcht vor dem Unbeherrschbaren ermöglichen es populistischen Kräften, auf überkommene, restriktive, national definierte Vorstellungen von Gesellschaft zurück zu greifen. Aber das Spiel mit der Angst ist längst auch in der Mitte angekommen. Wer heutzutage die meisten Regierungspolitiker*innen über Terrorismus reden hört, muss den Eindruck bekommen als lebten wir in einer Situation einer nie dagewesenen Bedrohung unseres Zusammenlebens durch islamistischen Terrorismus. Der Ruf nach innerer Sicherheit, nach Stabilität, aber auch der nach einer Wahrung des Bestehenden wird von den politischen Eliten der EU und der Mitgliedsstaaten auf die erste Forderung verkürzt. Das ist ein gravierender Fehler, der sich auch in der offensiv angekündigten Sicherheitsunion von Rat und Kommission zeigt, für die es noch nicht mal eine ordentliche vertragliche Grundlage gibt.

Zwar ist es richtig, dass seit einigen Jahren die Anzahl von Opfern terroristischer Anschläge wieder steigt, allerdings sind von dieser Entwicklung in erster Linie Länder wie Afghanistan und Irak betroffen. So waren die Zahlen in Europa trotz der großen Anschläge in Madrid 2004 und London 2006 kontinuierlich gefallen, und haben auch heute das Niveau aus früheren Hochphasen, wie in den 70er und 80er Jahren des letzten Jahrhunderts, bei weitem nicht erreicht. Dennoch ist das Unsicherheitsgefühl bei vielen Menschen erheblich angestiegen, weil das Ausmaß der terroristischen Bedrohung unklar ist.

Diese Unklarheit wird auch gefördert, indem gleichzeitig auch eine Anti-Terror-Gesetzgebung in Stellung gebracht wird, um unliebsame Proteste zu kriminalisieren, wie im Fall von Dresden Nazifrei, der Nuit Debout Bewegung in Frankreich und jüngst der „11 von Röszke“ in Ungarn, jenem Dorf an der serbischen Grenze, wo Orban 2015 einen Zaun errichten ließ. Unter ihnen befindet sich der Asylbewerber Ahmed H., der zu 10 Jahren Haft verurteilt wurde, ohne dass man ihm irgendeine ernsthafte Gewalttat, geschweige denn terroristische Handlungen hätte nachweisen können.[1] Ein wachsendes Problem ist daher auch der oft undifferenzierte und missbräuchliche Umgang mit dem Begriff Terrorismus. Diese Verunsicherung ist nicht zuletzt auch geschuldet dem oftmals undifferenzierten Umgang mit dem Begriff Terrorismus.

So sehr die Suche nach Halt und einfachen und schnellen Lösungen in einer sich ständig wandelnden Welt verständlich ist, so sehr ist sie jedoch Illusion. Pauschalisierung, Stigmatisierung und Ausgrenzung sind die logische Folge und lassen keinen Raum für Differenzierung. In dieser Hoch-Zeit für rechte Populist*innen und Rechtsextreme leben Rassismus, Nationalismus und Chauvinismus auf, als seien diese Monster aus ihrem Schlaf wieder erwacht.

Es ist wichtig festzustellen, dass es nur bis zu einem gewissen Grad möglich ist, Terroranschläge nicht nur im Nachhinein strafrechtlich aufzurollen, sondern sie mit Hilfe von Polizei und Geheimdiensten zu verhindern. Noch wichtiger ist es zu verstehen, wie Menschen überhaupt zu der Bereitschaft kommen, grausame Anschläge zu verüben, und wie darauf reagiert werden kann. Aus diesem Grund darf die Bekämpfung von Terrorismus nicht allein durch Repression zu stattfinden, sondern muss als gesellschaftliche Herausforderung verstanden werden. Dafür müssen wir in eine Reihe von Maßnahmen investieren, die über die Rolle von Polizei und Justiz hinausgehen.

[1] https://www.amnesty.org/en/latest/campaigns/2017/01/dangerously-disproportionate/

Tausende Vorschläge und Konzepte schießen zurzeit wie Pilze aus dem Boden, ohne dass jemals sachlich überprüft würde, was sie wirklich bewirken können und was sie wirklich nützen. Den Bürger*innen wird damit eine Sicherheit vorgegaukelt, die es gar nicht gibt. Der ständige Ruf der Innenminister nach Kompetenzerweiterung des Staates führt dazu, dass immer mehr Unsicherheit erzeugt wird. Diese Forderung nach vermeintlicher Sicherheit geht nicht einher mit einem reflektierten Denken, das Sicherheit und die damit verbundenen Maßnahmen immer wieder kritisch hinterfragt. Ein bisher nirgendwo sachlich definiertes Recht auf Sicherheit wird anderen Rechtsgütern, wie Gerechtigkeit, Gleichbehandlung, Privatsphäre, Mobilität, freie Meinungsäußerung mehr und mehr übergeordnet.

So werden die Ängste und Sorgen der Bürger*innen ausgenutzt, und die nationale Sicherheit, die gar keinem Gemeinschaftsrecht der EU unterliegt, mit so genannter innerer oder öffentlicher Sicherheit vermischt. Alles scheint plötzlich „Sicherheit" zu sein, Sicherheit als Suprarecht, wie es einst Innenminister Friedrich auf den Punkt brachte. Diese Unklarheit schafft Grauzonen, die in Wirklichkeit Spielräume für „Sicherheitsexpert*innen" aller Art sind genauso wie für die Sicherheitsindustrie, die jede zusätzliche Überwachungsmaßnahme zum Heilsmittel erklärt, so lange sie kraftvoll daran verdient.

Sicherheit ist nach Lesart der LINKEN deutlich mehr als der vorgegaukelte Schutz vor terroristischen Gefahren. Sie heißt auch sich frei bewegen zu können im öffentlichen Raum, sich eines handelnden Rechtsstaates und der eigenen Rechte sicher sein zu können. Es geht dabei um Rechte wie den Schutz der Privatsphäre, den Schutzes vor Gewalt und Missbrauch, und nicht zuletzt soziale Rechtsgüter.

Daher fordern wir auf europäischer Ebene, die Relevanz und Wirksamkeit aller bestehenden Sicherheitsinstrumente und Konzepte zu prüfen. Wir brauchen eine Evaluation der bestehenden Maßnahmen durch unabhängige Sachverständige, bevor wieder neue Instrumente hektisch eingeführt werden; wir brauchen einen Leitfaden zur Prüfung der Sicherheitsmaßnahmen und die Ergebnisse müssen öffentlich sein. Sicherheitspolitik muss aus der politischen Grauzone heraus und der demokratischen Kontrolle unterzogen werden. Gleichsam gilt es, die Balance zwischen Sicherheit und anderen rechtsstaatlichen Grundwerten strikt zu wahren. Nur so kann ein Sicherheits- und Überwachungsstaat verhindert werden, der sich über die Grundrechte der Bürger*innen stellt. Vor allem aber benötigen wir einen seriösen Umgang mit dem Terrorismusbegriff.

2. Massenüberwachung und Pauschalverdächtigungen der Bürger beenden!

In den letzten Jahren wurde der Glaube genährt, viel hilft viel. Ein ums andere Mal wurden im Namen der Terrorismusbekämpfung und der inneren Sicherheit neue Systeme zur Sammlung und Speicherung von Massendaten geschaffen. Daten der Massenüberwachung stehen schon lange nicht mehr nur den Geheimdiensten zur Verfügung. Über Europol, Vorratsdatenspeicherung und Fluggastdatenspeicherung sowie eine Vielzahl weiterer nationaler Projekte haben die europäischen Polizeibehörden Zugang zu einer riesigen Menge privater Daten. Bis heute gibt es keinerlei Evaluierung, obwohl wiederholt vom Europaparlament gefordert, in Resolutionen wie in Gesetzestexten. Der rote Faden für eine effiziente und gezielte Verfolgung terroristischer Straftaten ist im Wust ständig neuer Maßnahmen und Instrumente verloren gegangen.

Stattdessen entstand ein unüberschaubares Ausmaß an Überwachung der Bürger*innen. Der/die Bürger/*in als Verdachtsobjekt kehrt das rechtsstaatliche Verhältnis von Bürger*innen und Staat um. Und es gibt noch eine zweifelhafte Folge dieser Politik: der Verlust einer der wichtigsten Werte der EU, der Freizügigkeit ihrer Menschen. Mit der gegenwärtigen Grenzpolitik wird ihr Selbstverständnis als Raum der Freiheit, der Sicherheit und des Rechts sukzessive abgeschafft.

Mit Hilfe dieser Daten lassen sich vielfältige Rückschlüsse auf das Privatleben der Menschen in Europa ziehen, wann wir uns wo für wie lange aufgehalten haben, mit wem wir über Telefon und Email in Kontakt stehen. Aber es geht nicht nur darum, vergangenes Verhalten zu speichern. Massenüberwachungsdaten werden genutzt, um Profile zu bilden, um bestimmtes Verhalten und bestimmte Gewohnheiten in virtuelle Schubladen einsortieren zu können. So sucht man nach Mustern im Verhalten der Menschen, nach Auffälligkeiten, die auf vergangene, gegenwärtige und vor allem zukünftige Straftaten Hinweise geben sollen (Profiling).

Wir fordern das Ende dieser pauschalen Datensammlungen. Wir fordern die Kehrtwende hin zu einem Ansatz, der wieder mehr Wert legt auf konkrete Fälle und menschliche Prüfung. Gezielte Überwachungsmaßnahmen sollen nach richterlicher Prüfung möglich sein. Auf europäischer Ebene existieren bereits diverse Instrumente zum Austausch solcher gezielter Erkenntnisse, eine sachliche Bewertung ihres Nutzens und ihrer Probleme steht aber auch hier aus.

Wir wenden uns klar gegen alle Forderungen, die Hintertüren in Kommunikationssoftware oder Beschränkungen für Verschlüsselungstechnik verlangen. Mit der Zunahme von verschlüsselter Kommunikation in den letzten Jahren wird oft das Argument des „going dark" vorgebracht, dass die Überwachungsinstrumente wertlos würden, weil zu viel verschlüsselt würde. Aber erstens lassen sich die Metadaten, also wer mit wem wann kommuniziert hat, nicht verschlüsseln, und zweitens bedeutet eine Schwächung von Verschlüsselung einen Verlust an Sicherheit. Schwachstellen stünden ja nicht nur den Behörden zur Verfügung, sie könnten ebenso gut von Kriminellen gefunden und ausgenutzt werden. Dasselbe gilt für den Einsatz von Viren und Trojaner, die ebenso schnell in falsche Hände gelangen können. Viren, Hintertüren oder gar ein Verbot verschlüsselter Nachrichtendienste bedeutet, das Kind mit dem Bade auszuschütten.

Der logische Ausweg ist es, von der Massenüberwachung abzukehren. Statt unterschiedsloser Massenüberwachung fordern wir die gezielte Überwachung von Verdächtigen, aufgrund vorheriger richterlicher Anordnung, um die Rechte von Betroffenen angemessen berücksichtigen zu können. Die gezielte Überwachung von Endgeräten von Verdächtigen, wie zum Beispiel Smartphones ermöglicht das Umgehen von Verschlüsselung, ohne diese zu schwächen oder zu knacken, stattdessen können auch heute noch einzelne Geräte verwanzt und Informationen direkt an Mikrofon oder Kamera der Geräte abgegriffen werden. Dabei müssen Reichweite, Umfang und Zweck der Maßnahmen klar und begrenzt sein, und in jedem Fall Einzelfälle betreffen. Dies ist nur dann sichergestellt, wenn sich rechtliche Vorgaben sich in den Funktionen der dazu verwendeten Software widerspiegeln. Dazu muss der Quellcode der Software nicht nur den Behörden, sondern auch ihren Kontrollgremien und Einrichtungen wie dem BSI zur Verfügung gestellt werden. Die Verwendung von Software, deren Quellcode nicht zur Prüfung zur Verfügung steht, lehnen wir für alle Grundrechtseingriffe grundsätzlich ab.

3. Statt mehr Macht den Geheimdiensten bessere Begrenzung ihrer Tätigkeit und demokratische Aufsicht!

In den vergangenen zwei Jahrzehnten sind die Geheimdienste nicht nur in Deutschland zunehmend stärker in die Sicherheitsarchitektur einbezogen worden. Diese Entwicklung ging einher mit massiven Investitionen in Systeme zur elektronischen Massenausspähung und deren rechtlicher Ausweitung.

Dies hat zu einer massenhaften Verletzung der Grundrechte von über einer Milliarde Menschen geführt. Die daraus gewonnenen vermeintlichen Erkenntnisse sind einerseits zu viele und andererseits von zu geringer Aussagekraft um einen wirklichen Nutzen zu haben. Einer der negativen Nebeneffekte von Massenüberwachung ist die große Fülle von Daten von unzuverlässiger Qualität.

Zwar waren viele der Attentäter*innen der vergangenen Jahre in Europa den Geheimdiensten bekannt, doch hatte dies keinen erkennbaren Nutzen. Zugleich entziehen sich die Geheimdienste quasi überall der Kontrolle durch die Öffentlichkeit, die Parlamente und regelmäßig auch ihrer eigenen Regierungen.

Die Anschläge der jüngsten Vergangenheit haben gezeigt, dass auch die Geheimdienste in der Terrorabwehr vollständig versagt haben. In Deutschland wurde dies am deutlichsten bei der Aufklärung der NSU-Morde. DIE LINKE. kritisiert seit langem das Agieren von Geheimdiensten. Ein Blick in den Abschlussbericht der Untersuchung des Innenausschusses des Europaparlaments zur Massenüberwachung durch die NSA von 2014 zeigt, dass die Schlussfolgerungen bis heute nicht einmal im Ansatz realisiert wurden, weder in den Mitgliedsstaaten, noch auf europäischer und internationaler Ebene. Weder wurden Transparenz und bessere Kontrollstrukturen geschaffen, die Massenüberwachung wurde nicht beendet und ihr Nutzen keiner öffentlich nachvollziehbaren sachlichen Prüfung unterzogen. Letztlich handeln die Geheimdienste wie ein „Staat im Staate", unkontrollierbar, und wie zahlreiche Beispiele immer wieder zeigen, auch an den Gesetzen vorbei.

Wir als Linke im Europaparlament lehnen die Erweiterung der Rechte und Befugnisse von Geheimdiensten strikt ab. Solange Geheimdienste existieren, ist unser vordringliches Ziel, die hemmungslose Überwachung und Ausspähung der Bürger*innen durch die Geheimdienste zu beenden. Ihre Rolle im Sicherheitskonzept muss zurückgedreht werden. Wir fordern, dass ihre demokratische Aufsicht durch parlamentarische Gremien gestärkt wird und unabhängige Kontrollinstanzen, die mit Expert*innen zu besetzen sind, geschaffen werden. Zugleich lehnen wir es ab, dass ein europäischer Geheimdienst geschaffen wird. Wir wenden uns ebenso dagegen, dass Forschungsprojekte von Geheimdiensten mit der Hilfe von EU-Mitteln finanziert werden, insbesondere wenn dies über Tarnfirmen und ähnliches geschieht.

Wir fordern ein Ende der elektronischen Massenüberwachung. Die Arbeit der Geheimdienste muss sich im Rahmen des Kampfes gegen den Terrorismus auf die Voraufklärung gefährlicher Strukturen beschränken. Dabei muss klar und

kontrollierbar sein, dass die Zuständigkeit an die Polizeibehörden übergeht, sobald Anzeichen konkreter Gefahren erkennbar werden. Die V-Mann-Tätigkeit oder Unterstützung gefährlicher Gruppierungen muss tabu sein. Genauso wenig soll es einen regulären und pauschalen Zugriff auf die europäischen Datenbanken für Geheimdienste geben.

4. Statt Massenüberwachung und Pauschalverdächtigungen gezielte Gefahrenabwehr

Die gesamte Geschichte der jüngsten Anschläge in Europa seit dem Januar 2015 ist leider auch eine Geschichte von Polizeibehörden, die bestenfalls willens, aber letztlich außerstande waren, in die Anschläge in geeigneter Weise einzugreifen. Am deutlichsten war dies in Paris im November 2015, und der gesamten Zeit bis weit nach den Brüsseler Anschlägen. Praktisch alle großen Anschläge in der EU seit der Attacke auf Charlie Hebdo im Januar 2015 wurden von Täter*innen verübt, die in einem, meist aber in mehreren EU-Ländern als mögliche Terroristen eingestuft worden waren. Amri, der Attentäter von Berlin, war sogar erst als verdächtig geführt worden, seine Beobachtung wurde aber eingestellt.

Der Umgang mit Terrorverdächtigen und Terrorist*innen ist in den Mitgliedsstaaten höchst widersprüchlich. Auch in Deutschland ist spätestens nach der Pannenserie der sächsischen Justiz im Fall al-Bakr klar geworden, dass es sehr viel zu verbessern gibt. Einerseits zeigt sein Fall, dass Gefahren falsch eingeschätzt wurden und es kein Zusammenwirken der Strafverfolgungsbehörden gab, andererseits ist der Umgang mit gefassten Täter*innen häufig unter dem Druck der Öffentlichkeit kopflos.

Die aktuellen Rezepte für den Umgang mit Verdächtigen sind Placebos. Fußfesseln, Staatsbürgerschaft entziehen, Ein- und Ausreiseverbote, Kennzeichnung ihrer Ausweise, unbeschränkte Vorbeugehaft a la Guantanamo, Grenzen schließen oder verschärft kontrollieren, Ausnahmezustand von Mitgliedsstaaten über Monate gehen am eigentlichen Problem vorbei und treffen nicht die Gefahren, denen sie begegnen sollen.

Solche Maßnahmen sind Symbolpolitik und suggerieren fälschlicherweise, man könne damit Sicherheit herstellen. Stattdessen muss gefragt werden: Ist die angedachte Maßnahme geeignet, auf eine bestimmte Terrorismusgefahr zu reagieren? Wie kann die Ausschaltung einer Gefahr oder die Reaktion auf einen Terroranschlag genutzt werden, um für künftige Vorfälle besser vorbereitet zu sein? Wie kann wirklich konsequent gegenüber diesen Personen gehandelt werden?

Politische Schnellschüsse helfen nicht weiter. Stattdessen ist eine effiziente polizeiliche und justizielle Zusammenarbeit grenzüberschreitend notwendig, um Gefahren zu erkennen und schnellstmöglich zu stoppen. Zweifellos müssen auch besonders sensible öffentliche Orte im stärkeren Fokus der Polizei sein. Aber weder Totalüberwachung ganzer öffentlicher Räume noch monatelange Grenzkontrollen, bringen echte Lösungen und verschwenden Ressourcen.

Die unmittelbare Bekämpfung des Terrorismus muss Aufgabe der Polizei sein. Ein entscheidender Eckpunkt einer Politik, die Terrorismusgefahren erkennen und abwehren hilft, ist die gezielte Kooperation der vorhandenen Strafverfolgungsinstrumente und -behörden. Die notwendigen Bedingungen dafür müssen auf Ebene der Mitgliedstaaten wie der EU geschaffen werden. Es ist klar, dass diese dazu auch in die Lage versetzt werden muss, und zwar in jeder notwendigen Hinsicht, also personell, strukturell und organisatorisch. Dazu gehört auch eine wirkungsvolle Korruptionsbekämpfung in den Mitgliedsstaaten und die Wahrung bzw. Wiederherstellung der Unabhängigkeit der Justiz.

Der erste Schritt ist, dass in der Polizeiausbildung und in Übungen der Umgang mit bestimmten Verdächtigen und Täter*innengruppen trainiert wird, und entsprechend geschultes Personal vorhanden ist. Das betrifft Beamte von Bundes- und Landeskriminalämtern, Polizeidirektionen bis hin zu Justizanstalten. Dazu sind allein in Deutschland Tausende neue Stellen notwendig, mit den damit verbundenen Investitionen. Die EU muss die Mitgliedsstaaten dazu anhalten, dass die Fortbildung von Polizei, Staatsanwaltschaften und Justizbeamten auf diesem Gebiet zu sichern ist. Wichtig ist, dass mehr Stellen „on the ground“ geschaffen werden auf Positionen, die direkten Kontakt mit Verdächtigen und Täter*innen haben, sowie Sachbearbeiter*innen, die mit konkreten bekannten Verdachtsfällen befasst sind. Dazu sind konkrete Projekte zu fördern, wie das positive Beispiel der Stadt Mechelen in Belgien anschaulich belegt.

Auch die Zuständigkeiten zwischen verschiedenen Behörden auf den unterschiedlichen Ebenen sind klar zu regeln, besonders auch dann, wenn es notwendig ist, dass die Zuständigkeit von einer Behörde oder Dienststelle zu einer anderen wechselt.

Das A und O sind natürlich die zügige und seriöse Aufklärung von terroristischen Straftaten, die Würdigung aller

Fakten und Tatumstände, ohne voreilige Beschuldigungen, einschließlich einer entsprechenden Bewertung der Polizeieinsätze und der gesamten staatlichen Reaktion. Auf Ebene der Mitgliedstaaten muss dafür gesorgt werden, dass es nicht zu einem Verzögern oder Aussitzen von Untersuchungen durch politisch Verantwortliche kommt, und eine ehrliche Fehleranalyse mit belastbaren Schlussfolgerungen stattfindet.

Über 30 Jahre nach der Unterzeichnung der ersten Schengen-Verträge gilt es auch der Tatsache Rechnung zu tragen, dass von Kroatien bis Norwegen und von Portugal bis Estland die Grenzkontrollen abgeschafft sind. Ein funktionierender Informationsaustausch der Polizeibehörden auf europäischer Ebene ist daher unverzichtbar, genauso wie Strukturen, die unverzüglich eine fallbezogene Zusammenarbeit erlauben. Anlassbezogen muss die reibungslose Kooperation zwischen den Polizeibehörden der Mitgliedsstaaten bei der Weitergabe relevanter Daten von Verdachtspersonen sichergestellt werden, damit rasch grenzüberschreitende Ermittlungsteams gebildet werden können. Die Förderung der Interoperabilität der Datenbanken der Polizeibehörden ist dafür ein nötiger Schritt. Ein effektiver und gezielter Datenaustausch unter strikter Wahrung der Grundrechte von Betroffenen wie Unbeteiligten im Einklang mit geltenden Datenschutzregeln lässt sich nur dann realisieren, wenn es um einen konkreten Anlass geht.

Die Zentren der Polizei- und Zollzusammenarbeit im grenznahen Raum benötigen dafür institutionalisierte enge Kooperationsbeziehungen, ähnliches sollte im Justizbereich erfolgen. Eine Einrichtung wie Europol kann dann sinnvoll sein, wenn sie den gezielten Datenaustausch und die EU-weite Kooperation fördert und dabei verbindlich alle Rechte derjenigen achtet, deren Daten von der Agentur verarbeitet werden. Dazu bedarf es einer starken Datenschutzaufsicht durch den europäischen Datenschutzbeauftragten und die nationalen Aufsichtsbehörden. Gleichzeitig muss die demokratische Kontrolle über die Agentur deutlich ausgebaut und effizienter werden, damit deren Arbeits- und Wirkungsweise endlich überprüft werden kann.

Schließlich ist es notwendig, dass Beamte mit Kontakt- und Beziehungsarbeit mit anfälligen lokalen Szenen beauftragt sind. Solche Beamte können im Rahmen von Anti-Radikalisierungsprojekten als Ansprechpartner*innen fungieren und eine zentrale Stelle in einem Frühwarnsystem einnehmen. Auch hierfür ist es notwendig, eine Vielzahl neuer Stellen zu schaffen, mit einem nicht auf Repression ausgelegten Auftragsprofil. Entscheidend aber ist, dass diese Beamt*innen an bestehende öffentliche und zivilgesellschaftliche Strukturen andocken können.

5. Quellen von Terrorismus konsequent bekämpfen, Finanzquellen austrocknen, internationale Unterstützer isolieren!

Richtig ist, dass sich das Gesicht des Terrorismus in den letzten 20 Jahren gewandelt hat. Dazu gehört auch, dass terroristische Zellen früher stärker regional begrenzt waren, jetzt aber transnationale Ausbreitung haben, zahlreiche Netzwerke, die flexibel und hochgefährlich agieren, sind entstanden. Neben bereits aktiven rechten Terrornetzwerken in der EU haben vor allem islamistische, religiös verbrämte Terrororganisationen an Bedeutung zugenommen. Es ist dringend geboten über die Ursachen dafür nachzudenken, und darüber, wie Quellen terroristischer Gewalt künftig ausgetrocknet werden können.

Denn Terrorismus ist das Ergebnis vielfältiger Entwicklungen, von Armut, Unterentwicklung, Diskriminierung, Demütigung und Ungerechtigkeit, Arroganz und Überheblichkeit westlicher Politik und zugleich auch der verfehlten postkolonialen Entwicklungen in den jeweiligen Regionen. Deshalb ist ihm einseitig mit polizeilichen oder gar geheimdienstlichen Mitteln nicht beizukommen.

Jahrelang haben die USA und andere westliche Staaten etwa Dschihadisten in ganzen Regionen gefördert, um eigene Interessen durchzusetzen, wie Zugang zu Rohstoffen und andere strategische Interessen. Der Irak ist ein Paradebeispiel für die verfehlte Politik des Westens, die vorrangig mitschuldig an der gegenwärtigen Situation im Nahen Osten geworden ist.

Dem Narrativ der Propaganda von Gruppen wie ISIS, nach dem sich die arabische Zivilisation in einem Terrorkrieg gegen westliche Dominanz, Ausbeutung und Zerstörung verteidigen muss, muss der Boden entzogen werden. Wir müssen die gesamte Politik gegenüber dem Nahen Osten überdenken. Arroganz, Einmischung und Geringschätzung anderer religiöser Überzeugungen haben zur Ablehnung des Westens beigetragen und ein Feindbild daraus entstehen lassen. Die konsequente Bevorzugung von Diktator*innen gegenüber demokratischen Bewegungen, wie etwa in Ägypten geschehen, tut ihr Übriges.

Wir fordern eine Abkehr von dieser Politik. Dazu braucht es eine faire Handels-, Wirtschafts- und Entwicklungspolitik auf Augenhöhe, die deutlich erkennbar nicht neokolonialen Zwecken dient. Damit Hand in Hand muss ein Kurswechsel in der Asyl- und Entwicklungspolitik gehen. Neben der Aufnahme von Geflüchteten in und durch alle Mitgliedsstaaten der

EU muss eine reguläre Grundlage geschaffen werden, Arbeitsmigration zu erleichtern, aber auch Flüchtlinge außerhalb der EU nachhaltig zu unterstützen. Kombiniert mit einer entschlossenen Unterstützung der durch den Krieg zerschlagenen Staaten und Regionen beim Wiederaufbau durch eine Art Marshallplan kann ein Weg eingeschlagen werden, der durch ehrliche Partnerschaft und Wohlstand zu Verständnis und Versöhnung zwischen dem Westen und anderen Teilen der Welt führt.

Damit Frieden entstehen kann, ist es jedoch unerlässlich, die Finanzierungsquellen terroristischer Netzwerke auszutrocknen. Das heißt internationale Geldgeber*innen, wie etwa Saudi-Arabien, zu identifizieren, ihr Handeln zu ächten, und Sanktionen und Sperren auf dem internationalen Geldmarkt gegen sie zu erwirken. Das bedeutet gleichzeitig, Waffenexporte, insbesondere in Krisenregionen und an Terror-Unterstützer, unverzüglich einzustellen. Hohe Profite gewinnen Terrornetzwerke heute auch aus kriminellem Handel mit Rohstoffen, Drogen, Kunstwerken und Waffen. Die organisierten Strukturen müssen schwerpunktmäßig in der Polizeikooperation angegangen und die beteiligten Netzwerke von Firmen und Hinterleuten identifiziert verfolgt werden.

6. Opfer unterstützen, Zusammenhalt stärken, Ausgrenzung beenden!

Allen, die direkt oder indirekt von einem Terroranschlag betroffen sind, gilt unsere volle Solidarität. Ihnen muss Hilfe jedweder Art zustehen. Dafür sind in allen Mitgliedsstaaten alle Rahmenbedingungen zu schaffen. Opfer von Terrorismus sollen Zugang zu finanzielle Hilfen, medizinischer psychologischer Beratung und Betreuung erhalten, solange sie dies benötigen. Dies ist zum Teil in der neuen EU-Terrorismusbekämpfungsrichtlinie bereits geregelt und muss nun schnell umgesetzt werden.

Auch vor Gericht müssen besondere Schutzmaßnahmen gelten, Schutzprogramme sind erforderlich. Wichtig ist auch die direkte und wirksame Hilfe, wenn Opfer den Klageweg vor dem Internationalen Strafgerichtshof und andere Strafverfahren anstrengen, um Täter*innen zur Verantwortung zu ziehen. Das betrifft soziale Hilfsangebote sowie kostenlose Rechtsberatung und Vertretung. Opfer von Terrorismus müssen erleichterte Aufnahmebedingungen in der EU erhalten, dürfen auf keinen Fall abgeschoben werden. Ihre schnelle und unbürokratische Integration ist ein Muss. Das gilt ebenso für ihre Familien.

Letztlich ist die Bekämpfung von Terrorismus eine Aufgabe für die gesamte Gesellschaft. Sozial abgehängte Milieus mit Menschen, die zu Recht glauben, von unseren Gesellschaften nichts mehr erwarten zu können, kann sich keine Gesellschaft dauerhaft leisten. Junge Leute, die unabhängig von ihren Schulnoten keine Aussicht haben, Arbeit zu finden und für die die einzige Chance auf Wohlstand und ökonomischen Aufstieg Kriminalität heißt, sind nach wie vor die am meisten empfängliche Gruppe für die Rekrutierer vom ISIS. Wir wollen eine Gesellschaft, die niemanden zurück lässt - und das ist auch das beste Rüstzeug gegen Terrorismus.

Unsere Antwort auf Terrorismus muss sein, den Zusammenhalt in den Gesellschaften Europas wieder auf die Tagesordnung zu bringen. Wir müssen dazu die Ausgrenzung von Menschen beenden. Mehr miteinander zu reden, lautet die Formel. Wir müssen mehr reden mit denen, die ausgegrenzt werden, und mit denen, die sich selbst ausgrenzen. Dabei müssen wir für die Regeln und Normen unserer Gesellschaft ebenso eintreten, wie wir es lernen müssen, Verständnis zu haben für Andersartigkeit, für Diversität. Dies ist der Ansatzpunkt einer modernen Inklusionspolitik, und es ist auch die Grundlage einer umfassenden Anti-Radikalisierungspolitik. Es gilt, das Immunsystem unserer Gesellschaft zu stärken.

Dazu brauchen wir flächendeckende Strukturen, die als Frühwarnsystem dienen, wenn Menschen in gewalttätige, radikalisierte Milieus rutschen. Neben der notwendigen Sensibilisierung von Lehrer*innen, Sozialarbeiter*innen, Geistlichen und anderen Vertrauenspersonen müssen Strukturen geschaffen werden, die es erlauben, schnell zu reagieren, sobald es Anzeichen von gewalttätiger Radikalisierung gibt. Ausdrücklich gilt das nicht nur für den islamistischen Terrorismus, sondern auch für den rechtsextremen Terrorismus. Das ist wichtig, weil gerade im Kampf gegen Rechtsextremismus in Deutschland wertvolle Erfahrungen gemacht worden sind. Daher wissen wir auch, wie wichtig die Rolle von Aussteigern ist und das Wissen darüber, wie und unter welchen Bedingungen Radikalisierung stattfindet. Wir benötigen wirksame Aussteigerprogramme und eine entsprechende Infrastruktur, wie Beratungsangebote und Schutzräume. Aussteiger sind die Einzigen, die die Szene wirklich kennen, Gefahren benennen und Gründe für einen Ausstieg erklären können. Diese Programme müssen auch EU-finanziert werden.

Eine vordringliche Aufgabe in den Mitgliedsstaaten sind Präventionsprojekte. Diese dürfen nicht nur auf repressive Maßnahmen beschränkt bleiben, sondern müssen auf Kooperation und Vertrauen ausgerichtet sein. Runde Tische, die eine Zusammenarbeit von Schulen, Vertreter*innen von

Glaubensgemeinschaften, Sozialarbeiter*innen, Vereinen und Verbänden der verschiedensten Communities ermöglichen, müssen eingerichtet werden. Entsprechend sensibles und ausgebildetes Personal ist dafür nötig, Sensibilisierungsmaßnahmen müssen sprichwörtlich auch für ehrenamtliche Fußballtrainer*innen angeboten werden. Ein spezieller Entradikalisierungsplan der EU für Gefängnisse, wo bislang das Radikalisierungspotential erheblich ist, ist überfällig.

Entscheidende Partner*innen sind bei der Entradikalisierung die Kirchen und Gemeinden, insbesondere auch die muslimischen Gemeinden. Wir lehnen jede Stigmatisierung von Religionen strikt ab, Religionsfreiheit muss für alle gelten. Vorschläge, wie Minarettverbote oder das Verbot von Burkas oder des Tragens von Kopftüchern sind Mummenschanz, sie treffen die Falschen und erreichen das Gegenteil. Zweifellos sind die meisten Moscheen Teil der Lösung, nicht das Problem. Religiöse Würdenträger*innen nehmen eine Schlüsselrolle ein, sie können am besten verdeutlichen, dass religiös verbrämter Terrorismus nichts mit ihrer Religion zu tun hat, sondern einen Missbrauch darstellt.

Entsprechend unterstützen wir die lange erhobenen Forderungen der muslimischen Gemeinden nach einer universitären Ausbildung islamischer Theologen in den Mitgliedsstaaten, was auch für alle anderen Religionen gelten muss. In den EU-Staaten, wo es Religionsunterricht in der Schule gibt, muss es auch einen islamischen Unterricht geben, mit Lehrer*innen, die auch dort ausgebildet worden sind. In Deutschland sollten islamische Gemeinden endlich als Körperschaften des öffentlichen Rechts anerkannt werden. So kann ein Umgang auf Augenhöhe erreicht werden.

7. Über hate speech reden, nicht schweigen!

Welche Auswirkungen Terrorismus auf unsere Gesellschaften hat, hängt am Ende maßgeblich davon ab, wie wir in der Öffentlichkeit darüber reden. Unsere Diskurse in den Medien machen einen Unterschied. Von ihnen hängt ab, ob eine Mehrheit auf einen Terroranschlag reagiert mit Hass, Ausgrenzung und Krieg, oder mit Besonnenheit und Verantwortung. Das betrifft nicht nur die etablierten Medien, sondern uns alle. Schon lange finden solche Diskussionen in Kommentaren, in Foren und in sozialen Medien statt, und immer mehr Menschen sind daran beteiligt.

Von den Medien erwarten wir, dass sie in ihrer Berichterstattung auf der einen Seite nichts verschweigen, was relevant ist, auf der anderen Seite aber auch nicht ungewollt dazu beitragen, Täter*innen hoch zu stilisieren. Das entspricht einem journalistischen Ethos und ist Aufgabe der Medien und ihren Vertreter*innen, in ihrem Arbeitscodex sicher zu stellen. Dieser Verantwortung können und müssen sie gerecht werden. Wir sehen auch eine besondere Verantwortung bei den sozialen Medien und Betreibern und Betreiberinnen von Foren und Kommentaren, hate speech und rassistische und zur Gewalt oder Terror aufrufende Hetze unverzüglich zu löschen, sobald sie bekannt sind. Die Löschung von solchen Inhalten muss auch erzwungen werden können, dazu bedarf es gesetzlicher Vorschriften.

Wir wollen hier keiner Zensur das Wort reden. Meinungs- und Redefreiheit müssen definitiv gesichert sein. Daher wenden wir uns gegen alle Formen von Netzsperren und intransparente Selbstverpflichtungsmodelle. Solche Maßnahmen behindern die öffentliche Auseinandersetzung. Die endgültige Entscheidung, welche Beiträge die Grenzen der Redefreiheit hin zu hate speech und Hetze überschreiten, muss am Ende in den Händen der Gerichte liegen, nicht in den Händen von facebook und Co. Gefordert sind aber auch die Bürger*innen selbst, die ihre Kommentare veröffentlichen, an den Debatten teilnehmen. Und die es lernen müssen, selbstbewusst mit Fake News umzugehen. Nichts kann den souveränen und bewussten Umgang der Nutzer*innen, und damit der Öffentlichkeit damit ersetzen.

Ansprechpartner*innen

Dr. Cornelia Ernst

Mitglied des Europäischen Parlaments
Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres

In Brüssel:
Dr. Cornelia Ernst MdEP
Europäisches Parlament
Rue Wiertz 60, WIB 03 M 19
B -1047 Brüssel
Belgien
Telefon: +32 (0) 228/ 476 60
fax +32 (0) 228/ 496 60
Mail: cornelia.ernst@europarl.europa.eu

In Dresden:
Dr. Cornelia Ernst
Wahlkreisbüro / Europabüro Dresden
Großenhainerstr.93
01127 Dresden
Tel. 0351/426 900 05
Fax: 0351/206 990 46
Mail: europa@cornelia-ernst.de

www.cornelia-ernst.de

„Sicherheit ist nach Lesart der LINKEN deutlich mehr als der vorgegaukelte Schutz vor terroristischen Gefahren. Sie heißt auch sich frei bewegen zu können im öffentlichen Raum, sich eines handelnden Rechtsstaates und der eigenen Rechte sicher sein zu können.“ Dr. Cornelia Ernst