Handbuch Überwachung

Angelika Adensamer (Hrsg.)

EPICENTER .WORKS
for digital rights

HANDBUCH ÜBERWACHUNG

Herausgeberin:
Angelika Adensamer

Autor_innen:
Angelika Adensamer
Andreas Czák
Alina Hanel
Marlene Kreil
Reinhard Kreissl
Christof Mackinger
Hanna Prykhodzka
Clara Schermer
Teresa Schwaninger
Lisa Seidl
Erwin Ernst Steinhammer
Christoph Tschohl
Herbert Waloschek
Levin Wotke

Handbuch Überwachung

Herausgegeben von epicenter.works – Plattform Grundrechtspolitik
(ehemals: Arbeitskreis Vorratsdaten Österreich)
Widerhofergasse 8/2/4
1090 Wien

Zuständige Vereinsbehörde: Landespolizeidirektion Wien, Büro für Vereins-, Versammlungs- und Medienrechtsangelegenheiten
ZVR-Zahl: 140062668
UID: ATU66502037

Herausgeberin: Angelika Adensamer
Autor_innen: Angelika Adensamer, Andreas Czák, Alina Hanel, Marlene Kreil, Reinhard Kreissl, Christof Mackinger, Clara Schermer, Teresa Schwaninger, Lisa Seidl, Erwin Ernst Steinhammer, Christof Tschohl, Herbert Waloschek, Levin Wotke.
Satz, Layout, Grafiken: Hanna Prykhodzka

Finanziert durch eine Projektförderung von netidee und durch einen Druckkostenzuschuss der Arbeiterkammer.

Publiziert Mai 2020

ISBN Web: 978-3-200-06869-8
ISBN Druck: 978-3-200-06870-4

Inhaltsverzeichnis

Überwachungsbefugnisse

Rechte von Betroffenen

Abstract

Das Handbuch Überwachung stellt den rechtlichen und gesellschaftlichen Rahmen polizeilicher Überwachung im sicherheitspolizeilichen und strafprozessrechtlichen Bereich, sowie im Aufgabenbereich des Verfassungsschutzes in Österreich, dar. Mit diesem Unterfangen wurde von epicenter.works schon 2016 mit der Publikation des Handbuchs zur Evaluation der Anti-Terror-Gesetze in Österreich (HEAT) begonnen. In dieser Neuauflage wurde auf der Arbeit von damals aufgebaut und die Ausführungen, Ideen und Konzepte weiterentwickelt.

Für die Beurteilung, wann in einer Gesellschaft das Maß der Überwachung über die Schwelle des Ertragbaren getreten ist, müssen die Überwachungsmaßnahmen in ihrer Gesamtheit und in ihren Kombinationen betrachtet werden. Daher muss mit einer Überwachungsgesamtrechnung festgestellt werden, wie stark der Überwachungsdruck auf die Bevölkerung ist. Das bedeutet nicht nur, einzelne Überwachungsbefugnisse dahingehend zu beurteilen, ob sie verhältnismäßig und gerechtfertigt sind, sondern den Blick umzudrehen und aus der Perspektive einer Person festzustellen, wie vielen Überwachungsmaßnahmen sie schon unterliegt, wie viele Daten über sie vorhanden sind und wie diese verknüpft werden können. Dieses Handbuch ist ein erster Schritt für die Konzeption einer solchen Überwachungsgesamtrechnung.

Mit dem Handbuch soll Journalist_innen, Studierenden verschiedener Studienrichtungen, Beamt_innen und Mandatar_innen, sowie einer interessierten Zivilgesellschaft erleichtert werden, die – oftmals sehr technischen und komplizierten – Debatten über die Ausweitung von Überwachungsbefugnissen nachzuvollziehen und sich aktiv an ihnen zu beteiligen. Die Kapitel stehen nebeneinander und müssen nicht in einer bestimmten Reihenfolge gelesen werden. Es kann daher umso hilfreicher sein, hervorgehobene Begriffe parallel im Glossar nachzulesen oder den Verweisen auf andere Textstellen zu folgen. Das Handbuch ist in vier Kapitelgruppen eingeteilt, wovon sich die erste mit Überwachung und Gesellschaft beschäftigt, die zweite mit den Überwachungsbefugnissen im Detail, die dritte mit Betroffenenrechten und die die vierte mit der Evaluierung von Gesetzen.

Vielen Dank an netidee, deren Förderung dieses Projekt möglich gemacht hat!

Vorwort

In den letzten Jahren wurde die österreichische Bevölkerung immer wieder mit neuen Überwachungsmaßnahmen konfrontiert. Sowohl der Österreichische Rechtsanwaltskammertag (ÖRAK) als auch epicenter.works haben sich entschieden und mit fundierter Argumentation gegen diese Tendenz – wie beispielsweise Polizeiliches Staatsschutzgesetz, Bundestrojaner und Co. – ausgesprochen.

Die mittlerweile in der Politik einkehrende Vernunft bezüglich mancher Überwachungsvorhaben ist sicher auch unserer langjährigen kritischen Bewusstseinsbildung zu verdanken. So hat die letzte Entscheidung des VfGH zum Sicherheitspaket gezeigt, dass wir mit unserer Meinung richtig lagen.
Der Staat hat die Grund- und Freiheitsrechte der Bürgerinnen und Bürger zu achten und zu wahren. Gesetze dürfen in einem Rechtsstaat nicht zur anlasslosen Überwachung unschuldiger Bürginnen und Bürger führen. Im Gegenteil. Die Politik muss sich ihrer Verantwortung bewusst sein. In einer Zeit, in der die Menschen im Alltag immer leichtfertiger mit ihren Daten umgehen (Stichwort Alexa), ist es Aufgabe der Politik, diesen Trend nicht auch noch zu verstärken.

Der vorliegende Bericht von epicenter.works setzt sich umfassend und detailliert mit einzelnen Überwachungsmaßnahmen auseinander. Eine solche Gesamtevaluierung, wie sie auch im aktuellen Regierungsprogramm vorgesehen ist, ist dringend notwendig und eine langjährige Forderung der Rechtsanwaltschaft.

Wie man anhand zahlreicher Beispiele im Ausland sehen kann, ist selbst umfassende Überwachung keine Garantie für die Verhinderung von Straftaten. Vielmehr ähnelt eine solche Vorgehensweise der Suche nach einer Nadel im Heuhaufen, wobei der Heuhaufen durch jede weitere Überwachungsmaßname vergrößert wird. Überwachungsbefugnisse müssen stets gezielt, verhältnismäßig und mit den erforderlichen Rechtsschutzinstrumenten ausgestaltet sein, ohne dass die Grund- und Freiheitsrechte der Bevölkerung dadurch ausgehöhlt werden.
Denn: Wie schon der ehemalige US-Präsident Benjamin Franklin sagte, wird jemand, der Freiheit aufgibt, um Sicherheit zu gewinnen, am Ende beides verlieren.

Dr. Rupert Wolff
Präsident des ÖRAK – Österreichischer Rechtsanwaltskammertag

Autor_innen

Mag.a **Angelika Adensamer**, MSc, ist Juristin und Kriminologin und arbeitet als Policy Advisor bei epicenter.works. Sie hat das Handbuch herausgegeben und editiert, sowie u.a. die Kapitel „Überwachungstechnologien und Big Data“, „Datenschutz im Polizeibereich“ und Teile über die Überwachungsbefugnisse im Einzelnen, sowie den Überblick verfasst.

Andreas Czák, B.Sc, arbeitet seit 2015 für epicenter.works (damals AK Vorrat) zu den Themen Netzpolitik, Menschenrechte und Überwachung. Er hat für das Handbuch Überwachung parlamentarische Anfragen zur Überwachungsstatistik recherchiert und grafisch aufbereitet.

Mag.a **Alina Hanel**, BA, ist Politik- und Rechtswissenschafterin und überarbeitete und ergänzte für das Handbuch Überwachung das Kapitel „Videoüberwachung“, und verfasste den Abschnitt „Bundestrojaner“ für das Kapitel über umstrittene Überwachungsbefugnisse.

Mag.a **Marlene Kreil** ist Juristin und studiert Politikwissenschaften im Masterprogramm der Universität Wien. Ihr großes Interesse für Grund- und Menschenrechte bewegte sie dazu, im vorliegenden Buch das rechtliche Verhältnis von Freiheit und Überwachung zu analysieren. Neben Netzpolitik befasst sich Marlene Kreil auch mit Bildungs- und Asylpolitik.

Reinhard Kreissl, Dipl.-Soz. Dr. phil., PD, ist Gründer und Leiter des Vienna Centre for Societal Security, Lehre und Forschung im Bereich Rechtssoziologie, Sicherheitsforschung und Kriminologie und verantwortlich für das Kapitel „Überwachung aus sozialwissenschaftlicher Perspektive“.

Christof Mackinger schreibt als freier Journalist zu den Themen Gefängnis, Rechtsextremismus, Soziale Bewegungen, Klima, und in seinem Buch über die Überwachung der Tierrechtsbewegung (2011) als Betroffener des Prozesses. Er verfasste den Beitrag „Österreichs polizeiliche Überwachungsbefugnisse im Zeitraffer“.

Hanna Prykhodzka, BA, ist Medienwissenschaftlerin und war für Grafik und Satz bei dieser Publikation verantwortlich. Die verständliche Aufbereitung der komplexen Inhalte des Buches war ihr ein Anliegen. Hanna arbeitet bei epicenter.works seit 2017 und befindet sich im Masterstudium.

Clara Schermer, MA, war als Lektorin und in der Publikationsassistenz am Handbuch beteiligt. Sie ist als Medienkulturvermittlerin tätig, sowie als Filmexpertin unter anderem beim Kurzfilmfestival Vienna Shorts zuständig für Festivalkatalogredaktion, Filmauswahl und Filmvermittlung für Jugendliche.

Mag.a **Teresa Schwaninger** ist Juristin und arbeitete am Handbuch Überwachung zu den Themen Nachrichtenüberwachung, Auskunft von Telekommunikationsdaten und Anlassdatenspeicherung. Die Einhaltung von Grund- und Menschenrechten sind ihr nicht nur im Bezug auf staatliche Überwachung ein Anliegen, sondern auch im sozialen Bereich, weshalb sie auch im Sozialrecht tätig ist.

Lisa Seidl, LL.M., ist Juristin und arbeitet als Policy Advisor bei epicenter.works. Sie erarbeitete in der Endphase der Publikation die Rechtsquellenübersicht zu Auskunftspflichten und Ermittlungsbefugnissen insbesondere nach TKG, SPG, PStSG und StPO.

Erwin Ernst Steinhammer studiert Politikwissenschaft an der Universität Wien. Er engagiert sich seit Jahren bei epicenter.works, arbeitete dort v.a. zum Bundestrojaner und als Beobachter des vorparlamentarischen und parlamentarischen Gesetzgebungsprozesses. Er bereitete für das Handbuch Überwachung den vorparlamentarischen Gesetzgebungsprozess auf.

Christof Tschohl ist Nachrichtentechniker und promovierter Jurist. Er arbeitet als wissenschaftlicher Leiter der Research Institute AG & Co KG – Digital Human-Rights Center und ist ehrenamtlicher Obmann von epicenter.works. Er hat das Kapitel zur Wirkungsfolgenabschätzung (WFA) sowie zur Gesamt-Qualitätssicherung der Publikation beigetragen.

Herbert Waloschek war als Abteilungsleiter einer österreichischen Großbank für IT-Strategie, Systemintegration, Safety/Securitymanagement zuständig. Dabei hat er Systementwicklung und -Integration als Geschäftsprozess etabliert und mehrere Großprojekte in Time, in Quality, in Budget abgewickelt.

Mag. iur. **Levin Wotke,** BA, hat in Graz Journalismus und Public Relations und in Wien Rechtswissenschaften studiert. Er beschäftigte sich für das Handbuch vor allem mit den Themen Observation und verdeckte Ermittlung und außerdem mit Datenauskünften im Rahmen des TKG, des ECG und der StPO.

Dank
Außerdem geht Dank an die Autor_innen des Handbuch zur Evaluation der Anti-Terror-Gesetze in Österreich, das als Grundlage für diese Neuüberarbeitung gedient hat: Christof Tschohl, Ewald Scheucher, Dieter Kargl, Julia Luksan, Alexander Czadilek, Herbert Waloschek, Reinhard Kreissl, Kilian Klinger und Walter Hötzendorfer.

Sowie Benedikt Gollatz, Bernhard Hayden, Iwona Laub und Tanja Mally des epicenter.works-Teams, die das Projekt in Planung, Öffentlichkeitsarbeit und Webauftritt unterstützt haben.

Für Reviews geht Dank an Heidi Scheichenbauer, Nora Pentz, Stefan Hirschmann und Lukas Daniel Klausner.

Einleitung und Hinweise für Leser_innen

Einleitung

Wäre die Leitfrage dieses Handbuchs für Überwachung „Wie soll der Staat seine Bürger*innen überwachen?“ würde unsere Antwort lauten: „So wenig wie möglich.“ Dies ist das Vorzeichen, unter dem der Verein epicenter.works schon seit 10 Jahren (vormals noch unter dem Namen „Arbeitskreis Vorratsdaten“) das Grundrecht auf Achtung der Privatsphäre und das Grundrecht auf Datenschutz verteidigt. Dieses Handbuch dient dazu, den rechtlichen und gesellschaftlichen Rahmen polizeilicher Überwachung darzulegen, um damit mehr Menschen die Möglichkeit zu geben, die – oftmals sehr technischen und komplizierten – Debatten über die Ausweitung von Überwachungsbefugnissen nachzuvollziehen und sich aktiv an ihnen zu beteiligen.

Die letzten Jahrzehnte sind geprägt vom Aufrüsten staatlicher Kontrolle im Namen vermeintlicher Sicherheit auf der einen Seite, und auf der anderen Seite vom Ausbau neuer milliardenschwerer Märkte, auf denen mit personenbezogenen Daten, Verhaltensprognosen und sogar mit dem Versprechen, dieses Verhalten beeinflussen zu können, gehandelt wird. Diese Entwicklungen sind nicht unabhängig voneinander und nähren und verstärken sich gegenseitig. In besonderem Maße betroffen sind oft gerade marginalisierte Menschen, wie z.B. arme Menschen, Schutzsuchende, Sozialhilfeempfänger_innen, oder Menschen, deren Namen und Aussehen als fremd und verdächtig gewertet werden. David Lyon schreibt in diesem Sinne über Überwachung, sie habe immer den Effekt des „sozialen Sortierens“[1], denn die systematische Erfassung von Menschen kann nur sinnbringend verarbeitet werden, wenn die Menschen kategorisiert werden. Manche dieser Kategorien sind an sich schon problematisch und haben kaum empirische Grundlagen wie Kriterien, anhand derer Gefährlichkeit oder Verdacht festgestellt werden sollen. Anhand welcher Kategorien es legitim ist, Menschen zu kategorisieren, und aus welchen Merkmalen es zulässig sein soll, Ableitungen zu machen, ist eine der heute brennenden politischen Fragen.

Auf politischer Ebene werden Überwachungsbefugnisse ausgeweitet und Massenüberwachungssysteme umgesetzt, indem ein Klima der Angst erzeugt wird. Indem Sicherheit als rein subjektiver Faktor akzeptiert wird, kann dieser auch durch Erzeugung von Emotionen in der Bevölkerung verändert werden. Die Einführung von Überwachungsmaßnahmen kann damit zwei Funktionen zugleich erfüllen: einerseits das ostentative Darstellen ihrer eigenen Notwendigkeit und andererseits die Präsentation von einfachen Lösungen auf komplizierte gesellschaftliche Fragen, wie der nach Identität und Zugehörigkeit.

Faktoren der Unsicherheit in einer Bevölkerung sind aber neben Verbrechen und Kriminalität auch prekäre Lebensverhältnisse, Instabilität der Wohnverhältnisse, Disfunktionalität der Krankenversicherung, Arbeits- und Perspektivenlosigkeit, Unsicherheit über das Leben in einer zukünftigen Klimakrise

sowie Betroffenheit von Diskriminierung und Rassismus. Soziale und staatliche Kontrolle und Überwachung verschärfen diese Unsicherheiten für weite Teile der Bevölkerung, anstatt sie zu beruhigen.

Oft werden in der politischen Debatte um die Ausweitung von Polizeibefugnissen der Schutz unserer „Grundwerte“, unserer Verfassungsordnung, ja unseres gesamten Staates heraufbeschworen. Abgesehen davon, dass der Staat und seine Institutionen im Österreich der letzten Jahrzehnte kaum unter einer echten Existenzbedrohung litten, und die Kriminalität in Österreich stetig sinkt, darf in dieser Debatte nicht vergessen werden, dass gerade die Freiheitsrechte im Kern unseres modernen demokratischen Rechtsstaats liegen. Die Integrität der Privatsphäre der Bürger_innen ist gemeinsam mit dem Recht auf physische Unversehrtheit, Freiheit der Meinungsäußerung und politischen Freiheiten geradezu der zentrale Wert, den eine Demokratie schützen soll. Es gibt keine freien Menschen mit freier Meinung, freiem Leben, Handlungsspielräumen, es gibt keine echten Debatten, keine echte Politik und keine Freiheit ohne Privatsphäre. Und es gibt auch keine Demokratie ohne Freiheit. Man kann daher auch die Verfassung und ihre Institutionen nicht schützen, indem man die Grundrechte aushöhlt. Tut man dies, wird man selbst zum Feind des Rechtsstaates.

Wo genau nun die Linie verläuft zwischen einer „wehrhaften Demokratie“, die sich vor extremistischen Angriffen zu schützen im Stande sein muss und zwischen dem autoritären Abbau von Grundrechten – ist eine der zentralen Debatten unserer Zeit.

Die Perspektive auf das Thema Überwachung dieses Handbuchs ist überwiegend – aber nicht nur – rechtlicher Natur und viele der Autor_innen sind Jurist_innen. Wir haben uns aber bemüht, das Handbuch für Nicht-Jurist_innen zu gestalten und erklären die notwendigen juristischen Grundbegriffe jeweils. Dies kann zwar bedeuten, dass man im Handbuch hin und her blättern muss, dafür sollten endlich aber alle wichtigen Begriffserklärungen im Glossar oder im dazu empfohlenen Kapitel zu finden sein. Das Ziel ist, dieses Handbuch Journalist_innen, Studierenden verschiedener Studienrichtungen, Beamt_innen und Mandatar_innen, sowie einer interessierten Zivilgesellschaft zur intensiveren Auseinandersetzung mit polizeilicher Überwachung in Österreich an die Hand zu reichen. Eine höhere Zugänglichkeit zu diesem komplexen Themenbereich ist unerlässlich, sollen die Debatten und die Entscheidungen, die wir auf ihnen beruhend als Gesellschaft treffen, auf demokratische Weise geführt werden. Wir hoffen, dass auch Jurist_innen das Handbuch gerne lesen werden, können aber in diesem Rahmen keine detaillierten Auseinandersetzungen mit den komplizieren Fragen des Polizei- und Verfassungsrechts bieten.

Die Überwachungsgesamtrechnung?

Je mehr wir unsere Smartphones bei uns tragen und in immer mehr Bereichen unseres Lebens von Software und Apps unterstützt werden, desto mehr Informationen gibt es über uns: Daten über unseren Aufenthaltsort, unsere Kontakte und Beziehungen, Kommunikation, Einkäufe, Kalender, Gesundheit und Familien sowie unsere Photos und Notizen. Durch die unterschiedlichen Überwachungsmaßnahmen können die verschiedenen Bereiche unseres Lebens ins Visier kommen. Für die Beurteilung, wann in einer Gesellschaft das Maß der Überwachung über die Schwelle des ertragbaren, getreten ist, reicht es nicht, die Überwachungsmaßnahmen jeweils im Einzelnen zu betrachten, sondern sie müssen in ihrer Gesamtheit und in ihren Kombinationen betrachtet werden. Das Konzept der Überwachungsgesamtrechnung geht auf ein Urteil des deutschen Bundesverfassungsgerichts aus 2010 zurück, in dem der Gesetzgeber „in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung“ angehalten wird.[2]

Mit einer Überwachungsgesamtrechnung soll festgestellt werden, wie stark der Überwachungsdruck auf die Bevölkerung ist. Das bedeutet, nicht nur eine einzelne Überwachungsbefugnis dahingehend zu beurteilen, ob sie verhältnismäßig und gerechtfertigt ist, sondern den Blick umzudrehen und aus der Perspektive einer Person festzustellen, wie vielen Überwachungsmaßnahmen sie schon unterliegt, wie viele Daten über sie vorhanden sind und wie diese von wem verknüpft werden können.

Es ist oft Bestandteil der rechtlichen Beurteilungen von Überwachungsbefugnissen, zu prüfen, ob aufgrund der erhobenen Daten Rückschlüsse auf die Persönlichkeit, das Privatleben, die Beziehungen und Lebensführung, Vorlieben und Meinungen der Betroffenen möglich ist. Dies ist manchmal aufgrund zweier Maßnahmen einzeln jeweils nicht möglich, sehr wohl aber durch deren Kombination, weil erst der Zusammenhang der Daten wichtige Erkenntnisse bringt. So können Verknüpfungen dazu führen, dass sich Überwachungsmaßnahmen gegenseitig potenzieren, statt einfach nebeneinander zu stehen. So lässt sich z.B. aus den Daten über den Standort einer Person allein ihre Identität nicht ableiten, sehr wohl aber durch den Abgleich mit dem Melderegister und öffentlichen Daten über Angestellte an der Adresse, die dem Arbeitsplatz der Person zugeordnet werden kann.

Die Gesamtrechnung muss mit einer kompletten Erfassung von Überwachungsmaßnahmen und der angewandten Technologien und Datenbanken beginnen. Dabei müssen auch private Speicherverpflichtungen mit Blick auf Abfragebefugnisse in die Betrachtung einbezogen werden. Da sich Technologien weiterentwickeln und sich ihre Funktionsweise ändert, ist auch die manchmal beschworene „Technologieneutralität“ des Rechts mitunter fehl am Platz. Auch die Größe von Datenbanken und von Abgleichsamples verändern die Eingriffsintensität von Überwachungsmaßnahmen. Diese Überlegungen werden in Kapitel 3 näher ausgeführt.

Eine umfassende Überwachung der Bevölkerung hat sogenannte „chilling effects“ zur Folge, was bedeutet, dass Menschen auch legales Verhalten unterlassen, aus Angst, dabei beobachtet zu werden, und aus Unsicherheit über mögliche Konsequenzen. So wirkt Kontrolle, ohne dass tatsächliche Repressionsmaßnahmen gesetzt werden müssen, und führt zu einer „Normalisierung“, also eines immer weiteren Angleichens des Verhaltens der Menschen. Dieser chilling effect kommt gerade in der Summe der Überwachungsbefugnisse zum Tragen, und wenn viele der Befugnisse in die Breite wirken, wie die Videoüberwachung im öffentlichen Raum, die Vorratsdatenspeicherung, oder die Aufzeichnung von Reisebewegungen. Auch der Verfassungsgerichtshof hat im Dezember 2019 in seiner Entscheidung über die automatische Kennzeichenerfassung festgestellt, dass das “Gefühl der Überwachung“[3] in der Bevölkerung Rückwirkung auf die Ausübung anderer Grundrechte, wie die Versammlungsfreiheit und die Freiheit der Meinungsäußerung haben kann.

Das Unterfangen einer Überwachungsgesamtrechnung wurde von epicenter.works schon 2016 mit der Publikation des Handbuchs zur Evaluation der Anti-Terror-Gesetze in Österreich begonnen.[4] Mit der vorliegenden Neuauflage des Handbuchs Überwachung wurde auf der Arbeit von damals aufgebaut und die Ideen und Konzepte wurden weiterentwickelt.

Wir können im Rahmen dieses Handbuchs keine komplette Gesamtrechnung erstellen, wir wollen aber unsere Vorarbeiten und Überlegungen zu einer solchen strukturiert weitergeben und hoffen, sowohl selbst daran weiter arbeiten zu können, als auch andere dazu zu animieren, sich ihrer konzeptuellen Weiterentwicklung anzunehmen. Das Handbuch Überwachung ist nur ein weiterer Schritt.

Die Gesamtevaluation soll ergeben, wo Überwachungshäufungen und wo Lücken liegen. Sie soll auch dazu führen, die Überwachungsbefugnisse, die nicht notwendig sind, die z.B. so gut wie nie angewendet werden, nicht erfolgreich, oder überflüssig sind, weil die Daten auch auf andere Weise ermittelt werden können, zurück zu nehmen. Zugleich muss für jede neue Überwachungsmaßnahme gezeigt werden können, dass sie gegenüber dem Ist-Stand einen eindeutigen Mehrwert darstellt. Nachdem diese Forderung viele Jahre lang unerfüllt geblieben ist, heißt es nun im Programm der Türkis-Grünen Regierung, es werde endlich eine umfassende Evaluierung gesetzlicher Regelungen von Ermittlungsmaßnahmen bestehender Überwachungssysteme unter Einbindung der Zivilgesellschaft und unabhängiger Expertinnen und Experten sowie die Erstellung eines Berichts“[5] geben.

Überblick

Damit das Handbuch Überwachung in seiner Länge handhabbar bleibt, beschränken wir uns inhaltlich auf die Überwachungsbefugnisse der österreichischen Polizei – im sicherheitspolizeilichen und strafprozessrechtlichen Bereich sowie im Aufgabenbereich des Verfassungsschutzes . Die Überwachungsbefugnisse anderer staatlicher Behörden, wie insbesondere des Militärs, oder der Finanzbehörden werden ebenso außer Acht gelassen, wie die weitgehende Überwachung, die von privaten Unternehmen ausgeht.

Die Kapitelgruppe A (S. 23) widmet sich gesellschaftlichen Perspektiven auf Überwachung und ihren Auswirkungen. Den Anfang macht ein sozialwissenschaftlicher Beitrag von Reinhard Kreissl, in dem er das Anwachsen des Überwachungsstaats in einen Kontext mit der Veränderung der Gesellschaftsordnung im Allgemeinem und dem Kampf gegen den Terrorismus im Konkreten stellt. Danach stellt Christof Mackinger die Ausweitungen der Überwachungsbefugnisse in Österreich der letzten 30 Jahre in einen historisch-politischen Kontext. Das 3. Kapitel von Angelika Adensamer widmet sich der Rolle, die technische Neuerungen und das Wachsen der Datenmengen der letzten Jahre auf die Wirkungen von Überwachung haben, und führt aus, wieso technische Möglichkeiten bei der Einführung von Überwachungsbefugnissen mitbedacht werden müssen.

Die Kapitelgruppe B (S. 51) bietet eine Einführung in die juristischen Aspekte der einzelnen geltenden Überwachungsbefugnisse. Sie beginnt mit einem Überblickskapitel, in dem der juristische Rahmen, der für alle Überwachungsbefugnisse gilt, abgesteckt wird. Hier wird u.a. die Bedeutung der Unterscheidung zwischen dem Strafprozessrecht und dem Sicherheitspolizeigesetz erklärt, werden Kontrolle und Aufsichtsbefugnisse und der besondere Schutz der Berufsgeheimnisträger und des Bankgeheimnisses beschrieben, sowie ein Überblick über die Quellen, die uns über den Einsatz von Überwachungsbefugnissen in Österreich zur Verfügung stehen, gegeben. Darauf folgen drei Kapitel, die sich im Detail Überwachungsbefugnissen widmen, die in der politischen Debatte besonders viel Aufmerksamkeit bekommen und in den letzten Jahren immer wieder geändert wurden: verdeckte Ermittlung, Videoüberwachung und Telekommunikationsüberwachung. Es wird jeweils die Rechtslage der einzelnen Befugnisse unter diesen Klammern sowohl im sicherheitspolizeilichen als auch im strafprozessrechtlichen Bereich dargestellt.

Dabei haben wir uns Mühe gegeben, dies auch für Menschen ohne juristische Vorkenntnisse verständlich aufzubereiten. Jeweils werden auch – soweit vorhanden – die Zahlen der tatsächlichen Einsätze der Maßnahmen dargestellt und deren Entwicklung und die damit einhergehenden politischen Debatten thematisiert. Schließlich werden in einem eigenen Kapitel besonders umstrittene Befugnisse zusammengefasst, die teilweise unlängst von Höchstgerichten aufgehoben wurden, bzw. gegen die noch offene Beschwerdeverfahren laufen:

der Bundestrojaner, die Fluggastdatenverarbeitung, die Kfz-Überwachung und Section Control, die Rasterfahndung und die Beschlagnahme von Briefen. Teile dieser Kapitelgruppe stammen aus dem Handbuch für Evaluation der Anti-Terror-Gesetze, Teile sind unter enger Zusammenarbeit von Angelika Adensamer, Andreas Czák, Alina Hanel, Teresa Schwaninger und Levin Wotke entstanden.

Die Kapitelgruppe C (S. 127) widmet sich den Rechten der von Überwachung Betroffenen. Kapitel 9 von Marlene Kreil stellt einen umfangreichen Abriss der für polizeiliche Überwachung einschlägigen Judikatur zu dem Recht auf Achtung des Privat- und Familienlebens, dem Grundrecht auf Datenschutz, der Freiheit der Meinungsäußerung, der Versammlungsfreiheit und dem Recht auf ein faires Verfahren dar. In diese Analyse wurden sowohl das Staatsgrundgesetz (StGG), das Datenschutzgesetz (DSG), die Europäische Menschenrechtskonvention (EMRK), und die Grundrechtecharta (GRC) einbezogen, deren Verhältnis und Geltungsbereich zu Beginn des Kapitels erklärt werden. Um die Unterscheidung dieser verschiedenen Grundrechtsquellen zu erleichtern, führt ein Farbschema durch dieses Kapitel: die Texte der rein österreichischen Grundrechtsnormen, des StGG und des DSG sind rot, die der EMRK grün und die der GRC blau markiert, ebenso jeweils die Fallnotizen am Rand. Diese sind nur mit abgekürzten Namen zitiert und können im Fallverzeichnis am Ende des Kapitels nachgeschlagen werden. In Kapitel 10 von Angelika Adensamer wird ein Überblick über den Datenschutz im Polizeibereich geboten, der ein neben der Datenschutzgrundverordnung weniger beachteter Teil des neuen europäischen Datenschutzregimes ist.

In der Kapitelgruppe D (S. 169) beschäftigen wir uns schließlich mit der Evaluierung von Gesetzen. Kapitel 11 beginnt mit einer Beschreibung der Möglichkeiten zu vorparlamentarischer Partizipation am Gesetzgebungsprozess – dem Begutachtungsverfahren und dem Konsultationsmechanismus – von Erwin Ernst Steinhammer. Ausführlicher geht danach Christof Tschohl auf die gesetzlichen Regelungen zur Wirkungsorientierten Folgeabschätzung und die Datenschutz-Folgeabschätzung ein. In Kapitel 12 widmet sich Herbert Waloschek der Frage, wie der Gesetzgebungsprozess ziel- und ergebnisorientiert gestaltet werden kann. Abschließend werden in Kapitel 13 die gesammelten Erkenntnisse des Handbuchs in einer übersichtlichen Checkliste abgebildet, die zur Orientierung dienen soll, anhand welcher Fragen Überwachungsgesetze und -maßnahmen bewertet werden können.

Endnoten

1 *Lyon*, Surveillance as Social Sorting. Privacy, risk, and digital discrimination (2003).

2 1 Bvr 256/08 vom 02.03.2010, Rz 218. Vgl. auch *Bieker/Bremert/Hagendorff*, Die Überwachungs-Gesamtrechnung, oder: Es kann nicht sein, was nicht sein darf, in *Roßnagel et al.* (Hrsg.), Die Fortentwicklung des Datenschutzes (2018).

3 VfGH 11.12.2019, G 72-74/2019-48, G 181-182/2019-18, Rz 86.

4 HEAT – Handbuch zur Evaluation der Anti-Terror-Gesetze in Österreich 1.2 (2016). (https://epicenter.works/sites/default/files/heat_v1.2.pdf).

5 *Die neue Volkspartei/Die Grünen – Die Grüne Alternative*, Aus Verantwortung für Österreich. Regierungsprogramm 2020-2024 (2020). (https://gruene.at/themen/demokratie-verfassung/regierungsuebereinkommen-tuerkis-gruen/regierungsuebereinkommen.pdf)

Nützliche Hinweise für Leser_innen

- Dieses Buch soll als Handbuch dienen, weshalb wir uns bemüht haben, das Nachschlagen zu erleichtern.
- Die Kapitel stehen nebeneinander, es ist also nicht notwendig, sie in einer bestimmten Reihenfolge zu lesen, um den einzelnen Teilen folgen zu können.
- Es kann hilfreich sein, einzelne Begriffe parallel im Glossar nachzulesen. Verweise darauf sehen wie folgt aus:

🕮 *Host-Provider*

diese Seiten oder Dienste die IP-Adresse des_der Teilnehmer_in sowie der Zeitpunkt des Zugriffs durch den Host-Provider protokolliert und bei manchen

- Man kann den Begriffen auch an andere Stellen im Buch folgen, darauf weisen Kapitelverweise hin:

➲ *Verhältnismäßigkeit 9.1.3*

Es ist eine durch die Menschenrechte garantierte Voraussetzung, dass bei der Einführung von Überwachungsbefugnissen eine Einschätzung darüber zu treffen ist, ob

- Im zweiten Metakapitel (S. 51), das sich mit den einzelnen gesetzlichen Überwachungsbefugnissen beschäftigt, kann es hilfreich sein, das Überblickskapitel 4 als erstes zu lesen, da es die Grundlagen darlegt, die für die weiteren Kapitel 5 – 8 gelten.
- Schlagworte zu wichtigen Stellen sind ebenfalls am Rand zu finden.

Trefferquoten in der Massenüberwachung

Bei den 999.900 Unverdächtigen liegt das System also in 989.901 Fällen richtig, wenn es keinen Treffer anzeigt *(true negatives)*. Bei 9.999 der 999.900 Unverdächtigen

- Verweise auf Stellen im selben Kapitel finden sich direkt im Fließtext.

der Grundrechte und benennt die Grundrechtskataloge, die in Österreich gelten (siehe Kapitel 9.1.2).

- Die Gesetzesstellen, die am Rand des Fließtextes stehen, sind auch als Nachweise von wortwörtlichen Zitaten aus Gesetzestexten oder als Verweise dafür worauf Bezug genommen wird zu lesen.

Art. 4 Abs. 2 DSGVO

Eine Datenverarbeitung im Sinne der Datenschutz-Grundverordnung der EU (DSGVO) liegt dann vor, wenn Daten erhoben, erfasst, organisiert, geordnet,

- Englische Begriffe und Synonyme sind in *kursiv* gesetzt.
- Zum besseren Überblick haben wir in Kapiteln, die sich detailliert mit mehreren Gesetzen auseinander setzen, die jeweiligen Gesetze und dazugehörigen Fallbeispiele und Verweise farblich unterlegt. Das Farbschema ist dann im jeweiligen Kapitel ersichtlich.

Zur Übersichtlichkeit sind in diesem Kapitel verweise auf Fälle farblich gekennzeichnet. Es gibt folgende Kategorien von Verweisen und Hervorhebungen:
1. Bezug zur EMRK
3. Bezug zum StGG
2. Bezug zur GRC

Bestimmungen der EMRK können ebenfalls vom VfGH auslegt werden, da es sich dabei um österreichisches Verfassungsrecht handelt. Grundsätzlich folgt der VfGH aber der Rechtsanschauung des Gerichtshof für Menschenrechte (EGMR) in Straßburg. Der EGMR ist dem VfGH in Bezug auf die EMRK übergeordnet und kann daher von Betroffenen erst nach Ausschöpfung des innerstaatlichen Instanzenzugs angerufen werden.

- Am Ende des Handbuchs finden sich neben dem Glossar auch ein Abbildungverzeichnis, ein Rechtsmittelverzeichnis und Leseempfehlungen, um sich in das Thema zu vertiefen.Am Ende des Handbuchs finden sich neben dem Glossar auch ein
- Weitere Verweise und Informationen als Links, sowie Informationen zur Druckfassung dieses Buches finden sich auf der Webseite www.handbuch-ueberwachung.at

ÜBERWACHUNG UND GESELLSCHAFT

Freedoms we now take for granted
were often viewed as threatening
or even criminal by the past power
structure. Those changes might
never have happened if the
authorities had been able to achieve
social control through surveillance

Bruce Schneier

1. Überwachung aus sozialwissenschaftlicher Perspektive

1.1 Vorbemerkung: Ein sozialwissenschaftlicher Blick auf Überwachung

Überwachung ist in der politischen Diskussion über die von vielen Seiten diagnostizierte Bedrohung moderner Gesellschaften durch eine Vielzahl von Feindbildern ein zentraler Begriff geworden. Ausdifferenzierte Debatten über das Verhältnis von Freiheit und Sicherheit, über Notwendigkeit, Grenzen, Wirkungen und Nebenwirkungen verschiedener Überwachungsmaßnahmen befeuern politische und rechtspolitische Auseinandersetzungen. Tritt man von der aktuellen Diskussion ein Stück zurück, ergeben sich hier möglicherweise Anhaltspunkte für eine erweiterte Perspektive und eine Rationalisierung der Kontroversen. Daher wird im Folgenden eine sozialwissenschaftlich inspirierte und damit etwas distanzierte Auseinandersetzung mit dem Phänomen Überwachung vorgestellt. Ausgehend von eher konzeptuellen allgemeinen Überlegungen werden dann zentrale Elemente des aktuellen Überwachungsregimes, das sich mit erschreckender Geschwindigkeit in den modernen Rechtsstaat einschreibt und ihn immer mehr zum Überwachungsstaat macht, behandelt.
Betrachtet man Überwachung aus sozialwissenschaftlicher Perspektive, so übernimmt man eine Reihe von Vorannahmen begrifflicher und methodischer Natur. Begrifflich geht es darum, Überwachung als ein soziales und gesellschaftliches Phänomen zu erfassen. Es geht also um das Verhältnis von Überwacher_innen und Überwachten, um die sozialen Folgen und Funktionen von Überwachung. Methodisch analysieren Sozialwissenschaften die empirisch nachweisbaren Korrelationen oder Zusammenhänge zwischen Ursachen und Wirkungen. Letztlich stellt sich aus sozialwissenschaftlicher Perspektive immer auch die Frage nach möglichen größeren gesellschaftlichen Zusammenhängen, nach kulturellen, ökonomischen, historischen Entwicklungslinien, die ein beobachtbares Phänomen hervorbringen und prägen.

1.2 Einige konzeptionelle Grundlagen: Was ist Überwachung?

Befasst man sich mit Überwachung als sozialer Praxis und der dazu verfügbaren Literatur in den Sozialwissenschaften, so ist zunächst festzustellen, dass sich im sozialwissenschaftlichen Diskurs kaum brauchbare oder einheitliche Definitionen finden lassen.[1] Eindeutige Konzeptualisierungsversuche scheitern auch daran, dass dem Konzept Überwachung – wie David Lyon feststellt – eine gewisse Ambiguität inhärent ist.[2] Überwachung muss als ein vielschichtiges Phänomen begriffen werden, das einerseits Praktiken freiheitsbeschränkender sozialer Kontrolle umfasst, andererseits aber auch Ansprüche der Fürsorge verfolgen kann. Eltern überwachen ihre Kinder, Nachbar_innen überwachen sich gegenseitig und bei genauerem Hinsehen stellt sich heraus, dass Überwachen eine normale und in vielen Bereichen sinnvolle, soziale Praxis ist. Selbst der durchweg kritisch gesehene Einsatz von modernen Überwachungstechnologien,

kann ein freundliches Gesicht haben – man denke hierbei beispielsweise an den Bereich des sogenannten *Ambient Assisted Living* oder AAL[3], bei dem im Pflegebereich moderne Überwachungstechnologien zum Einsatz kommen um etwa alten und behinderten Menschen in ihrem Alltag behilflich zu sein.
Man muss diese Normalität von Überwachung als lokale soziale Praxis mitbedenken, wenn man das Wachstum neuer und als problematisch erachteter Formen von Überwachung verstehen will. Die freundliche, kulturell gewachsene, natürlich wirkende Art der Überwachung entwickelt sich in kleinen, überschaubaren, stabilen, sozialen Einheiten, in denen sich die Akteur_innen von Angesicht zu Angesicht gegenübertreten. In solchen Lebenswelten, im Dorf, der Familie, der Gemeinde, stellt sich eine Reihe von Fragen nicht, die wir uns heute stellen, wenn wir nach den Grenzen und Möglichkeiten von Überwachung in modernen Gesellschaften fragen. Das wird schnell deutlich, wenn man bspw. die Frage nach dem Verhältnis von Überwachung und Privatsphäre stellt. Dorfbewohner_innen haben als Mitglieder kleiner lokaler sozialer Einheiten keine nennenswerte Privatsphäre. Sie sind dem dauerhaften Blick der Anderen ausgesetzt, ebenso wie sie ihren Blick auf andere richten. Man beobachtet sich gegenseitig, weiß, mit wem man es zu tun hat, und realisiert schnell, wenn etwas Ungewöhnliches geschieht, das möglicherweise ein Eingreifen erfordert, um die gefährdete Ordnung wiederherzustellen.

Überwachung als soziale Praxis

Ändern sich die Lebensformen, ändern sich auch Formen und Praktiken der Überwachung. In historischer Perspektive ist das der Übergang von segmentierten einfachen Gesellschaften zu funktional differenzierten komplexen Gesellschaften, oder einfacher ausgedrückt vom Dorf zur Stadt. Ein wichtiges Merkmal dieser Veränderung ist der Übergang von einer im Wesentlichen horizontalen Form der Überwachung – die Bewohner des Dorfes überwachen sich gegenseitig und achten auf Einhaltung der Ordnung – zu einer vertikalen, formalisierten und hierarchisierten Form der Kontrolle. Das hat weitreichende Konsequenzen. Die Identität des_der Stadtbewohner_in und Staatsbürger_in stellt sich anders her, als die des_der Dorfbewohner_in. Die einen werden durch ihre Nachbar_innen identifiziert, die anderen durch Dokumente und Merkmale, die ihnen von einer mehr oder weniger fernen staatlichen Behörde zugewiesen werden. So kann man etwa die Geschichte der modernen Überwachungsregime entlang der Entstehung staatlicher Verwaltungssysteme, vom Finanzamt bis zu den Sozialbehörden, rekonstruieren. Die Frage „Wer bist du?“ wird in modernen, städtischen, mobilen, globalisierten Gesellschaften anders beantwortet werden müssen als im stabilen dörflichen (oder familiären) Rahmen. Tradition, persönliche Bekanntheit und Vertrauen werden ersetzt durch Ausweisdokumente, biometrische Merkmale, Sozialversicherungsnummern, die alle an eine zentrale Dokumentations- und Registrierungsstelle gebunden sind, die für jede_n Bürger_in über personenbezogene und die Person definierende Informationen verfügt.

Veränderung der Lebensformen

In grober Stilisierung kann man also sagen, dass soziale Ordnung sich nicht mehr über eine horizontale Praxis der handlungskoordinierenden Überwachung herstellt, sondern über die hierarchisierte und von staatlichen Behörden geschaffene Struktur von formalen, einheitlichen Identifizierungsmerkmalen. Soziale Identität wird zu behördlich vermittelter Identifizierung.
Diesen vielschichtigen historischen Übergang für sich genommen, könnte man nun konstatieren, dass soziale Ordnung in modernen Gesellschaften sich anders herstellt, dass nun jede_r mehr oder weniger leben kann, wie er oder sie will, und dass es, wenn man es mit staatlichen Behörden zu tun hat, genügt, sich entsprechend auszuweisen. Darüber hinaus ist die Privatsphäre der Bürger_innen zu respektieren, die weiterhin ihren alltäglichen Geschäften nachgehen, Verträge schließen, Verpflichtungen eingehen und ihr Leben im Rahmen der neu gewonnenen Freiheit nach den ihnen verfügbaren Möglichkeiten gestalten

Hierarchisierte, staatliche Strukturen

Wie sich allerdings zeigt, beschränkt sich die neue, durch staatliche Behörden vermittelte Form der Überwachung nicht auf diese minimale Funktion. Die Gründe hierfür sind vielschichtig und können an dieser Stelle nicht weiter ausgeführt werden. Es genügt die Beobachtung, dass mit dem Anwachsen der staatlichen Verwaltung, der Entwicklung und dem massiven Einsatz neuer

Dokumentations- und Identifizierungstechnologien sich neue Möglichkeiten ergeben und vermeintliche Notwendigkeiten entdeckt werden. Die Bürger_innen werden in ein immer dichteres und engeres Netz der Kontrolle eingebunden und verwandeln sich, wie David Lyon es einmal formuliert hat, in leckgeschlagene Datencontainer, die mit jedem Schritt, den sie tun, eine Datenspur hinterlassen, die gierig aufgesaugt wird – von staatlichen, wie privaten Datensammler_innen gleichermaßen.

Politische Theorie Oikodespot

Die Idee, als Bürger_in und Mensch eine individuelle, eigene Privatsphäre als eine gegen Übergriffe von außen zu verteidigende Sphäre, als Rechtsgut zu besitzen, entwickelt sich historisch erst vor dem Hintergrund dieser epochalen Transformationsprozesse. Noch in der klassischen politischen Theorie, wie sie etwa Hannah Arendt rekonstruiert, ist die Differenz zwischen dem privaten Oikos und der öffentlichen Sphäre der Agora mit eindeutigen normativen Wertungen belegt.[4] Der Oikodespot, der (männliche) Mensch als Privatperson in seinen vier Wänden wird erst dann, wenn er hinaustritt und seinesgleichen in der Sphäre der Öffentlichkeit gegenübertritt, zum voll entwickelten Individuum.

Das Private und das Öffentliche

Es bedarf der gleichgestellten Anderen, die ihn als Gleichen anerkennen, um zur voll entfalteten Person zu werden. Das Private ist das Defizitäre und der Mensch wird nicht als Individuum, sondern als genuin soziales Wesen verstanden, das im Angesicht der Anderen und nur durch sie zum Menschen wird. Hier ergibt sich ein Anschluss an die oben kurz skizzierte Form der horizontalen reziproken Überwachung, die normales Element eines aktiven Lebens in einer Gemeinschaft ist, die sich dadurch selbst reproduziert – oder wie man heute sagen würde: für ihre Sicherheit sorgt.

1.3 Staatliche Überwachung: Schutzmaßnahme oder Angriff auf die Freiheit

In Diskussionen über Privatsphäre und ihre Gefährdung durch Überwachungsmaßnahmen in modernen Gesellschaften muss diese soziale Dimension immer mitgedacht werden. Es geht auch bei einem modernen Überwachungsregime nicht nur um den isolierten Einzelnen, sondern um Menschen als soziale Wesen, um ihr Verhältnis zu anderen, ihr soziales Handeln. Hier liegt auch die Gefahr: Moderne techno-soziale Überwachungsregime erfassen durch die Beobachtung des_der Einzelnen im Namen der Sicherung der staatlich zu garantierenden Ordnung zugleich soziale Strukturen, Netzwerke, Kommunikationszusammenhänge. Auf einen einfachen Nenner gebracht, operiert die Idee einer staatlich vermittelten gesellschaftlichen Ordnung nach wie vor mit dem Idealbild der sich selbst transparenten kleinen (dörflichen) Gemeinschaft, allerdings im Bewusstsein der Tatsache, dass sich diese Ordnung nicht mehr spontan herstellt, sondern durch entsprechende Interventionen und Überwachungsmaßnahmen gesichert werden muss. Das Leitmotiv dieser Idee ist dabei nach wie vor die Konformität, die jetzt in der Form einer mehr oder weniger abstrakten Normalitätsfiktion auftritt. Während moderne Gesellschaften eine bisher nicht gekannte Heterogenität und Komplexität in kultureller und sozialer Hinsicht herausgebildet haben, basiert die Idee der staatlich vermittelten Ordnung auf der Annahme, dass einfache, stabile Klassifikationssysteme ausreichen, um solche Gesellschaften zu regieren. Zugleich wächst im Angesicht der für den staatlichen Blick – und tendenziell auch für die Bürger_innen – unübersichtlich gewordenen Gesellschaft der Wunsch nach ordnungssichernden Maßnahmen. Bei der Erfüllung dieses Wunsches steht das traditionelle Bild der sicheren, lokalen Gemeinde immer im Hintergrund. Die Welt, wie sie ist, erscheint vor diesem Hintergrund einerseits als tendenziell gefährlich und anderseits als bedroht und das rechtfertigt weitreichende Maßnahmen sie zu sichern.[5] Die propagierten Gefährdungen wechseln. Sie können in ihren jeweiligen Ausprägungen oder Erscheinungsformen nach zwei unterschiedlichen Mustern konstruiert werden. Einmal lässt sich die Gefährdung durch das Eindringen des Fremden und Unbekannten konstruieren. Der Fremde gilt als typische Figur, die die Ordnung bedroht.[6]

Herstellen von Ordnung

Konstruktion der Gefahr durch Fremde

Auf ihn hat sich besondere Aufmerksamkeit und weitreichende Überwachung zu richten. Das andere Muster operiert mit der Vorstellung der Selbstgefährdung, das heißt der Verunsicherung und dem Bewusstsein des alltäglichen Risikos. Mit dem Verlust des Vertrauens in die unmittelbare Lebenswelt und dem Verlust der ontologischen Sicherheit[7] und dem Verfall dessen, was Richard Sennett als öffentliche Umgangsformen analysiert hat[8], werden die Bürger_innen sich sozusagen selbst zur Quelle der Unsicherheit und Gefahr. Die Zunahme entsprechender Verunsicherungen, Störungen und Verstörungen lässt sich in modernen Gesellschaften diagnostizieren.[9] Das befördert dann u.a. Regime der Selbstoptimierung und Selbstüberwachung, der gesteigerten Risikowahrnehmung und letztlich auch der Bereitschaft, weitere Überwachungs- und Kontrollmaßnahmen in anderen Bereichen zu akzeptieren.

Schutz vor Selbstgefährdung

Macht man sich die hier kurz entwickelte Herangehensweise an das Phänomen Überwachung zu eigen, so wird deutlich, wie die Themen Sicherheit, Bedrohung, Überwachung und Privatsphäre in historischen und sozialen Prozessen an Form und Bedeutung gewinnen. Gleichzeitig ist damit aber noch nichts darüber ausgesagt, ob die aktuell wahrgenommenen Bedrohungen nun wirklich so bedrohlich sind, wie sie erscheinen[10], ob die in ihrem Angesicht vorgeschlagenen Maßnahmen der erweiterten Überwachung und die Forderung nach Aufgabe wohl erworbener und rechtlich garantierter Freiheitsrechte gerechtfertigt sind. Verlässt man nun die Ebene allgemeiner sozialwissenschaftlicher Analysen und wendet sich den aktuell in westlichen Gesellschaften erhobenen Forderungen nach mehr Überwachung im Angesicht steigender Bedrohungen zu, so kann man am konkreten Beispiel zeigen, wie Überwachungsmaßnahmen und Bedrohungen der Sicherheit zusammenhängen, wie sich dabei Kosten und Nutzen zueinander verhalten, welche Treiber für die Entwicklung zu immer technisch vermittelte Überwachung zu finden sind, welche Folgen und Nebenfolgen das für Gesellschaften haben kann, und wo Ansatzpunkte für eine fundierte Politik zu finden wären. Betrachten wir also im Folgenden das aktuell akute Beispiel für die Begründung von Überwachungsmaßnahmen im Namen der Sicherheit, die Bedrohung unserer Gesellschaften durch den Terrorismus.

Sicherheit durch mehr Überwachung

1.4 Terrorismus, Bedrohung und Überwachung

Terrorismus wird derzeit als eine der zentralen Bedrohungen unserer Gesellschaft verstanden und dient als Begründung für den Ausbau unterschiedlichster Überwachungsmaßnahmen. Zunächst erscheint es hier sinnvoll, den Begriff der Bedrohung zu differenzieren. Nimmt man die Wahrscheinlichkeit, dass man als Bürger_in westlicher Gesellschaften Opfer einer terroristisch motivierten Straftat wird, so ist die Bedrohung sehr gering. Würde man die Zahl der Opfer terroristischer Anschläge zum Maßstab nehmen, so verblassten sowohl die Angriffe auf die New Yorker Twin Towers als auch alle anderen prominenten Attacken im Vergleich zu den Todesfällen, die durch Verkehrsunfälle, medizinische Kunstfehler oder ungesunde Ernährung verursacht werden. Allerdings ist das nicht die einzige Form von Bedrohung, um die es hier geht. Die eigentliche Wirksamkeit terroristischer Anschläge bemisst sich nicht an der Zahl der unmittelbar betroffenen Opfer, sondern vielmehr an der Wirkung auf die Wahrnehmung der Bürger_innen, auf die politische Diskussion und die letztlich hervorgerufene Reaktion der staatlichen Behörden. Terrorismus zielt also auf symbolische Wirkungen.

Terrorismus

Attacken wie die von 9/11 in New York oder die aktuelleren Anschläge in Paris, Brüssel, Istanbul und Berlin waren insofern extrem wirksam oder erfolgreich, als sie nicht nur ganze Gesellschaften tiefgreifend verändert, sondern neue globale Konfliktherde befeuert haben, was wiederum den ideologisch-politischen Zielen der Terrorist_innen förderlich war. Die einfache Formel lautet hier: je stärker die Reaktion des Staates auf terroristische Aktionen, desto erfolgreicher die Strategie der Terrorist_innen. Das führt zu folgendem Dilemma: Je stärker ein Staat oder eine Gesellschaft reagieren, je mehr mit dem Kampf gegen den Terror begründete politische

Maßnahmen ergriffen werden, je größer die mediale Aufmerksamkeit und Erregung über einen terroristischen Anschlag, desto besser für die terroristischen Akteur_innen.

Betrachtete man Terrorismus wie jede andere Form der Kriminalität, die es zu bekämpfen und nach Möglichkeit schon durch entsprechende Maßnahmen im Vorfeld zu verhindern gilt, so müsste man davon kein besonderes Aufheben machen. Terroristische Anschläge sind selten, die Wahrscheinlichkeit Opfer zu werden gering und die Möglichkeiten solche Taten mit polizeilichen Mitteln oder vermehrte Überwachung zu verhindern sehr begrenzt. Dennoch gibt es seit den Anschlägen von 2001 in New York eine mehr oder weniger unkontrollierte Zunahme an technisch vermittelten Überwachungsmaßnahmen. „Trotz kaum vorhandener Kenntnisse hinsichtlich ihrer Wirksamkeit haben politische Entscheidungsträger seit dem 11. September 2001 weltweit eine nahezu unüberschaubare Fülle von Maßnahmen beschlossen und dadurch die Sicherheitsbehörden mit neuen, oftmals bereits weit im Vorfeld strafbarer Aktivitäten einsetzenden Kontroll- und Überwachungsbefugnissen ausgestattet.“[11]

Ausweitung von Überwachung

Nicht nur scheint der Politik eine rationale Strategie abzugehen, viele der ergriffenen Maßnahmen sind reaktiv und von einer erstaunlichen forensischen Schlichtheit. Betrachtet man die terroristischen Anschläge der Vergangenheit, so zeigt sich, dass nach jedem dieser Anschläge (oder Versuche) gezielt Maßnahmen ergriffen wurden, die gleichartige Aktionen in Zukunft vermeiden helfen sollen. So wurden nach 9/11 die Cockpits von Verkehrsflugzeugen mit entsprechenden technischen Maßnahmen abgesichert; nach dem Versuch, flüssigen Sprengstoff an Bord eines Flugzeugs zu schmuggeln, wurde die Mitnahme von Flüssigkeiten im Handgepäck untersagt und als der sogenannte „Schuhbomber“ den Versuch unternahm, durch in seiner Schuhsohle geschmuggelten Sprengstoff ein Flugzeug zum Absturz zu bringen, wurden die Schuhe der Flugpassagier_innen in die Kontrolle beim Check-In miteinbezogen.

Kontraproduktive Maßnahmen

Gleichzeitig sind viele Maßnahmen offensichtlich kontraproduktiv. Wenn etwa Angehörige vermeintlich verdächtiger Gruppen verstärkt ins Visier der präventiven Fahndung geraten, leistet das einer ethnischen Kollektivstigmatisierung und tendenziell auch der Radikalisierung in diesen Gruppen Vorschub. Wenn durch ungebremsten Ausbau der Datensammlung und Überwachung die Identifikation der sprichwörtlichen Nadel im immer größeren Heuhaufen unmöglich wird, ist das ebenso kontraproduktiv. Parallel dazu werden für alle diese Maßnahmen kontinuierlich die entsprechenden rechtlichen Grundlagen angepasst oder neu geschaffen.

Es gibt in der kritischen politik- und sozialwissenschaftlichen Sicherheitsforschung eine Vielzahl von Belegen für die mangelnde Wirksamkeit von Überwachungsmaßnahmen, für die damit einhergehenden kontraproduktiven Wirkungen, die verschiedenen Kosten – mit einem Wort, eine an erkennbaren Kriterien der Rationalität orientierte Politik könnte sich bei der Reaktion auf den Terrorismus eines anderen Ansatzes bedienen.[12] Gleichzeitig lässt sich zeigen, dass die zunehmende im Namen der Terrorismusbekämpfung ausgebaute Überwachung das Wachstum eines sicherheitspolitisch-industriellen Komplex befördert.[13]

Neben diesen an aktuellen Zahlen und Befunden ablesbaren Problemen fördert eine politische Strategie, die im Wesentlichen auf technologische Überwachungsmaßnahmen zur Erhöhung der Sicherheit setzt, gesellschaftliche Entwicklungen, die den konstitutiven Grundideen moderner rechtsstaatlich verfasster Demokratien entgegenstehen, bzw. ist in diese eingebettet.

Mangelnde Wirksamkeit von Überwachungsmaßnahmen

Erweist sich der Ausbau von staatlich eingesetzter Überwachungstechnologie, gestützt durch eine Entbindung der Exekutive von präzisen rechtlichen Vorgaben wie etwa der Unschuldsvermutung als offensichtlich ungeeignet, stellt sich die Frage, warum die Strategie der Überwachung kontinuierlich und großflächig in allen westlichen Gesellschaften ausgebaut wird.

Sicherheitspolitisch-indrustrieller Komplex

Hier kann man verschiedene Interpretationen ins Feld führen. Der Verweis auf den oben erwähnten sicherheitspolitisch-industriellen Komplex ist eine Möglichkeit der Erklärung. Die enge Verbindung von Politik und Industrie, wie sie aus den USA bekannt und in Europa zusehends auch zu beobachten ist, leistet einer Politik Vorschub, die auf den Einsatz von Technologien setzt, die von den einschlägigen Unternehmen angeboten werden, nachdem sie zuvor meist mit öffentlichen Mitteln im Rahmen sogenannter Sicherheitsforschungsprogramme entwickelt wurden.

➲ *Einsatz von Technologien 3.3*

Eine andere Interpretation sieht als wesentlichen Treiber dieser Politik die interne Dynamik des politischen Prozesses. Politisch verantwortliche Akteur_innen stehen im Angesicht medial verstärkter Bedrohungen der Sicherheit unter dem Druck, Handlungsfähigkeit zu beweisen und entsprechende Maßnahmen vorzuschlagen und umzusetzen. Die Erweiterung von Überwachungsmaßnahmen nach dem Motto *more of the same* erscheint da als eine wohlfeile Lösung – unabhängig von der Frage, ob dieses Mehr an Überwachung auch ein Mehr an Sicherheit bedeutet. Hier kommt eine als „Politik mit der Angst“ analysierte Strategie zum Einsatz[14], die sich der Loyalität der Bürger_innen nur mehr über das Versprechen, Böses abzuwenden, versichern kann. In Zeiten der seit langem schwelenden fiskalischen Krise und enger werdender staatlicher Handlungsspielräume[15] greift dieses Politikmodell immer weiter um sich und fördert damit den Ausbau des staatlichen Überwachungsregimes.

Politik mit der Angst

Mit dieser Entwicklung geht zudem eine deutliche Verschiebung in der Balance des institutionellen politischen Gefüges einher, die als Kolonisierung des Rechts durch exekutivisches Sicherheitsdenken beschrieben worden ist.[16] Rechtsstaatliche Grundsätze werden im Angesicht von vermeintlichen Bedrohungsszenarien auf den Prüfstand und zur Disposition gestellt.

Der faktische Ausbau von Überwachungsmaßnahmen und der damit komplementär einhergehende Abbau von rechtlichen Garantien im Namen vermeintlich unabdingbarer Sicherheitserfordernisse leisten einer Entwicklung Vorschub, die in der Literatur als „chilling effect“ analysiert worden ist.[17] Die für das zivilgesellschaftliche politische Engagement erforderliche Unbekümmertheit, die es den Bürger_innen erlaubt, unkontrolliert und ohne Überwachung ihre (politische) Kommunikation zu gestalten, Meinungen zu bilden, Mehrheiten zu sammeln, Pläne zu schmieden, geht verloren, wenn sich das Bewusstsein breit macht, dass jede Äußerung überwacht, dokumentiert und später gegen einen verwendet werden kann. Hier zeigt sich die wichtige politisch-soziale Dimension der Idee einer rechtlich zu schützenden Privatsphäre als Grundlage einer funktionierenden Demokratie.

➲ *chilling effect 9.3*

Es ist möglicherweise eine Ironie der Geschichte, dass staatliche Strategien, die im Namen des Kampfs gegen den Terrorismus auf einen ungebremsten Ausbau eines im Geheimen operierenden und der demokratischen Kontrolle entzogenen Überwachungsregimes setzen, bei einer wachsenden Zahl von Bürger_innen, die mit dieser Politik geschützt werden sollen, selbst terroristische Effekte erzeugt: die Angst, immer und überall Opfer von staatlichen Angriffen auf die eigene Privatsphäre zu werden, wobei das reale und das gefühlte Risiko hier (noch) immer so weit auseinanderliegen wie bei den Anschlägen, die zu verhindern diese Politik der Überwachung vorgibt.

Überwachung schafft selbst terroristische Effekte

Endnoten

1 Vgl. Kreissl, R. et al. (2015). Surveillance. Preventing and detecting crime and terrorism. In: D. Wright, & R. Kreissl (Hg.), *Surveillance in Europe.* London, New York: Routledge, S. 155.
2 Vgl. Lyon, D. (2007). *Surveillance Studies: An overview.* Cambridge: Polity Press, S. 14.
3 Vgl. Kreissl, R. et al. (2015). S. 155.
4 Vgl. Arendt, H. (2003). *Was ist Politik?* München: Piper.
5 Siehe McNamara, L., & Quilter, J. (2016). The 'bikie effect' and other forms of demonisation: The origins and effects of hyper-criminalisation. *Law in Context,* 34/2, S. 5.
6 Siehe Simmel, G. (1987). *Der Fremde. Das individuelle Gesetz–Philosophische Exkurse,* Frankfurt am Main: Suhrkamp.
7 Siehe Giddens, A. (2013). *The consequences of modernity.* New York: John Wiley & Sons.
8 Vgl. Sennett, R. (1992). *The fall of public man.* New York: W.W. Norton & Company.
9 Siehe Lasch, C. (1995). *Das Zeitalter des Narzißmus.* Hamburg: Hoffmann und Campe.
10 Siehe Pinker, S. (2011). *The better angels of our nature: The decline of violence in history and its causes.* New York: Viking.
11 Hegemann, H., & Kahl, M. (2016). Konstruktionen und Vorstellungen von Wirklichkeit in der Antiterror-Politik: Eine kritische Betrachtung. In: S. Fischer, & C. Masala (Hg.), *Innere Sicherheit nach 9/11. Sicherheitsbedrohungen und (immer) neue Sicherheitsmaßnahmen?* Wiesbaden: Springer, S. 110.
12 Siehe Mueller, J. E., & Stewart, M. G. (2015). *Chasing ghosts: The policing of terrorism.* Oxford University Press.
13 Siehe Hayes, B., Rowlands, M., & Buxton, N. (2009). *Neoconopticon: The EU security-industrial complex.* Transnational institute.
14 Vgl. Furedi, F. (2005). *Politics of fear.* New York: Bloomsbury.
15 Vgl. O'Connor, J. (1979). *The fiscal crisis of the state.* Transaction Publishers.
16 Vgl. Albrecht, P. A. (2007). Das nach-präventive Strafrecht: Abschied vom Recht. In: U. Neumann (Hg.), *Jenseits des rechtsstaatlichen Strafrechts.* Frankfurt am Main: Peter Lang, S. 3-26.
17 Vgl. Sidhu, D. S. (2007). The chilling effect of government surveillance programs on the use of the internet by Muslim-Americans. *University of Maryland Law Journal of Race, Religion, Gender and Class,* S. 375.

2 Österreichs polizeiliche Überwachungsbefugnisse im Zeitraffer

„Regierungen kommen und gehen, was bleibt ist die Staatspolizei“, schrieb Matthäus Zinner vor 31 Jahren in der Nullnummer der kritischen Zeitschrift für Rechtswissenschaft juridikum unter dem Titel „Wer kontrolliert die Kontrollore?“.[1] Im Jahr 1852 entstand mit kaiserlichem Beschluss die oberste Polizeibehörde, eine dem Kaiser direkt unterstellte polizeiliche Zentralstelle. Ihr Leiter war Gendarmeriechef Johann Freiherr Kempen von Fichtenstamm, der auch den geheimen Ausforschungsdienst sowie ein Netz aus Geheimagenten und Konfidenten aufbaute.[2]

Konfidenten

Die Geheimagenten und Konfidenten gibt es noch heute. Die Befugnisse der Polizei sowie die Rechte der Bevölkerung aber haben sich über die Jahrhunderte verändert. Verändert haben sich auch die technischen Möglichkeiten der Behörden, die Bevölkerung zu erfassen und zu überwachen. In diesem Kapitel wird ein Überblick der jüngsten Geschichte der Überwachung in Österreich gegeben.

Seit jeher sind die Befugnisse der Polizei in den meisten Staaten von politischen Entwicklungen innenpolitischer als auch weltpolitischer Natur geprägt: Die Geschehnisse um die französische Revolution ließen auch in Österreich die Geheimdienste und die politische Polizei entstehen. „Dem Zusammenbruch des Metternich’schen Polizeistaates folgten die Bach’sche Polizeireform von 1850 und, mit einer gewissen Verzögerung, die Grundrechte von 1862 und 1867, die ihrem Ziel und Inhalt nach in erster Linie gegen polizeiliche Übergriffe gerichtet waren“, schrieb der Rechtswissenschafter Benjamin Davy 1993.[3] Und wohl war es kein Zufall, dass dem Justizpalastbrand eine Zentralisierung der Sicherheitspolizei beim Bund durch die Verfassungsnovelle 1929 folgte.

2.1 Sicherheitspolizeigesetz 1991

Neue polizeiliche Befugnisse, lascher Datenschutz, Legalisierung verdeckter Polizei

Es war die zunehmende Kritik an gewalttätigen Polizeieinsätzen und an Aktivitäten der Staatspolizei, die den Ausschlag für das erste Sicherheitspolizeigesetz (SPG) gab. Schon seit 1969 debattiert, wurde schließlich im Oktober 1991 ein neues, übersichtliches Kompendium der polizeilichen Befugnisse beschlossen. Dem gingen heftige Debatten über seinen Inhalt voraus: „Hausdurchsuchungen ohne richterlichen Durchsuchungsbefehl, faktische Einführung der generellen Ausweispflicht, unkontrollierbare Erfassung und automationsunterstützte Vernetzung personenbezogener Daten, ein Verordnungsrecht, womit die Polizei insbesondere gegen UmweltaktivistInnen und Streikende vorgehen könnte, Legalisierung der Staatspolizei und anderer verdeckt agierender Sondereinheiten, das gegen gesellschaftliche Randgruppen gerichtete Wegweiserecht“, listete Thomas Sperlich die nicht enden wollenden zivilgesellschaftlichen und juristischen Bedenken an dem Gesetz in der Zeitschrift juridikum auf.[4] Kleine Abänderungen konnten die Kritiker_innen durchsetzen, insbesondere die „Lex Karlsplatz“, das Wegweiserecht, wurde gestrichen. Damit entledigte man sich zwar des populärsten Zankapfels, die Parlamentsdiskussion zum SPG zeigte jedoch genügend weitere problematische Punkte der Regelung auf: In gewohnt populistischer Manier kritisierte etwa Grünen-Abgeordneter Peter Pilz das SPG. Es sei das „Sicherheitspolizeigesetz der Festung Europa!“.[5] Insbesondere die Abschnitte zur personenbezogenen Datenübermittlung machten ihm Sorgen. Diese wurde erlaubt, „wenn […] zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich“.[6] Den Grünen zufolge sei damit der grenzüberschreitende Datenverkehr „aus rein technischen Gründen fast nicht mehr kontrollierbar“.[7]

Wegweiserecht

Einig waren sich die Oppositions- und Regierungsparteien ÖVP und SPÖ, dass es positiv sei, die Staatspolizei (heute: Bundesamt für Verfassungsschutz und Terrorismusbekämpfung) und die militärischen Nachrichtendienste mit dem SPG erstmals unter parlamentarische Kontrolle zu stellen.

Seine erste Bewährungsprobe hatte das im Mai 1993 in Kraft getretene Gesetz schon ein Monat später, als eine Baustellenblockade von Umweltschützer_innen an der geplanten Enns-Schnellstrasse (Enns-Trasse) polizeilich aufgelöst wurde. Von den Beamt_innen zeigte kein_e einzige_r den fordernden Aktivist_innen die Dienstnummer vor, obwohl neuerdings gesetzlich vorgegeben. Zudem ließen Beamt_innen einen Mitarbeiter der blockierten Baufirma die Daten der beamtshandelten Demonstrierenden mitnotieren[8] – Datenschutz sieht anders aus.

2.2 Der große Lauschangriff 1997

Die Russenmafia, polnische Autodiebe, türkische Jugendbanden, arabische Terroristen und afrikanische Drogendealer – das Bild vom vernetzten, kriminellen Migranten wurde in den 1990ern medial verbreitet und dieser politisch zum Sicherheitsrisiko erklärt. 1992 wurde die „polizeiliche Einsatzgruppe zur Bekämpfung der Organisierten Kriminalität“ (EDOK) ins Leben gerufen. Dennoch stieg dem Justizministerium zufolge der Anteil an Straftaten durch organisierte Kriminalität im Jahr 1996 an. In diesem Klima wurden 1997 in der Strafprozessordnung besondere Ermittlungsmaßnahmen zur Bekämpfung organisierter Kriminalität verankert. Insbesondere wurde die „optische und akustische Überwachung von Personen unter Verwendung technischer Mittel“, sowie der Große Lauschangriff – versteckte Mikrofone und Kameras in Innenräumen – eingeführt. Ab sofort mussten „besonderen Ermittlungsmaßnahmen“ von Rechtsschutzbeauftragten genehmigt werden.[9] Der Grundstein für den Lauschangriff war schon Jahre zuvor gelegt worden: 1993 waren die Tatbestände der „kriminellen Organisation“ (§ 278a StGB) sowie der „terroristischen Vereinigung“ (§ 278b StGB) geschaffen worden.

Großer Lauschangriff

Im Jahr 1999 fand schließlich der Große Lauschangriff seine erste Anwendung. Der nigerianische Staatsbürger Marcus Omofuma erstickte am ersten Mai aufgrund polizeilicher Zwangsmaßnahmen bei seiner Abschiebung nach Sofia im Flugzeug. Es folgten Proteste der afrikanischen Community gegen behördlichen Rassismus. Die Reaktion: die größte kriminalpolizeiliche Aktion der zweiten Republik. Im Mai 1999 wurden 127 Menschen aus der afrikanischen Community als Drogendealer_innen-Netzwerk festgenommen, auf Basis fragwürdiger Ergebnisse des ersten Großen Lauschangriffs Österreichs. Dutzende Schwarze wurden als vermeintliche Drogendealer_innen oder Drogenbosse verurteilt, allen voran zentrale Organisator_innen der antirassistischen Proteste.[10] Die den Verurteilungen zugrundeliegenden Beweise werden bis heute massiv in Zweifel gezogen, Betroffene und ihre Anwält_innen sprachen von erfundenen Beweisen. Emmanuel Chukwujekwu, einer der Betroffenen, kommentierte in der Zeitung Augustin: „Es war kein Krieg gegen Drogen, es war ein Krieg gegen die Black Community in Wien. Unvorstellbar, dass so etwas in einem zivilisierten Land wie Österreich passiert.“[11]

Mai 1999 Festnahme von 127 Menschen i. Zuge d. ersten großen Lauschangriffs

Einst für die Fahndung nach der militanten linken RAF geschaffen, sollten mittels Rasterfahndung in Österreich rechte Terrorist_innen ausfindig gemacht werden. Dem Handbuch des Polizeirechts zufolge ist die Rasterfahndung eine „Massendatenverarbeitung, bei der automatisiert Informationen aus Fremdda-

Rasterfahndung

tenbeständen mit anderen Datenbeständen abgeglichen werden, um bestimmte Personen zu ermitteln“.[12] Anlassfall war eine Briefbombenserie Rechtsextremer, die seit 1993 vier Todesopfer und 15 schwer Verletzte zur Folge hatte. Trotz breiter Kritik trat die Maßnahme 1997 in Kraft, konnte aber zur Ergreifung des Bombenbauers Franz Fuchs keinen Beitrag leisten. Der Briefbombenterrorist wurde bei einer zufälligen Autokontrolle der Polizei festgenommen.[13]
Zudem wird den Berichten über den Einsatz der besonderen Ermittlungsmaßnahmen des Justizministeriums zufolge diese Maßnahme bis heute kaum genutzt.[14] Die Abgeordnete des Liberalen Forums Heide Schmidt kritisierte vor Einführung der Rasterfahndung, dass Daten von Versandhäusern, Vereinen, Videotheken und Zeitungsverlagen durch die Polizei genutzt werden könnten.[15] Dem Kriminalsoziologen Reinhard Kreissl zufolge habe man mit dem Gesetz „den Polizeistaat in der Schublade“.[16]

➲ *5. Verdeckte Ermittlung*

Mit Einführung des Sicherheitspolizeigesetzes 1991 wurde es nun auch möglich, gefälschte Urkunden für verdeckte Ermittler_innen – die eingangs erwähnten Konfident_innen – zu erstellen. Somit konnten erstmals durch Behörden Urkunden generiert werden, die „über die Identität eines Menschen täuschen“.[17]

2.3 Erweiterte Gefahrenerforschung 2000

„Wer Vertrauen hat, der wird mit ruhigem Gewissen ja zu diesem Gesetz sagen. Jene, die präventiv Ängste schüren wollen, die werden nicht zustimmen“, sagte Sicherheitssprecher Paul Kiss im Ausschuss für Innere Angelegenheiten am 23.05.2000.[18] Die Grünen hingegen warnten vor „Gesinnungsobservierung“. Zur Diskussion stand eine weitere Novelle des Sicherheitspolizeigesetzes. Wenig später wurde damit unter anderem die erweiterte Gefahrenerforschung gesetzlich verankert: eine Maßnahme, um verdächtigte Gruppen unter Beobachtung zu stellen, noch bevor sie im Verdacht stehen, konkrete Straftaten begangen zu haben. Karl Schlögl von der SPÖ zufolge sei dieser nur ein „zahnloser Tiger“, Helene Partik-Pablé von der FPÖ hingegen fand in dem Gesetz eine „absolute Garantie gegen Missbrauch.“[19]
Nicht von ungefähr war die Einführung dieser Ermittlungsbefugnis umstritten. Seit Inkrafttreten der Änderung im Oktober 2000 ist die Polizei angehalten, „Gruppierungen“ zu beobachten, aus deren Umfeld mit Kriminalität zu rechnen ist, bzw. die eine „schwere Gefahr für die öffentliche Sicherheit“ darstellen; „insbesondere zu weltanschaulich oder religiös motivierter Gewalt“, so der schwammige Wortlaut im Gesetz. Seien keine „sofortigen Ermittlungen zur Abwehr schwerer Gefahr“ erforderlich, so müsse ein neu eingesetzter Rechtsschutzbeauftragter einbezogen werden.[20]

Gesetzlich vorgesehene Beobachtung von Gruppen aus vermutet kriminellem Umfeld

2.4 Vermummungsverbot 2002

Vermummungsverbot vs. Recht auf Anonymität

Keine zwei Jahre später, am 3. Juli 2002, tagte der Innenausschuss. Am Plan stand eine Diskussion des von ÖVP und FPÖ geforderten Verbots der Vermummung bei Versammlungen. Für und Wider des Vorschlags wurden diskutiert. Franz Höpfel vom Institut für Strafrecht der Universität Wien vertrat die Rechtsmeinung, dass vor Begehen eines Deliktes ein Recht auf Anonymität bestehe. Die Grünen machten geltend, dass es viele gute Gründe gäbe, sich zu vermummen, wie etwa für „Mitarbeiter_innen, deren Betriebe aus geschäftlichem Interesse die Teilnahme an Demonstrationen untersagen“ oder Menschen, welche „polizeiliche Überwachungen fürchten, wie KritikerInnen der Regierung, die eine Beschäftigung im öffentlichen Dienst haben oder anstreben“.[21] Die FPÖ war der Meinung, Gewalttätigkeiten hätten die letzten beiden Jahre bei Demonstrationen überhand genommen. Beamte aus Deutschland berichteten von ihren Erfahrungen mit dem dort bestehenden Vermummungsverbot, die Wiener Einsatzgruppe Alarm plädierte für ein solches.[22]

Wenige Tage nach dem Hearing wurde das Gesetz beschlossen. Demzufolge ist es Menschen verboten, an Versammlungen teilzunehmen, wenn sie „Gesichtszüge durch Kleidung oder andere Gegenstände allein zu dem Zweck verhüllen oder verbergen, ihre Wiedererkennung im Zusammenhang mit der Versammlung zu verhindern“ oder wenn sie „Gegenstände mit sich führen, die ihrem Wesen nach dazu bestimmt sind, die Feststellung der Identität zu verhindern“.[23]

Im selben Jahr entstand das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT), ebenso wie seine neun Landesämter (LVT). Im BVT wurden die Staatspolizei, die Einsatzgruppe zur Bekämpfung des Terrorismus (EBT) und die Einsatzgruppe zur Bekämpfung der organisierten Kriminalität (EDOK) zusammengeführt.[24]

2.5 Videoüberwachung 2004

Bei einer Tagung mit dem Titel „Videoüberwachung zu sicherheits- und kriminalpolizeilichen Zwecken“ im Juni 2004 schwor sich das Innenministerium auf den überaus großen Nutzen der Videoüberwachung im öffentlichen Raum ein. Demzufolge seien 2004 rund 160.000 Kameras zur Videoüberwachung im Einsatz gewesen, zum Großteil im privatwirtschaftlichen Bereich (Banken, Postämtern, Casinos…). „Nur 1.200 Kameras“ seien in behördlicher Verwendung gewesen, so ein Bericht in der BMI-Zeitung Öffentliche Sicherheit: „Die Kameras erfüllen nicht nur Überwachungsfunktionen, sondern tragen auch zu einer Steigerung des Sicherheitsgefühls der Bevölkerung bei.“[25]
Die daraufhin folgende Sicherheitspolizeigesetz-Novelle 2004 brachte nicht nur eine Zusammenlegung von Gendarmerie und Polizei zur Bundespolizei, sondern auch die Videoüberwachung an öffentlichen Orten, an sogenannten Kriminalitätsbrennpunkten. Eingeführt wurde auch die Videoüberwachung bei Grenzkontrollen sowie die KFZ-Kennzeichenerkennung in bestimmten Fällen. Einig waren sich ÖVP und FPÖ: Dank dem neuen Gesetz sei die Exekutive „fit für das 21. Jahrhundert“.[26]

Grenzkontrollen, KFZ-Kennzeichenerkennung

2.6 Ausweitung Bild- und Tonaufzeichnungen 2006

Kaum mehr als ein Jahr zog ins Land und eine weitere Ausweitung der Überwachungsbefugnisse wurde als Novelle des Sicherheitspolizeigesetzes im November 2005 eingebracht. Anlässlich von Sportgroßveranstaltungen wurde die Möglichkeit der zentralen Speicherung von sogenannten Gewalttätern geschaffen – die „Hooligan-Kartei“. Da Österreich und der Schweiz 2008 die Fußball-Europameisterschaft bevorstand, bezog sich das Gesetz auch auf „ausländische gewaltbereite Fans“. Ähnlich wie im europäischen Ausland wurde es möglich, „Gefährder“ durch die Behörden im Vorfeld zu kontaktieren. Man versprach sich damit, die „potentiellen Gewalttäter“ durch „persönliche Ansprache und Belehrung für rechtskonformes Verhalten bei Sportgroßveranstaltungen zu sensibilisieren“.[27]
Eine weitere Neuheit im Gesetz: die Verankerung der Software „Sicherheitsmonitor“. Das Arbeitsinstrument ermögliche es, „die tägliche und stündliche Kriminalitätsentwicklung zu diagnostizieren“, so das Bundeskriminalamt. Einer Presseerklärung des Bundeskriminalamts zufolge würden „noch nicht verifizierte Verdachtsmomente sofort in das System eingespeist, um möglichen Serientaten täglich oder stündlich mit operativen Maßnahmen gegenzusteuern“.[28] Einzig die Grünen stimmten aus datenschutzrechtlichen Bedenken gegen den Vorschlag. Mit Jahresbeginn 2006 trat die Novelle in Kraft.

Sportgroßveranstaltungen, „Hooligan- Kartei“

Software „Sicherheitsmonitor“ zur Kriminalitätsentwicklungsdiagnose

2.7 Ausweitung erweiterte Gefahrenerforschung 2012

„Anti-Terror-Paket“, Peilsender und Handyortung

Der Direktor des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT) Peter Gridling betonte mit Verweis auf den Verfassungsschutzbericht in den Medien: „Extremismus und Terrorismus stellen für die österreichische Demokratie im Moment keine ernsthafte Bedrohung dar.“[29] In einem Expertenhearing zum dennoch initiierten „Anti-Terror-Paket“ nannte Gridling aber den rechtsextremen Terrorakt vom Juli 2011 in Norwegen als Anlass für eine weitere Verschärfung des Sicherheitspolizeigesetzes.[30] Bei dem Anschlag in Norwegen waren 77 Menschen durch den Rechtsextremen Anders Breivik ermordet worden.
Eine „Stärkung der Terrorismusprävention“ sei das zentrale Anliegen, und dieses solle mit einer Ausweitung der erweiterten Gefahrenerforschung sowie der Anwendung von „technischen Mitteln“ für die Observation erreicht werden.[31] Konkret wurde mit dem Gesetz die erweiterte Gefahrenerforschung auf das Beobachten von Einzelpersonen ausgeweitet. Der gesetzlichen Regelung vom Jahr 2000 zufolge war dies nur bei Gruppen von Verdächtigen möglich. Doch da die Sicherheitsbehörden „immer öfter die Erfahrung [machten], dass sich Einzelne aus unterschiedlichen Beweggründen selbst radikalisieren“ sei die Beschränkung auf eine Gruppe widersinnig, so die Erklärung zur Regierungsvorlage. Darüber hinaus wurde der Einsatz von Peilsendern auf Autos Verdächtigter sowie die Handy-Ortung zur Unterstützung von Observationen erlaubt. Besonders umstritten aber beschlossen wurde die Ortung der Handys von Begleitpersonen. Argumentiert als „Abwehr einer gegenwärtigen Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen“ wolle man damit im Sinn der Hilfeleistungspflicht „eine bestehende gesetzliche Lücke schließen“. Das in der Regierungsvorlage besonders hervorgestrichene Szenario der „Selbstmordgefahr bei einem Jugendlichen“ dürfte aber wohl kaum das übliche Anwendungsgebiet der neuen Befugnisse sein.[32]
Laut der Kriminalsoziologin Andrea Kretschmann handelte es sich bei der Gesetzesinitiative um einen Entwurf, der „in fast identischer Form bereits ein Jahr zuvor vorgelegt, aber aufgrund von Grundrechtsbedenken abgelehnt worden war“.[33] Die Debatte um das Sicherheitspaket polarisierte zwischen „Sicherheit“ und der „Aushöhlung bürgerlicher Freiheiten“. Heinz Patzelt von Amnesty International kritisierte den Gesetzesentwurf in einem Expert_innenhearing ob seiner „schwammigen Formulierungen, die viel zu weite Handlungsspielräume zuließen“.[34] Auch die Vizepräsidentin der Rechtsanwaltskammer Wien, Elisabeth Rech, sprach sich dagegen aus, „Bürgerrechte unter dem Titel ‚Kampf gegen den Terror‘ immer weiter einzuschränken“.[35]
Die Gesetzesnovelle trat mit Anfang 2012 in Kraft, der Grünen-Abgeordnete Albert Steinhauser kommentierte den Beschluss bei der Abstimmung: „Der Nationalrat stellt heute eine Lizenz zum Spitzeln aus.“[36]

2.8 Vorratsdatenspeicherung ca. 2010-2014

Vorratsdatenspeicherung wegen Grundrechtsverletzung gekippt

Anlasslose Massenüberwachung könnte man sie auch nennen: die Verpflichtung der Netzbetreiber_innen, Verbindungsdaten aus allen Telefon- und Internetverbindungen sechs Monate lang zu speichern. Auf gerichtliche Anordnung, bei Verdacht einer schweren Straftat, müssen die Daten den Strafverfolgungsbehörden übergeben werden, so die damalige EU-Vorgabe. Auf EU-Ebene war es das kürzeste Gesetzgebungsverfahren seit Bestehen der Union, in Österreich zog sich die juristische Auseinandersetzung um die Umsetzung der Vorratsdatenspeicherung dafür mehrere Jahre. Während eine Evaluierung des Ludwig Boltzmann Instituts für Menschenrechte zum Schluss kam, die EU-Richtlinie könne nicht ohne Grundrechtsverletzung umgesetzt werden, beschloss der Nationalrat 2011 die Regelung auf nationaler Ebene dennoch. Ein Jahr später trat sie in Kraft. Kampagnen, Petitionen, eine Bürger_inneninitiative und die NGO AKVorrat, aus der später epicenter.works hervorging, setzten im Vorfeld alles daran, das Gesetz zu verhindern. Ursprünglich als Anti-Terror-Maßnahme gedacht, wurden die gespeicherten Vorratsdaten im ersten Jahr überwiegend für Bagatelldelikte von Ermittlungsbehörden abgefragt.
Der AKVorrat brachte zusammen mit den Grünen eine Verfassungsklage ein, die zum Europäischen Gerichtshof weitergereicht wurde.[37] Dort befand man die EU-Richtlinie zur Vorratsdatenspeicherung für nicht mit den Grundrechten vereinbar. Als Folge daraus musste die Vorratsdatenspeicherung auch in Österreich gekippt werden.

➲ *Vorratsdatenspeicherung Grundrechte 9.2*

2.9 Polizeiliches Staatsschutzgesetz 2016

Um 21:17 Uhr am 13. November 2015 erschütterte eine Bombe das Stade de France in Paris, zehn Minuten später eine weitere Detonation. Währenddessen fielen Schüsse in zwei Lokalen in der Rue Alibert im 10. Arrondissement. Fünfzehn Menschen starben. Bis zur dritten Explosion im Stade de France fielen in den Straßen Paris’ weitere Schüsse, 24 weitere Menschen starben im Kugelhagel. Um 21:40 Uhr betraten drei Männer, die sich dem Islamischen Staat zurechneten, die Konzerthalle Bataclan und töteten 89 Konzertbesucher_innen mit Maschinengewehrfeuer und Handgranaten.
Am darauffolgenden Tag, dem 14. November 2015 um 7:38 Uhr twitterte Reinhold Lopatka, Vize-Obmann der ÖVP „Schockierende Anschläge! Terror ist zurück in Europa. Auch Österreich muss reagieren! Null Toleranz gegen Intolerante! Staatsschutzgesetz!“[38]
Wenig überraschend warfen Twitter-User_innen dem Politiker vor, die mörderischen Anschläge vom November 2015 in Paris zu nutzen, um ein offenbar lange geplantes Gesetz durchzudrücken. Zwei Tage später zitierte Der Standard die Innenministerin Johanna Mikl-Leitner: „Es braucht diese Instrumente im Kampf gegen die Terroristen.“[39]
Im heftig umstrittenen Staatsschutzgesetz von 2016 finden sich neben dem rechtlichen Rahmen der Organisation des Bundes- als auch der neun Landesverfassungsschutzämter die Aufgaben der Behörden. Diese beinhalten nicht nur die Überwachung Verdächtiger durch Observation, per Videofallen, über das Internet und das Telefon, sondern auch den Einsatz verdeckter Ermittler_innen, von Vertrauenspersonen und vieles mehr. Erlaubt wurde auch das Tragen von sogenannten Bodycams; Videokameras, die Beamt_innen bei Einsätzen mitlaufen lassen können.

🕮 *Body Cams*

Der Grüne Sicherheitssprecher Peter Pilz sprach sich insbesondere gegen die Weitergabe von Inhalten der Analysedatenbank an fremde Geheimdienste aus.[40]
Das Netzwerk Kritische Rechtswissenschaften stellte fest, dass das Gesetz „in mehrfacher Hinsicht gegen die österreichische Verfassung“[41] verstoße, Anwält_innen beklagten die Unbestimmtheit verschiedener Gesetzespassagen[42] und auch die Arbeiterkammer befand, das Gesetz sei eine „massive Beschränkung der individuellen Grundrechte unbeteiligter BürgerInnen“[43]; auch der Österreichische Rechtsanwaltskammertag sah im vorgelegten Gesetzesentwurf keinen Grundrechtsschutz, er höhle diesen vielmehr aus.[44]
Das Gesetz wurde unter erheblichem Widerstand der Opposition sowie der Zivilgesellschaft verabschiedet und trat mit Juli 2016 in Kraft. Eine Verfassungsklage von FPÖ und Grünen wurde in Teilen abgewiesen, zum Teil wurden die gesetzlichen Formulierungen konkretisiert.

2.10 Verhüllungsverbot 2017

„SPÖ und ÖVP stimmen geschlossen für Integrationspaket“, ließ die Parlamentskorrespondenz Nr. 583 vom 16.05.2017 verlauten.[45] Klingt gut, doch neben Integrationsverpflichtungen für anerkannte Flüchtlinge beinhaltet das Paket auch das Anti-Gesichtsverhüllungsgesetz, das mit 1. Oktober 2017 Gültigkeit erlangte. Nach wiederholter Einforderung der FPÖ und der Billigung des Burka-Verbots in Frankreich durch den EGMR[46] flammte die Diskussion europaweit

wieder auf. Dem Gesetz zufolge solle es „die Förderung von Integration durch die Stärkung der Teilhabe an der Gesellschaft und die Sicherung des friedlichen Zusammenlebens in Österreich“[47] fördern, wofür es von der Islamischen Glaubensgemeinschaft Österreichs für kontraproduktiv erachtet wurde[48]. Um den rassistischen Beigeschmack im Gesetz auszuschließen, ist die Regelung bewusst offen als Anti-Gesichtsverhüllungsgesetz formuliert. Mit der Folge: polizeiliche Abstrafung von Werber_innen in Hasenkostümen, Straßenmusiker_innen mit Eselsmaske und winterlichen Radfahrer_innen mit Schal vor dem Mund. Die Neue Zürcher Zeitung titelte am 26.10.2017: „Österreichs Polizei jagt Haie, Hasen und Lego-Figuren.“[49]

2.11 Sicherheitspaket 2018

Die erwähnten islamistischen Anschläge in Paris waren Anlass auch in Österreich im März 2016 den Einsatz eines „Bundestrojaners“ vorzuschlagen. Juristisch formuliert wäre das „die Überwachung von verschlüsselten Nachrichten“.[50]

Bundestrojaner

Spätestens seit dem NSA-Skandal um Whistleblower Edward Snowden 2013 war das Bewusstsein um Computersicherheit gestiegen, die Anwendung von Verschlüsselungssoftware bekam Aufwind. Es war Zeit, sich staatlicherseits zu überlegen, wie dieser effektive Schutz der Privatsphäre umgangen werden könnte. Ziel der Trojaner-Software war es, sich Zugang zu Kommunikationsinhalten zu verschaffen, die nicht mit den üblichen Überwachungsbefugnisse erreichbar waren. Roland Pichler vom Institut für Strafrecht und Kriminologie an der Uni Wien war einer der zahlreichen Kritiker_innen der Gesetzesinitiative. Da die Polizei plane, mit sogenannten angekauften *Exploits* (Sicherheitslücken in der Software) zu arbeiten, würde der Staat „kriminelle Kreise unterstützen“; die Überwachungssoftware sei „Schadsoftware von staatlicher Seite“. Die Maßnahme sei „nur gegen ‚virtuelle Eierdiebe‘ vom Schlage eines amateurhaft agierenden eBay-Betrügers wirksam anzuwenden“. Dem Ministerium zufolge sollte der Staatstrojaner hingegen „auf den Bereich schwerster Kriminalität (organisierte Kriminalität und Terrorismus) beschränkt bleiben“.[51]

Aufgrund rechtsstaatlicher Bedenken vielerseits wurde der Gesetzesvorschlag zum Bundestrojaner 2016 ad acta gelegt. Auch ein zweiter Anlauf des Innenministers Sobotka für eine Spähsoftware scheiterte 2017 mitsamt der SPÖ-ÖVP Regierungskoalition.[52] Wenig überraschend war es dann aber 2018 so weit. Nur zwei Monate nach Angelobung der neuen türkis-blauen Regierung schlug Innenminister Herbert Kickl (FPÖ) den Trojaner im Zuge eines Umfangreichen Sicherheitspakets vor. 2017 wetterte Kickl noch von der Oppositionsbank gegen Sobotkas Überwachungspaket. Der Vorschlag sei eine „gefährliche Drohung“, die Kickl an die DDR-Überwachung erinnere.[53]

Sicherheitspaket

Im Zuge eines sogenannten Sicherheitspakets wurde am 20. April 2018 dann unter Herbert Kickl als Innenminister der Staatstrojaner beschlossen. Doch das ist bei weitem nicht alles. Mit dem Sicherheitspaket 2018 bekam das Innenministerium Zugriff auf die Video- und Tonüberwachung öffentlicher Einrichtungen, welche die Aufnahmen vier Wochen speichern müssen. Nach richterlichem Beschluss ist der Einsatz von IMSI-Catchern möglich, welche eine Funkzelle simulieren um somit örtlich beschränkt Handydaten absaugen zu können, ebenso ist seit 2019 der Verkauf anonymer Prepaid-Karten verboten. Das ÖVP-FPÖ Sicherheitspaket erleichtert die Beschlagnahmung von Briefen durch die Behörden und weitet die Videoüberwachung im öffentlichen Raum sowie ihre Speicherung aus. Mit der „anlassbezogenen Datenspeicherung“ wurde auch eine eingeschränkte Version der Vorratsdatenspeicherung eingeführt. Auch die anlasslose und verdachtsunabhängige Erfassung aller Fahrzeugkennzeichen auf Österreichs Straßen hätte erlaubt werden sollen. Nach einem Anfangsverdacht können Internetdaten personenbezogen bis zu zwölf Monate lang gespeichert werden.[54] Das Ökobüro – Allianz der Umweltbewegung lehnte das Gesetz in seiner Gesamtheit ab, die Überwachungsmaßnahmen können „als repressive Instrumente gegen die Zivilgesellschaft eingesetzt werden“.[55]

IMSI-Catcher

Auf Anträge eines Drittels der Abgeordneten des Nationalrats sowie des Bundesrats hin wurden im Dezember 2019 sowohl die Kfz-Überwachung, als auch der Bundestrojaner nach der Prüfung durch den VfGH als grundrechtswidrig aufgehoben. Die Piratenpartei öffnet eine Perspektive, welche die gesellschaftspolitische Entwicklung der letzten Jahrzehnte anspricht und über eine Lösung von Problemen durch noch mehr Überwachung und Polizeibefugnisse hinaus weist: „Zweckmäßiger als mit unverhältnismäßigen Mitteln immer mehr Rechte zu beschneiden, wäre es, dass die Politik darauf abzielt, den Menschen wieder verstärkt Perspektiven zu eröffnen. Gute Ausbildung, faire Chancen, gelungene Integration statt Ausgrenzung, soziale Sicherheit und Gerechtigkeit – all das sind wirksamere Mittel gegen Kriminalität als eine maßlose Ausweitung der Überwachung.“[56]

Endnoten

1 *Zinner*, Wer kontrolliert die Kontrollore? juridikum 0/1989, 11-12. (https://www.juridikum.at/fileadmin/user_upload/ausgaben/juridikum%200-1989.pdf)
2 Vgl. *Sablitzer*, Geschichte des Kriminaldienstes bis 1960, https://www.polizei.gv.at/wien/publikationen/geschichte/kriminaldienst.aspx (02.12.2019) sowie Sablitzer, Die Revolution 1848 und die Polizei, Öffentliche Sicherheit 11-12/2018, 34ff.
3 *Davy*, PolizistInnen auf Identitätssuche, juridikum 03/1993, 22-25. (https://www.juridikum.at/fileadmin/user_upload/ausgaben/juridikum%203-1993.pdf)
4 *Sperlich*, Sicherheitspolizei. Verfassungswidriges Verfassungsrecht, juridikum 03/1990, 7-9, 7. (https://www.juridikum.at/fileadmin/user_upload/ausgaben/juridikum%203-1990.pdf)
5 41. Sitzung Nationalrat am 03.10.1991, Stenographisches Protokoll: https://www.parlament.gv.at/PAKT/VHG/XVIII/NRSITZ/NRSITZ_00041/imfname_142031.pdf (02.12.2019)
6 Ebd.
7 Ebd.
8 Vgl. *Pöllinger*, Sein & Sollen, juridikum 04/1993, 13-14. (https://www.juridikum.at/fileadmin/user_upload/ausgaben/juridikum%204-1993.pdf)
9 *Gesellschaft für Menschenrechte von Marginalisierten und MigrantInnen*, 1000 Jahre Haft Operation Spring und institutioneller Rassismus, Verein für antirassistische Öffentlichkeitsarbeit Wien 2005, 26ff.
10 Vgl. ebd.
11 Emmanuel Chukwujekwu zitiert von Robert Sommer in: Entsetzlich fades Kino, Augustin 03/2004, siehe auch *Chukwujekwu*, Ich habe einen Traum. 3. Brief aus der – nun bereits ein Jahr dauernden – U-Haft, https://augustin.or.at/3-brief-aus-der-nun-bereits-ein-jahr-dauernden-u-haft/ (02.12.2019).
12 Thomas *Petri*, in Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts (2012), 5. Aufl., Kapitel G, Rn. 528-564.
13 Vgl. ORF, Rasterfahndung vor 20 Jahren eingeführt, v. 29.9.2017, https://oesterreich.orf.at/v2/stories/2869269/ (02.12.2019).
14 Vgl. *Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz*, Gesamtbericht über den Einsatz besonderer Ermittlungsmaßnahmen im Jahr 2018, III-317 der Beilagen XXVI. GP https://www.parlament.gv.at/PAKT/VHG/XXVI/III/III_00317/index.shtml (2.12.2019), siehe: https://www.parlament.gv.at/PAKT/VHG/XXVI/III/III_00317/imfname_763732.pdf, 13.
15 Vgl. Parlamentskorrespondenz Nr. 493 vom 10.07.1997: Nationalrat entscheidet über Lauschangriff und Rasterfahndung https://www.parlament.gv.at/PAKT/PR/JAHR_1997/PK0493/index.shtml (02.12.2019).
16 Vgl. *Kreissl*, Polizeistaat in der Schublade, Datum 04/2017.
17 BGBl I 1997/105. (https://www.ris.bka.gv.at/Dokumente/BgblPdf/1997_105_1/1997_105_1.pdf)
18 Nationalrats-Ausschusssitzung vom 23.05.2000: Sicherheitspolizeigesetz und erweiterte Gefahrenforschung https://www.parlament.gv.at/PAKT/PR/JAHR_2000/PK0293/ (02.12.2019).
19 Ebd.
20 BGBl I 2000/85. (https://www.ris.bka.gv.at/Dokumente/BgblPdf/2000_85_1/2000_85_1.pdf)

21 Sitzung des Nationalrats vom 09.07.2002, Stenographisches Protokoll https://www.parlament.gv.at/PAKT/VHG/XXI/NRSITZ/NRSITZ_00109 (02.12.2019).
22 Vgl. APA-OTS vom 03.07.2002: Innenausschuss – Regierungsfraktionen beschließen Vermummungsverbot, https://www.ots.at/presseaussendung/OTS_20020703_OTS0261/innenausschuss-regierungsfraktionen-beschliessen-vermummungsverbot-exekutive-mehrheitlich-fuer-manche-experten-gegen-neue-regelung (02.12.2019).
23 BGBl 1953/98, zuletzt geändert durch BGBl I 2002/127, https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40034322/NOR40034322.html (02.12.2019)
24 Vgl. Die Presse, Spurensuche beim Verfassungsschutz, 27.11.2010, https://www.diepresse.com/613857/spurensuche-beim-verfassungsschutz (02.12.2019).
25 Resl, Videoüberwachung. Kameras gegen Verbrechen, Öffentliche Sicherheit, 11-12/2004. (https://www.bmi.gv.at/magazinfiles/2004/11_12/files/videoueberwachung.pdf)
26 Parlamentskorrespondenz Nr. 925 vom 09.12.2004: Opposition kritisiert Sicherheitspolizeigesetz und seine Maßnahmen, https://www.parlament.gv.at/PAKT/PR/JAHR_2004/PK0925/ (02.12.2019).
27 *Andre/Vogl/Weiss*, Die SPG-Novelle 2006, BMI SIAK-Journal. Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis 2/2006. (https://www.bmi.gv.at/104/Wissenschaft_und_Forschung/SIAK-Journal/SIAK-Journal-Ausgaben/Jahrgang_2006/files/Vogl_2_2006.pdf)
28 Bundeskriminalamt/OTS vom 19.9.2008, Kriminalstatistik und Sicherheitsmonitor sind zwei Paar Schuhe, https://www.ots.at/presseaussendung/OTS_20080919_OTS0240/bundeskriminalamt-kriminalstatistik-und-sicherheitsmonitor-sind-2-paar-schuhe (02.12.2019).
29 Tiroler Tageszeitung, Verfassungsschutzbericht: Mehr Anzeigen, Warnung vor Islamismus, 06.08.2011, https://www.tt.com/politik/innenpolitik/3167061/verfassungsschutzbericht-mehr-anzeigen-warnung-vor-islamismus (02.12.2019).
30 Vgl. Parlamentskorrespondenz Nr. 1170 vom 01.12.2011: Expertenhearing zur Polizeibefugnisgesetz-Novelle im Innenausschuss https://www.parlament.gv.at/PAKT/PR/JAHR_2011/PK1170/#XXIV_I_01520 (02.12.2019).
31 Vgl. *Andre*, Terrorprävention im Fokus, Öffentliche Sicherheit 5-6/2012, 92f. (https://www.bmi.gv.at/magazinfiles/2012/05_06/files/polizeirecht.pdf)
32 Vgl. Vorblatt und Erläuterungen zur Regierungsvorlage, 1520 d. B. XXIV. GP. (https://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01520/fname_235569.pdf)
33 *Kretschmann*, Das Wuchern der Gefahr. Einige gesellschaftstheoretische Bemerkungen zur Novelle des Sicherheitspolizeigesetzes 2012, juridikum 03/2012, 320-333. (https://www.juridikum.at/fileadmin/user_upload/ausgaben/juridikum_3-2012.pdf)
34 Parlamentskorrespondenz Nr. 1170 vom 01.12.2011: Expertenhearing zur Polizeibefugnisgesetz-Novelle im Innenausschuss, https://www.parlament.gv.at/PAKT/PR/JAHR_2011/PK1170/#XXIV_I_01520 (02.12.2019).
35 Ebd.
36 Ebd.
37 Siehe *epicenter.works*, Vorratsdatenspeicherung. Alle Menschen unter Generalverdacht, https://epicenter.works/thema/vorratsdatenspeicherung (02.12.2019).
38 Tweet v. Reinhold Lopatka, 13.11.2015, 22:38 Uhr: https://twitter.com/ReinholdLopatka/status/665418555161210881 (02.12.2019).
39 Der Standard, Staatsschutzgesetz: Mikl-Leitner will SPÖ-Bedenken ausräumen, 17.11.2016, https://www.derstandard.at/story/2000025882051/mikl-leitner-will-bedenken-der-spoe-ausraeumen (02.12.2019).
40 Vgl. *Futurezone*, Staatsschutzgesetz: Basis für Geheimdienstverbund. 10.02.2015, https://futurezone.at/netzpolitik/staatsschutzgesetz-basis-fuer-geheimdienstverbund/156.199.539 (02.12.2019).
41 *Netzwerk Kritische Rechtswissenschaften*, Stellungnahme 35 zu ME/110 XXV. GP, https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_03746/index.shtml (02.12.2019).
42 Vgl. *Ortner*, Stellungnahme 36 zu ME/110 XXV. GP, https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_03750/index.shtml (02.12.2019).
43 *Bundeskammer für Arbeiter und Angestellte*, Stellungnahme 22 zu ME/110 XXV. GP, 12.05.2015 https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_03718/index.shtml (02.12.2019).
44 Vgl. *Österreichischer Rechtsanwaltskammertag*, Stellungnahme 20 zu ME/110 XXV. GP, 12.05.2015 https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_03716/index.shtml (2.12.2019).
45 Parlamentskorrespondenz Nr. 583 vom 16.05.2017: Nationalrat: SPÖ und ÖVP stimmen geschlossen für Integrationspaket https://www.parlament.gv.at/PAKT/PR/JAHR_2017/PK0583/ (02.12.2019).
46 Vgl. Die Presse: EGMR erklärt Burka-Verbot in Frankreich für rechtmäßig, 01.07.2014, https://www.diepresse.com/3830414/egmr-erklart-burka-verbot-in-frankreich-fur-rechtmassig (02.12.2019).
47 *Rechtsinformationsystem des Bundes*, Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Anti-Gesichtsverhüllungsgesetz, Fassung vom 02.12.2019, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009892 (02.12.2019).
48 Vgl. Kurier: Ein Verbot bedient die Propaganda der Extremisten, 20.08.2016, https://kurier.at/politik/ausland/ein-verbot-bedient-die-propaganda-der-extremisten/216.564.157 (2.12.2019).
49 Neue Zürcher Zeitung: Österreichs Polizei jagt Haie, Hasen und Lego-Figuren, 26.10.2017, https://www.nzz.ch/international/oesterreichs-polizei-jagt-haie-hasen-und-lego-figuren-ld.1324167 (02.12.2019).
50 Parlamentskorrespondenz Nr. 443 vom 20.04.2018: Nationalrat beschließt Sicherheitspaket mit Bundestrojaner. https://www.parlament.gv.at/PAKT/PR/JAHR_2018/PK0443/index.shtml (02.12.2019).
51 *Technische Universität Wien, Fakultät für Informatik*, Stellungnahme 29 zu 15. d. B. XXVI. GP https://www.parlament.gv.at/PAKT/VHG/XXVI/SN/SN_00029/index.shtml (02.12.2019).
52 Vgl. Kleine Zeitung: Sobotka sieht Sicherheitspaket als gescheitert, 01.09.2017, https://www.kleinezeitung.at/service/newsticker/5278215/Sobotka-sieht-Sicherheitspaket-als-gescheitert (02.12.2019).
53 Vgl. Freiheitlicher Parlamentsklub/OTS, Kickl: Sicherheitspaket der ÖVP ist gefährliche Drohung und wird von der FPÖ abgelehnt!, 26.07.2018, https://www.ots.at/presseaussendung/OTS_20170726_OTS0044/kickl-sicherheitspaket-der-oevp-ist-gefaehrliche-drohung-und-wird-von-der-fpoe-abgelehnt (02.12.2019).
54 Vgl. *epicenter.works*, Überwachungspaket. Die schwarz-blaue Regierung will Überwachung massiv ausweiten, https://epicenter.works/thema/ueberwachungspaket (02.12.2019).
55 *Ökobüro*, Stellungnahme 79 zu 17. d. B. XXVI. GP https://www.parlament.gv.at/PAKT/VHG/XXVI/SN/SN_00079/imfname_687721.pdf (02.12.2019).
56 *Piratenpartei*, Stellungnahme 121 zu XXVI. GP https://www.parlament.gv.at/PAKT/VHG/XXVI/SN/SN_00121/imfname_690316.pdf (02.12.2019).

3. Überwachungstechnologien, Algorithmen und Big Data

Der Überwachungsdruck auf die Bevölkerung verändert sich nicht nur durch politische Entscheidungen und die Ausweitung gesetzlicher Befugnisse, sondern auch durch die Entwicklung und zunehmende Verwendung von Technologie. Dass wir das Internet, Computer und Mobiltelefone für immer mehr Bereiche unseres Lebens nutzen, bedeutet auch, dass es immer mehr Daten über alle diese Lebensbereiche gibt.[1] Die dabei entstehenden Datenmengen sind so groß, dass sie völlig neue Möglichkeiten der Kontrolle bieten *(Big Data)*. Da Speicherplatz zugleich billiger und die dafür nötige Hardware kleiner wird, und die Rechnerleistung steigt, wird es nicht nur möglich, noch mehr dieser Daten zu generieren, sondern auch, sie lange zu speichern und zu analysieren.
In diesem Kapitel werden wir ein paar Auswirkungen skizzieren, die neue Technologien auf den Überwachungsdruck haben. Diese sind aber keineswegs abschließend zu verstehen und unterliegen ständiger Veränderung und Ausweitung.

Big Data

3.1 Größe der Datensets und zunehmende Prävalenzfehler

Mit der zunehmenden Größe von Datensets bei sinkender Kriminalitätsrate[2] nimmt auch die Gefahr für alle Menschen zu, selbst als falscher Treffer *(false positives)* eingestuft zu werden. Die Vergrößerung der Datensets, mit denen gearbeitet wird, verschlechtert die Effizienz von Überwachungsmaßnahmen, statt sie zu verbessern oder auch nur neutral zu skalieren. Der für viele Menschen intuitiven Annahme, mehr Daten seien immer besser, entgegen steht der sogenannte Prävalenzfehler *(base rate fallacy)*. Dieser Fehler besteht darin, dass einer relativ hohen individuellen Treffsicherheit vertraut wird, ohne die zugrunde liegende sehr geringe Wahrscheinlichkeit eines Treffers in der Grundgesamtheit zu beachten.[3]

Prävalenzfehler

Fluggastdatenverarbeitung

Auch bei guter Trefferquote kommt es zu einer sehr hohen Rate an falschen Treffern, wenn in einem sehr großen Datenset (wie z.B. den Fluggastdaten) nach einem sehr seltenen Ereignis gesucht wird (wie z.B. versuchten Terroranschlägen).
Die Grafik (Abb. 1) demonstriert dies anhand eines Rechenbeispiels. Wir gehen hier davon aus, dass unter einer Million Menschen etwa hundert dringend tatverdächtige Personen sind (also 0,01 %). In Bezug auf terroristische Straftaten ist diese angenommene Zahl sehr wahrscheinlich höher als in der Realität. Jeder der ein Millionen Menschen wird durch einen automatischen Test bewertet, der bestimmen soll, ob er tatverdächtig ist oder nicht. Dieser Test liegt in 99 von 100 Fällen richtig (eine sehr viel höhere Trefferquote als tatsächlich jemals erzielt wird, was aber im Ergebnis das Argument nur unterstreicht). Bei den 999.900 Unverdächtigen liegt das System also in 989.901 Fällen richtig, wenn es keinen Treffer anzeigt *(true negatives)*. Bei 9.999 der 999.900 Unverdächtigen entscheidet das System falsch *(false positives)*. Bei den 100 Verdächtigen registriert das System 99 korrekte Treffer *(true positives)* und einen falschen *(false negative)*. Bei den Anwender_innen dieses Systems kommen also 10.098 Treffer an, von welchen 9.999 falsch und nur 99 korrekt sind. Obwohl das System also eine individuelle Trefferquote von 99 % hat, sind am Ende nur 0,9 % der Treffer

Trefferquoten in der Massenüberwachung

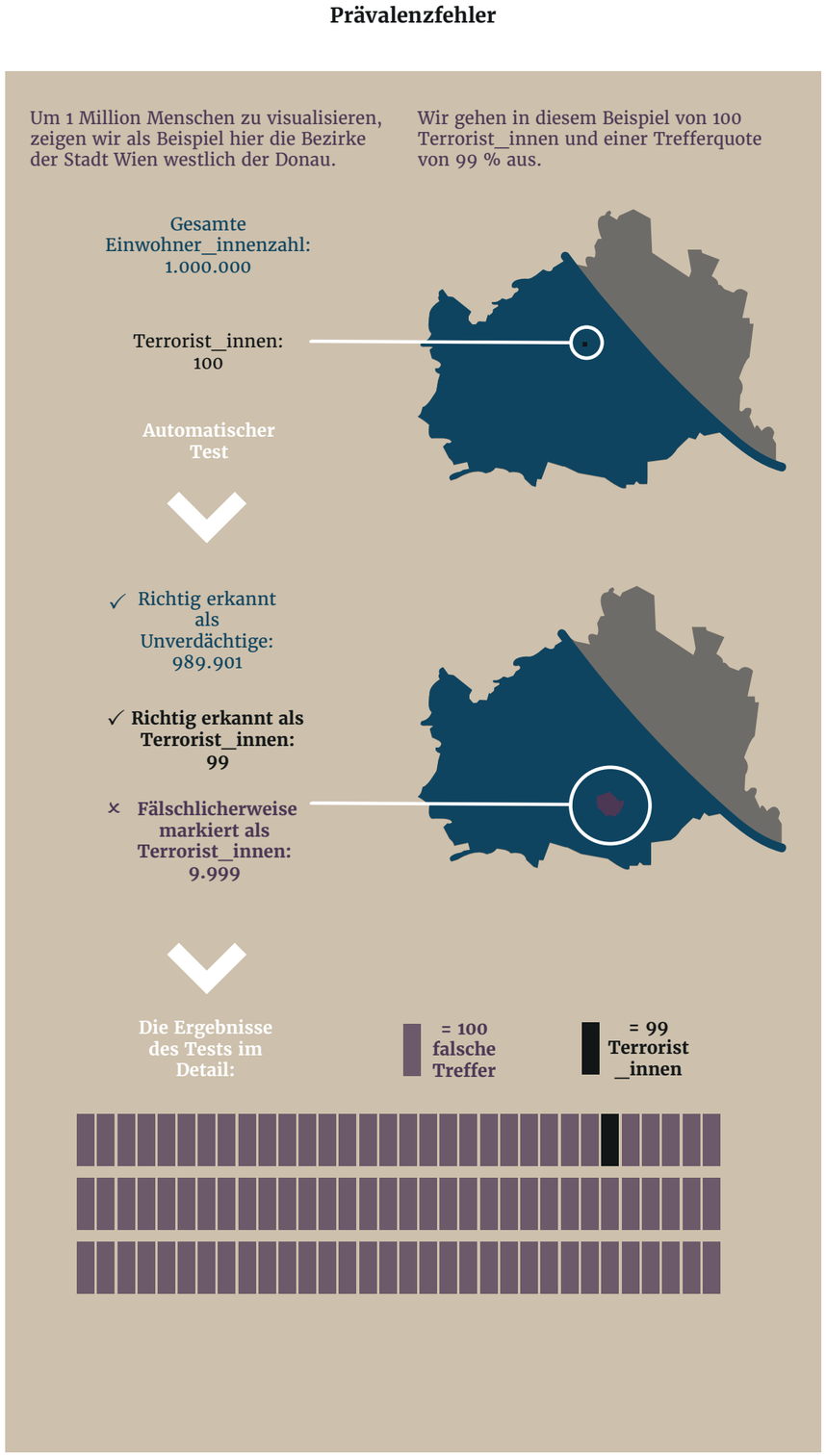


Abb. 1 Prävalenzfehler

im Gesamtsample richtig. Dies liegt an dem ursprünglichen Missverhältnis von Tatverdächtigen zu Tatunverdächtigen im Gesamtsample – dieses fundamentale mathematische Problem kann auch durch höhere Treffsicherheit nicht gelöst werden, sondern nur durch kleinere, eingegrenzte Grundsamples und eine Abkehr von anlassloser Massenüberwachung und -kontrolle.
Jeder falsche Treffer bedeutet, dass eine Person genauer überwacht wird, die sich nichts zu Schulden kommen hat lassen. Die Wahrscheinlichkeit, ungerechtfertigt ins Visier zu kommen, wird also immer höher. In Österreich hielten in den ersten acht Monaten des Fluggastdatensystems nur 0,15 % aller 190.541 Treffer einer genaueren Überprüfung stand[4] und auch in Deutschland geht man nur von 0,1 % korrekten Treffern aus.[5]
Da immer mehr Daten automatisch analysiert werden, um auf Basis von Algorithmen Entscheidungen zu treffen, werden auch die falschen Treffer zunehmen und mehr und mehr Menschen von den Folgen betroffen sein.

3.2 Interaktion von Speicherverpflichtungen mit polizeilichen Abfragen

➲ *7.3 Überwachung von Nachrichten, 7.4 Auskunft von Telekommunikationsdaten, Anlassdatenspeicherung*

Speicherverpflichtungen Privater, insbesondere von Telekommunikationsbetreiber_innen, können die Eingriffsintensität von polizeilichen Abfragebefugnissen stark beeinflussen. So ist die Polizei befugt, von Telekommunikationsbetreiber_innen ohne weitere Voraussetzungen Stammdaten zu verlangen. Auch die Auskunft über Verkehrs- und Standortdaten ist unter bestimmten Voraussetzungen möglich. Üblicherweise speichern die Betreiber_innen Verkehrs- und Standortdaten nur zu Verrechnungszwecken und löschen sie, sobald die Rechnungen unwidersprochen bezahlt wurden. Die Daten darüber hinaus zu speichern ist nicht im Interesse der Anbieter_innen, sehr wohl aber im Interesse der Polizei, wie die nicht endenwollende Debatte um die Vorratsdatenspeicherung zeigt. Obwohl sie 2014 vom EuGH für grundrechtswidrig erklärt wurde, gibt es auf EU-Ebene aktuell Bestrebungen, sie wieder einzuführen.[6] Hier wird eine Überwachungsmaßnahme nicht als polizeiliche Befugnis geregelt, sondern über den Umweg einer Speicherverpflichtung.

Vorratsdatenspeicherung

Mit dem Überwachungspaket wurde 2018 in Österreich unter anderem die Anlassdatenspeicherung *(Quick Freeze)* eingeführt. Nun können die Sicherheitsbehörden bei Bedarf eine Speicherpflicht von Verkehrs-, Standort- und Zugangsdaten für die Dauer von bis zu einem Jahr anordnen. Es handelt sich also quasi um eine Vorratsdatenspeicherung light.

7.5 Anlassdatenspeicherung

Ähnlich ist es bei der SIM-Karten-Registrierung, welche in Österreich ebenfalls mit dem Überwachungspaket 2018 eingeführt wurde und seit 01.01.2019 in Kraft ist. Seither müssen die Identitäten aller Personen registriert werden, die SIM-Karten oder Guthaben kaufen. Neu ist daran nicht nur eine Speicherverpflichtung, sondern auch die Pflicht, die Käufer_innendaten überhaupt zu erheben.

SIM-Karten-Registrierung seit Überwachungspaket 2018
§ 97 Abs. 1a TKG

Ermittlungstechnische Speicherverpflichtungen sind aber nicht die einzigen Maßnahmen, die das Potenzial dazu haben, Überwachung auszuweiten, ohne die gesetzlichen Grundlagen der Polizeiarbeit zu verändern. In dieser Hinsicht wurden beispielsweise Entwürfe zur Einführung einer Digitalsteuer der letzten österreichischen Bundesregierung kritisiert.[7] Eine Speicherverpflichtung von Browserverläufen zur Steuerberechnung würde dazu führen, dass die Sicherheitsbehörden auf diese Verläufe Zugriff erlangen können.
Eine Evaluierung von Überwachungsbefugnissen muss daher besonderes Augenmerk auf Auskunftsbefugnisse der Polizei legen und mit Erhebungen darüber einhergehen, welche und wie viele Daten von diesen Auskunftsbefugnissen betroffen sind. Verändern sich die privat gespeicherten Daten in Umfang und Qualität, verändert sich auch die Eingriffsintensität der polizeilichen Befugnisse: So kommen z.B. in den letzten Jahren immer mehr Daten von vernetzten Geräten *(Internet of Things)* dazu, die binnen kurzer Zeit alle Lebensbereiche der Menschen in noch nie dagewesener Kleinteiligkeit abdecken werden.

3.3 Ausweitung von Befugnissen durch Überwachungstechnologien

Technischen Fortschritt nutzen auch die Ermittlungsbehörden, und dies oftmals, ohne dass für den Einsatz neuer Überwachungstechnologien auch neue und eigene gesetzliche Befugnisse geschaffen werden. Die neuen Technologien werden auf Basis bestehender Rechtsgrundlagen eingesetzt, obwohl die neuen Überwachungstechnologien die Grundrechtseingriffe massiv verstärken. Oft wird in diesem Zusammenhang von einer „Technologieneutralität" der Rechtsgrundlagen gesprochen, beispielsweise in Bezug auf die Strafprozessordnung in den Materialien zum Überwachungspaket, das 2018 die Überwachungsbefugnisse massiv ausweitete.[8] Der Begriff der Technologieneutralität ist aber im Hinblick auf die veränderte Intensität der Grundrechtseingriffe irreführend.

Einsatz neuer Technologien auf Basis alter Rechtsgrundlagen

Technologieneutralität

Es ist eine durch die Menschenrechte garantierte Voraussetzung, dass bei der Einführung von Überwachungsbefugnissen eine Einschätzung darüber zu treffen ist, ob ihr Nutzen im Verhältnis zu ihrer Eingriffsintensität steht. Ändert sich im Nachhinein aber die Eingriffsintensität der Befugnis, kann sich auch das Ergebnis der Verhältnismäßigkeitsprüfung ändern und die Befugnis somit grundrechtswidrig werden. Aus diesem Grund wäre eine regelmäßige systematische Überprüfung der Recht- und Verhältnismäßigkeit der Überwachungsmaßnahmen notwendig. Unter Umständen müssen diese dann eingeschränkt, eingestellt oder abgeschafft werden. Die Ausweitung von Befugnissen durch neue Technologien lässt sich anhand folgender Beispiele illustrieren:

➲ *Verhältnismäßigkeit 9.1.3*

Gesichtserkennung: Im April 2019 wurde bekannt, dass die österreichische Polizei plant, ab Dezember desselben Jahres Software zur automatischen Gesichtserkennung einzusetzen.[9] Eine neue gesetzliche Grundlage ist dafür nicht vorgesehen; die neue Analysesoftware soll auf Basis allgemeiner sicherheitspolizeilicher Bestimmungen verwendet werden.[10] Die Software soll Standbilder aus Videoüberwachungsmaterial herausfiltern, die das Gesicht einer verdächtigen Person zeigen und diese automatisiert mit Bildern der polizeilichen erkennungsdienstlichen Datenbank abgleichen. Es wird davon ausgegangen, dass dieses Abgleichdatenset ein bis fünf Millionen Datensätze umfasst.[11] Es liegt auf der Hand, dass ein automatischer Abgleich mit Millionen von Gesichtern eine andere Dimension eines Grundrechtseingriffs darstellt als die manuelle Datenauswertung.

Erkennungsdienstliche Datenbank

Drohnen: In Österreich werden zur Zeit in einer Pilotphase erstmals 76 Drohnen zur polizeilichen Videoüberwachung – unter anderem zur Überwachung von Versammlungen – eingesetzt, und dies ohne neue Rechtsgrundlage.[12] Der Einsatz von Drohnen verändert die polizeilichen Befugnisse zur Videoüberwachung maßgeblich. Drohnen sind beweglicher als heute noch üblichere Stand- und Mastkameras. Das bedeutet auch, dass sie aus anderen Perspektiven filmen können – beispielsweise in Privatwohnungen hinein. Außerdem ist es weitaus schwieriger, einer Drohne bewusst auszuweichen, als dies bei weniger beweglichen Kameras möglich ist.

Predictive Policing: Eine weitere technologische Veränderung althergebrachter Polizeibefugnisse stellt *Predictive Policing* dar. Um ihre Arbeit vorausschauend zu gestalten, verarbeitet die Polizei je nach Programm große Mengen personenbezogener Daten, Daten über Kriminalitätsaufkommen u.Ä. In Österreich ist derzeit ein Programm in Betrieb, das der Vorhersage von Wohnraumeinbrüchen dienen soll.[13] In die Gebiete, die durch das Programm als besonders gefährdet gekennzeichnet werden, fahren Streifendienste öfter zur Prävention. Dadurch erlangt die einfache Befugnis des Streifendienstes eine völlig neue Bedeutung, die neue Fragen nach Diskriminierung durch Algorithmen, Verantwortlichkeit, Transparenz und Kontrolle aufwirft. Solche Systeme wirken

Veränderungseffekte von präventiver Überwachung

zurück auf die Datenbasis, auf der sie fußen. Es kann also z.B. sein, dass man aus den Gebieten, in denen öfter kontrolliert wird, mehr Daten über verdächtige Merkmale bekommt, die dann wiederum die Basis für weitere Kontrollen werden und so ein Feedback-Loop erzeugt – oder aber auch genau gegengleich einen Verdrängungseffekt hervorrufen. Hierzu gibt es noch so gut wie keine Evaluierung oder Reflexion über die erzielten Effekte. Auch die Frage, was ein Streifendienst eigentlich bewirkt, und ob er das richtige Mittel zur Bekämpfung von Wohnraumeinbruch ist, wird dabei überhaupt nicht mehr gestellt.
Auch die Evaluation der Wirksamkeit von *Predictive Policing* gestaltet sich schwierig, da die Ergebnisse nicht eindeutig interpretierbar sind. Fährt ein Streifendienst an den Ort, den das Programm vorschlägt, und findet dort nichts Verdächtiges vor, kann dies entweder den Grund haben, dass das Programm falsch lag, oder den Grund, dass die Prävention durch den Streifendienst funktioniert hat.

🕮 *Fluggastdaten-verarbeitung*

Data Mining

Auch das System der Fluggastdatenverarbeitung, die aufgrund einer EU-Richtlinie[14] für alle Mitgliedstaaten verpflichtend ist, bringt eine Form des *Predictive Policing* mit sich. Laut Erwägungsgrund 7 der Richtlinie sollen die Daten unter anderem dazu dienen, Personen zu ermitteln, die bis dahin nicht verdächtig waren. In diesen Datenbanken mit Daten von Millionen Menschen[15] wird also erstmals ohne vorherigen Verdacht mittels *Data Mining* erst Verdacht generiert – das heißt, die Polizei wird (für den österreichischen Rechtsrahmen erstmalig!) völlig unabhängig davon tätig, ob ein Verbrechen geplant wird oder begangen wurde. So verändert sich die Polizeiarbeit durch den Einsatz von Algorithmen grundlegend.
Diese Ausweitungen von Überwachung durch neue technologische Möglichkeiten sind ohne demokratische Beschlüsse und ohne breite gesellschaftliche Debatte auf keinen Fall vertretbar.

3.4 Diskriminierung durch Algorithmen

Der Einsatz von Algorithmen im polizeilichen Bereich birgt die Gefahr der Diskriminierung.[16] Wenn die Algorithmen zusätzlich auch noch intransparent sind, z.B. weil sie sich durch *Machine Learning* eigenständig weiterentwickeln und ihre Funktionsweise als sogenannte *Black Boxes* insbesondere für die Anwender_innen gar nicht mehr nachvollziehbar ist, wird es so gut wie unmöglich, auszuschließen, dass sie auf einer diskriminierenden Basis arbeiten. Oftmals sind schon die Daten diskriminierend, auf denen die Algorithmen beruhen, z.B. wenn People of Colour häufiger kontrolliert werden als Weiße und daher in Datenbanken von Verdächtigen mit überdurchschnittlich hoher Häufigkeit vorkommen.
Rechtlich handelt es sich um Diskriminierung, wenn eine Person ohne sachlichen Grund, sondern aufgrund der Zugehörigkeit zu einer geschützten Gruppe schlechter behandelt wird. In den nationalen Gesetzen zur Polizei sind diese geschützten Gruppen das Geschlecht, die „Rasse“ (§ 31 SPG Abs. 2 Z. 5, § 5 Richtlinien-Verordnung für die Polizei) oder Hautfarbe, die nationale oder ethnische Herkunft, das religiöse Bekenntnis, die politische Auffassung und die sexuelle Orientierung. Es ist der Polizei verboten, diskriminierend zu handeln, und die Beamt_innen müssen auch darauf Bedacht nehmen, dass dies von den Betroffenen nicht so empfunden wird.

§ 31 SPG Abs. 2 Z. 5, Richtlinien-Verordnung § 5 für die Polizei

Art. 7 Abs. 1 Bundes-Verfassungsgesetz iVm Art. 2 StGG

Auch die Verfassung und die Grundrechte schützen vor Diskriminierung. Laut dem Bundesverfassungsgesetz über die Beseitigung rassischer Diskriminierung von 1973 haben Gesetzgebung und Vollziehung jeder Unterscheidung „aus dem alleinigen Grund der Rasse, der Hautfarbe, der Abstammung oder der nationalen oder ethnischen Herkunft“ zu unterlassen. Der in der Verfassung verankerte Gleichheitssatz verbietet hingegen nur die Ungleichbehandlung unter Staatsbürger_innen und unter Fremden, schützt also bei weitem nicht vor allen Formen von Diskriminierung. Grundrechtlich schützen daneben auch Art. 14 EMRK und Art. 21 GRC vor Diskriminierung. Auch im Datenschutzrecht

➲ *10.1.2 Automatisierte Entscheidungen*

ist diskriminierendes Profiling verboten, insbesondere durch automatisierte Entscheidungen.
Gegen Diskriminierung durch die Polizei kann man sich durch eine Richtlinien-Beschwerde (z.B. im Fall einer rassistischen Beschimpfung), durch eine Maßnahmenbeschwerde (z.B. bei rassistisch motivierten Festnahmen und Kontrollen) oder bei der Volksanwaltschaft (bei strukturellen Missständen) wehren.

Richtlinienbeschwerde bei rass. Diskriminierung § 89 Abs. 1 SPG

Maßnahmenbeschwerde § 88 SPG iVm Art. 130 Abs. 1 Z 2 B-VG

3.5 Recht auf Verschlüsselung

Eine starke Verschlüsselung ist heute für viele Dienste und Anwendungen eine Grundvoraussetzung. Sie gewährleistet Datensicherheit, ermöglicht Online-Zahlungsverkehr, erschwert Identitätsdiebstahl und Internetbetrug und sichert die Privatsphäre. Durch die weitere Verbreitung von verschlüsselten Kommunikationsdiensten wird es allerdings auch für die Sicherheitsbehörden zunehmend schwieriger, diese zu überwachen: Seit Jahren wird in diesem Zusammenhang über das Phänomen des *Going Dark* diskutiert. Damit ist das Versiegen eines Informationskanals, entgegen der Sicherheitsinteressen eines Staats, gemeint. Tatsächlich kommt es für die Beurteilung der Einsichtbarkeit von Kommunikationsinhalten für den Staat aber darauf an, welchen Zeithorizont man betrachtet: Es war die längste Zeit der Menschheitsgeschichte nicht möglich, einen Großteil der menschlichen Kommunikation zu überwachen, da dieser mündlich stattfand. Erst seit immer größere Teile der Kommunikation digital stattfinden, wurde breite Überwachung überhaupt erst möglich. Daher ist nicht die Zeit der weit verbreiteten Verschlüsselung die historische Ausnahme, sondern die kurze Zeit der unverschlüsselten überwachbaren Kommunikation (das „Goldene Zeitalter der Überwachung“[17]). In Anbetracht dessen, dass wir immer abhängiger von vernetzten Systemen werden, und staatliche wie private Überwachung und Cyberkriminalität stetig ansteigen, ist ein Recht auf Verschlüsselung unentbehrlich. Dies würde bedeuten, dass es auch dem Staat verboten sein sollte, Sicherheitslücken auszunützen, statt diese zu reparieren oder Unternehmen auf diese hinzuweisen, und dass der Staat Unternehmen keinesfalls dazu zwingen darf, Verschlüsselungstechnologien schon gezielt mit Lücken zu bauen *(backdoors)* oder die eigenen Verschlüsselungssysteme zu brechen.

🕮 *Bundestrojaner*

Tipps zum Weiterlesen

Eubanks, Algorithms of Inequality. How High-Tech Tools Profile, Police and Punish the Poor (2017).
Ferguson, The Rise of Big Data Policing. Surveillance, Race and the Future of Law Enforcement (2017).
Harcourt, Against Prediction. Profiling, Policing, and Punishing in an Actuarial Age (2007)
Landau, Listening In. Cybersecurity in an Insecure Age (2017).
O'Neil, Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy (2016).
Schneier, Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World (2016)
Snowden, Permanent Record (2019).

Endnoten

1 Vgl. *Schneier*, Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World (2016) 15ff.
2 *Bundeministerium für Inneres*, Die Polizeiliche Kriminalstatistik 2018, 5. (https://bundeskriminalamt.at/501/files/PKS_18_Broschuere.pdf)
3 Zur ausführlichen Erklärung des Prävalenzfehlers und seiner Auswirkungen auf Systeme der Massenüberwachung siehe *McDermott*, An Explainer On The Base Rate Fallacy, https://en.epicenter.works/content/an-explainer-on-the-base-rate-fallacy-and-pnr (04.11.2019).
4 Siehe die Zahlen des Bundesministerium für Inneres, Anfragebeantwortung vom 01.10.2019, https://fragdenstaat.at/anfrage/fluggastdatenanalyse-datenschutzrechtliche-aspekte/ (04.11.2019).
5 Siehe https://nopnr.eu/pnr/ (04.11.2019).
6 Vgl. *Rat der EU*, Vorratsdatenspeicherung zum Zweck der Kriminalitätsbekämpfung: Rat verabschiedet Schlussfolgerungen, https://www.consilium.europa.eu/de/press/press-releases/2019/06/06/data-retention-to-fight-crime-council-adopts-conclusions/ (04.11.2019).
7 *epicenter.works*, Digitalsteuergesetz schreibt bis dato unerlaubte Datenspeicherung vor, https://epicenter.works/content/digitalsteuergesetz-schreibt-bis-dato-unerlaubte-datenspeicherung-vor (04.11.2019).
8 Vgl. Erläuterungen zum Strafprozessrechtsänderungsgesetz 2018, 17 d. B. XXVI. GP, 2. (https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00017/fname_682032.pdf)
9 *Wimmer*, Polizei startet im Dezember mit Gesichtserkennung, https://futurezone.at/netzpolitik/polizei-startet-im-dezember-mit-gesichtserkennung/400469524 (18.04.2019).
10 Vgl. *Bundesministerium für Inneres*, Anfragebeantwortung vom 25.09.2019, https://fragdenstaat.at/anfrage/gesichtserkennung/ (04.11.2019).
11 Vgl. *Bundesministerium für Inneres*, Anfragebeantwortung vom 11.06.2019, https://fragdenstaat.at/anfrage/ankauf-einer-gesichtserkennungs-software-durch-das-bundeskriminalamt/ (04.11.2019).
12 Vgl. *Bundesministerium für Inneres*, Anfragebeantwortung vom 22.08.2019, https://fragdenstaat.at/anfrage/drohneneinsatze-durch-die-polizei/ (04.11.2019).
13 Vgl. *Bundesministerium für Inneres*, Anfragebeantwortung vom 05.09.2019, https://fragdenstaat.at/anfrage/predictive-policing/ (04.11.2019).
14 Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27.04.2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität.
15 Allein in Deutschland wird von bis zu 180 Millionen betroffenen Personen pro Jahr ausgegangen (laut Anfrage der Abgeordneten Andrej Hunko, Martina Renner, Jan Korte u. a.: http://dipbt.bundestag.de/doc/btd/19/095/1909536.pdf Stand 04.11.2019). In Österreich, mit einer Gesamtbevölkerung von ca. 8,5 Millionen Menschen, waren im nicht voll ausgebauten Betrieb in den ersten acht Monaten schon 11,9 Millionen Menschen betroffen, vgl. *Bundesministerium für Inneres*, Anfragebeantwortung vom 08.10.2019, https://fragdenstaat.at/anfrage/fluggastdatenanalyse-datenschutzrechtliche-aspekte/ (04.11.2019).
16 Vgl. *O'Neil*, Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy (2016) 84–104. Siehe auch: *Ferguson*, The Rise of Big Data Policing. Surveillance, Race and the Future of Law Enforcement (2017) 47ff.
17 Vgl. *Center for Democracy & Technology*, 'Going Dark' Versus a 'Golden Age for Surveillance' https://cdt.org/blog/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99/ (04.11.2019).

ÜBERWACHUNGS-
BEFUGNISSE

Es ist völlig klar, wenn es eine totale
Überwachung gäbe, würde die
Zahl der kriminellen Handlungen
reduziert werden.
Aber die Frage ist:
Wollen wir in einer Welt leben, die
den Einzelnen auf Schritt und Tritt
bis ins Wohn- und Schlafzimmer
überwacht?

Gerhart Holzinger als Präsident des
Verfassungsgerichtshofs

4. Überwachung im Überblick

Dieses Kapitel dient der Auseinandersetzung mit dem rechtlichen Rahmen der Überwachung. Es werden darin die Gesetze dargestellt, die der Polizei Überwachungsmaßnahmen erlauben, ohne jedoch auf einzelne Maßnahmen im Detail einzugehen (siehe dazu aber die folgenden Kapitel). Es werden außerdem Kontrolle und Aufsicht sowie Einschränkungen wie Berufsgeheimnisse, Beweisverwertungsverbote und das Bankgeheimnis überblicksmäßig dargestellt. Weiters werden auch die Quellen, die über Überwachung Auskunft geben können, vorgestellt und Beispiele für Strafdrohungen häufiger Delikte gegeben, da sich die rechtlichen Befugnisse oft auf diese beziehen. Schließlich werden einzelne polizeiliche Datenbanken und internationale Kooperationen vorgestellt.

4.1 Rechtsgrundlagen für polizeiliche Überwachung in Österreich

Für jede Überwachungsmaßnahme, die die Polizei setzt, braucht sie eine konkrete gesetzliche Grundlage. In Österreich finden sich diese in verschiedenen Gesetzen, wie z.B. im Sicherheitspolizeigesetz (SPG) und in der Strafprozessordnung (StPO), aber auch im Polizeilichen Staatsschutzgesetz (PStSG), oder im Gesetz über die Fluggastdatenverarbeitung (PNR-G). Im Folgenden wird versucht, diesen Problemkreis zu skizzieren, eine abschließende juristische Analyse wird hier jedoch keinen Platz haben.

4.1.1 Abgrenzungen zwischen Kriminalpolizei, Sicherheitspolizei und Verfassungsschutz

Ermittlungsmaßnahmen vs. freier Raum in StPO und SPG

Überwachungsmaßnahmen können von der Polizei kriminal- oder sicherheitspolizeilich oder durch den Verfassungsschutz ausgeübt werden. Damit werden jeweils unterschiedliche Aufgaben erfüllt. Jede einzelne Ermittlungsmaßnahme muss einer konkreten Aufgabe zugeordnet werden: Wo es keinen Anlass für Ermittlungen gibt, muss im Gegenzug ein von Überwachung freier Raum herrschen.[1] Da die Ermittlungsbefugnisse je nach Aufgabe verschieden sind und unterschiedliche Voraussetzungen haben, ist die klare Unterscheidung rechtlich auch in der Praxis relevant.

Kriminalpolizei (StPO) nicht ohne konkreten Anfangsverdacht

Die Aufgabe der Kriminalpolizei ist es, Verbrechen aufzuklären und zu verhindern, und hauptsächlich in der StPO geregelt. Als Kriminalpolizei kann die Polizei demnach erst agieren, wenn ein konkreter Anfangsverdacht besteht. Dieser liegt vor, wenn auf Grund bestimmter Anhaltspunkte angenommen werden kann, dass eine Straftat begangen worden ist. Eine begangene Straftat muss allerdings nicht vollendet worden sein, sondern es kann sich auch um einen strafbaren Versuch handeln. Dass das Strafverfahren erst ab Vorliegen eines konkreten Verdachts beginnt, hat den Zweck, Menschen davor zu schützen „ohne Anlass zum Objekt von Ermittlungen zu werden".[2] Davor können keine Ermittlungen aufgrund der StPO eingeleitet werden.

Sicherheitspolizei bei drohender Gefahr

Sicherheitspolizeiliche Aufgaben sind u.a. die Gefahrenabwehr und die Aufrechterhaltung der öffentlichen Ordnung und Sicherheit. Hier geht es also darum, die Öffentlichkeit vor Gefahren zu schützen. Dazu zählt auch die Gefahrenerforschung, die Feststellung einer Gefahrenquelle und des für die Abwehr einer Gefahr sonst maßgeblichen Sachverhaltes. Diese wurde in den letzten Jahren immer wieder ausgeweitet, was jedes Mal für große Kritik sorgte (siehe im Detail unten). Diese Aufgaben können parallel zu denen der Strafverfolgung bestehen, je nachdem ob eine tatsächliche Gefahr droht, nicht jedoch z.B., wenn eine Straftat begangen wurde, und nur deren Aufklärung relevant ist, ohne dass die Gefahr einer Wiederholung besteht.[3]

➲ *2. Überwachungsbefugnisse im Zeitraffer*

Zu den Aufgaben des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT) zählt der „vorbeugende Schutz" vor verfassungsgefährdenden Angriffen. Da aber sogar straflose Vorbereitungshandlungen unter die Gefahrenabwehr nach dem SPG fallen, darf es für die Aufgabenerfüllung nach dem polizeilichen Staatsschutzgesetz (PStSG) noch zu keiner Vorbereitungshandlung und zu keiner tatsächlichen Bedrohung gekommen sein.[4] Verhärtet sich bei diesen Ermittlungen der Verdacht auf eine Straftat, darf die Polizei nur mehr nach der StPO vorgehen, mit oftmals höheren Voraussetzungen. Adensamer und Sagmeister nennen dies einen „Wertungswiderspruch", da ein konkreter Tatverdacht Ermittlungsmaßnahmen besser rechtfertigen kann als nur wahrscheinliche Angriffe.[5] Beamt_innen des BVT können auch die Aufgaben der Sicherheitspolizei erfüllen, da das SPG im PStSG subsidiär gilt.[6] Umgekehrt können aber andere Organisationseinheiten der Polizei keine Aufgaben nach dem PStSG erfüllen.[7]

Fluggastdatenverarbeitung

Das PNR-G zur Fluggastdatenverarbeitung ist das erste Gesetz, das Ermittlungstätigkeiten ohne jeglichen Anlass oder Verdacht auf Gefahren und begangene Straftaten ermöglicht. Somit stellt es einen Paradigmenwechsel in der österreichischen Rechtsordnung dar.[8] Nach dem PNR-G dürfen Fluggastdaten (Passenger Name Records, also PNR) von allen Menschen, die in die oder aus der EU fliegen, analysiert werden, mit der PNR-Verordnung des_der Innenminister_in auch die über Flüge innerhalb der EU. Dieses System soll laut der PNR-EU-Richtlinie unter anderem dazu dienen, Personen zu überprüfen, die davor noch unter keinem Verdacht standen[9]; diesen Verdacht also gerade erst zu generieren. Auf diese Weise wird der Raum, der frei von Überwachung bleiben muss, Stück für Stück aufgegeben.

Strafbarkeit vieler Delikte (u. somit Überwachungsrechtfertigung) rückt ins Vorfeld der Tat

Die Unterscheidung zwischen Aufgaben der Sicherheitspolizei und der Kriminalpolizei wird auch deswegen immer schwieriger, weil die Strafbarkeit vieler Delikte immer weiter ins sogenannte Vorfeld verlegt wird. Das heißt, dass z.B. auch schon allein die Ausbildung und das Reisen, sowie das Sammeln von Geldmitteln für terroristische Zwecke oder die bloße Teilnahme an einer staatsfeindlichen Verbindung strafbar ist. Dabei ist zu bedenken, dass im Strafrecht ohnehin grundsätzlich auch der Versuch, ein Delikt zu begehen, und die Beihilfe an Delikten strafbar sind. Wenn man dies mit den weiten Straftatbeständen kombiniert, bedeutet das, dass z.B. schon der Verdacht auf den Versuch, einer Organisation beizutreten, Überwachungsmaßnahmen rechtfertigt. Man entfernt sich so immer weiter von den tatsächlichen terroristischen Taten, die man verhindern will, und bringt immer mehr Menschen potentiell ins Visier von Überwachung.

4.1.2 Folgen der Unterscheidung zwischen polizeilichen Aufgabenbereichen

Mit der Strafverfolgung gehen besondere Grundrechte, insbesondere das Recht auf ein faires Verfahren, einher. Dass rechtsstaatliche Verfahrensregeln eingehalten werden, wird hier als besonders wichtig gesehen, weil eine Verurteilung und eine Freiheitsstrafe ganz besonders stark in das Leben der Menschen eingreifen und es daher besonders wichtig ist, dass das Verfahren, das dahin führt, fair ist. Deswegen gibt es in der StPO höhere Voraussetzungen für polizei-

➲ *5. Verdeckte Ermittlung*

liche Ermittlungen als im SPG, z.B. müssen einige Maßnahmen erst gerichtlich bewilligt werden, was im Sicherheitspolizeirecht üblicherweise nicht der Fall ist. Manche Maßnahmen im SPG müssen dafür von Rechtsschutzbeauftragten bewilligt werden (s.u.). Es ist umstritten, ob die geringeren Voraussetzungen im Sicherheitspolizeirecht überhaupt gerechtfertigt sind, da ja die so gesetzten Überwachungsmaßnahmen durchaus auch in Grundrechte eingreifen. Oft scheint es, als werde versucht, durch das Sicherheitspolizeirecht die strengeren Voraussetzungen des Strafprozessrechts zu umgehen. Ein gemeinsamer, hoher verfahrensrechtlicher Standard wäre wünschenswert, und wo das nicht möglich ist und die Trennung von Aufgaben bestehen bleibt, sollte das „Wechseln" zwischen den Rechtsgrundlagen klar geregelt sein. Auch durch Beweisverwertungsverbote (s.u.) im Strafverfahren kann diesem Problem begegnet werden, damit sich die Umgehung der strafrechtlichen Regeln nicht auszahlt.

Geringere Voraussetzungen im Sicherheitspolizeirecht

Auch die Rechtsschutzmöglichkeiten sind in den verschiedenen Gesetzen unterschiedlich. Aus Sicht der Betroffenen ist dies äußerst unbefriedigend, weil es bedeutet, dass man erst wissen muss, auf welcher Basis die Polizei agiert hat, um zu wissen, welchen Beschwerdeweg man dagegen einschlagen kann. Gegen Maßnahmen sicherheitspolizeilicher Befehls- und Zwangsgewalt kann man eine Maßnahmenbeschwerde beim Landesverwaltungsgericht erheben. Im Bereich der Kriminalpolizei hingegen gibt es die Möglichkeit, bei der Staatsanwaltschaft einen Einspruch nach der StPO zu erheben. Irrt man sich darin, welches Mittel das richtige ist, ist die Beschwerde unzulässig, und bis man das erfahren hat, könnten die Fristen des anderen Rechtsmittels schon verstrichen sein. Oft gibt es auch gar keine Möglichkeit, feststellen zu können, nach welchen gesetzlichen Grundlagen die Polizei eingeschritten ist. Diese Situation ist daher eine Belastung für die Betroffenen und hat auch den VfGH schon öfters beschäftigt.[10]

Rechtschutzmöglichkeiten, Beschwerden

4.1.3 Die erweiterte Gefahrenerforschung und der verfassungsgefährdende Angriff

Die erweiterte Gefahrenerforschung wurde erstmals 2000 im SPG eingeführt. Damals konnten Gruppierungen beobachtet werden, die im Verdacht standen sich in einem Umfeld zu bewegen, in dem es „zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität, insbesondere zu weltanschaulich oder religiös motivierter Gewalt" kommen könnte.
2012 wurde dies auf Einzelpersonen ausgeweitet, die sich öffentlich für Gewalt aussprechen und sich Mittel und Kenntnisse verschaffen, um große Schäden anzurichten. Diese Ausweitung sorgte für rechtsstaatliche Bedenken.[11] Auch die Datenverarbeitung zur Analyse und Bewertung der Wahrscheinlichkeit einer Gefährdung ist seitdem gesetzlich vorgesehen.
2016 wurde die erweiterte Gefahrenerforschung wiederum ausgeweitet und ins PStSG verschoben, das nun die Tätigkeiten des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT) regelt. Der Rechtsschutzbeauftragte des Innenministeriums hatte schon in der Begutachtungsphase des PStSG damit gerechnet, dass die neuen Aufgaben sehr viel öfter angewendet würden als die erweiterte Gefahrenerforschung davor im SPG, und dass die Änderung einen stark steigenden Aufwand bedeuten würde.[12]

Aufgaben des BVT

Das BVT hat heute drei Aufgaben:

1. die erweiterte Gefahrenerforschung, die sich allerdings wie ursprünglich nur auf Gruppen bezieht, da sich die erweiterte Gefahrenerforschung für Einzelpersonen laut den Erläuterungen als nicht zielführend erwies.

2. „den vorbeugenden Schutz vor verfassungsgefährdenden Angriffen durch eine Person" bei begründetem Gefahrenverdacht. Für einen begründeten Gefahrenverdacht ist mehr als die bloße Möglichkeit oder Nichtausschließbarkeit eines Angriffs notwendig, laut Heißl also eine „konkrete Bedrohungssituation".[13]

3. den Schutz vor „verfassungsgefährdenden Angriffen" aufgrund von Informationen zu Personen, die in Verdacht stehen, im Ausland einen verfassungsgefährdenden Angriff verwirklicht zu haben, ohne Bedrohungssituation.

Die Definition des „verfassungsgefährdenden Angriff" ist aufgrund weit verzweigter Gesetzesverweise sehr komplex und wurde allein dafür schon bei ihrer Entstehung vielfach kritisiert. Einerseits besteht ein solcher „verfassungsgefährdender Angriff" in bestimmten Straftatbeständen, wie z.B. die terroristischen Straftaten, oder solche nach dem Verbotsgesetz, das u.a. die nationalsozialistische Wiederbetätigung unter Strafe stellt. Auch eine Reihe weniger schwerwiegender Straftatbestände können allerdings unter die Definition fallen, wenn sie mit „ideologischer oder religiöser" Motivation begangen werden. Darunter fallen z.B. Körperverletzung und schwere Nötigung. Was genau hier die Bedeutung der Begriffe „ideologischer" und „religiöser" Motivation ist, ist auch in den Rechtswissenschaften unklar.[14]

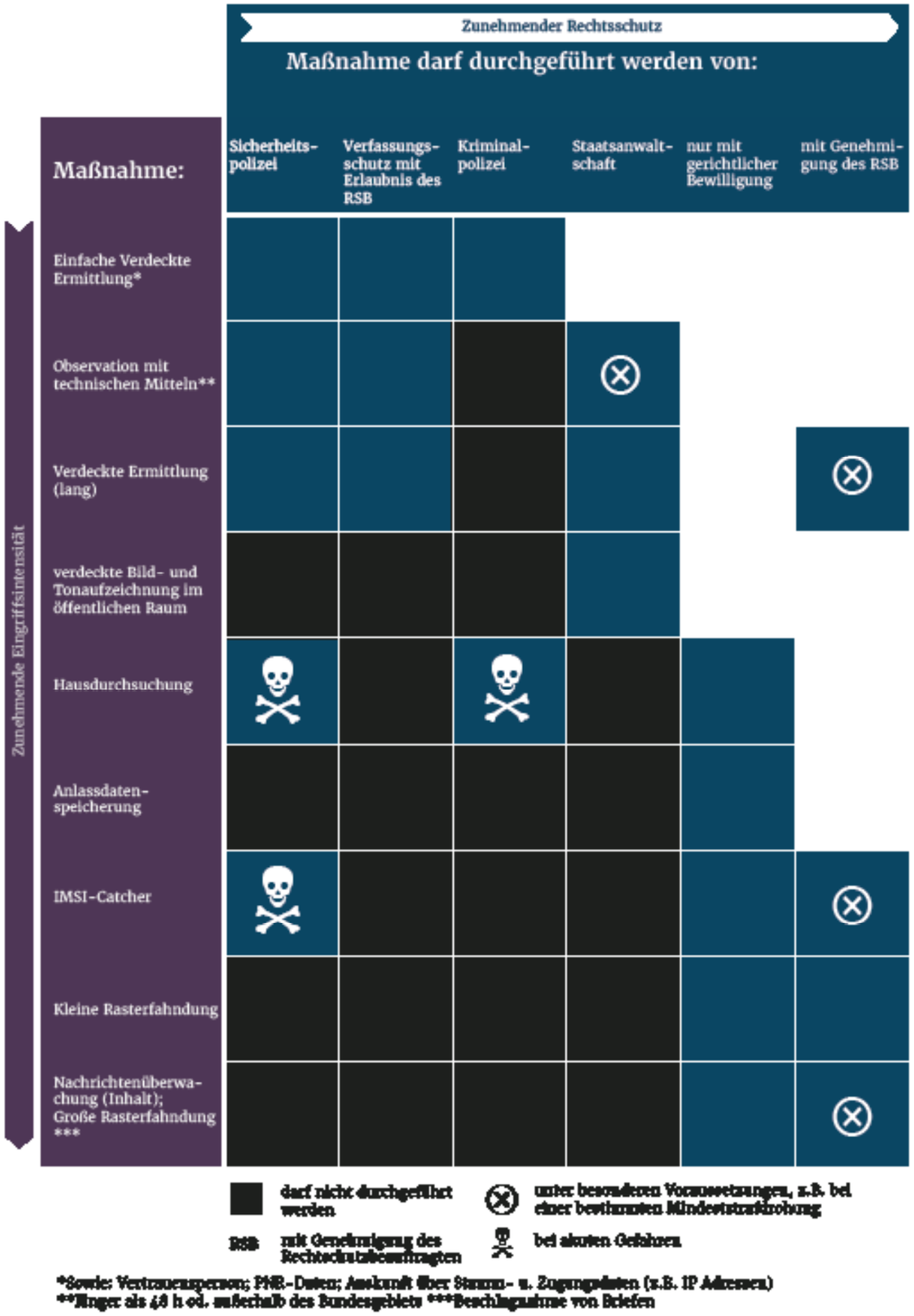
Definition „verfassungsgefährdender Angriff"

Auch Erklärungen, wieso diese Delikte bei ideologischer oder religiöser Motivation gefährlicher sein sollten als ohne, und wieso in diesen Fällen besondere Ermittlungsmaßnahmen notwendig sein sollten, gibt es nicht. Die Unterscheidung ist daher unsachlich und folglich verfassungswidrig.[15] Adensamer und Sagmeister schreiben dazu: „Das Abstellen auf weltanschauliche Motivationen zeugt von der Blindheit gegenüber der eigenen Position, die verhindert, auch diese als Weltanschauung zu erkennen. Denn die Bewertung bestimmter Gefahren als verfassungsgefährdend und der Verfassung als Gesamtes als schützenswert ist nichts anderes als das: Ausdruck einer Weltanschauung; somit ist das Beschließen eines Gesetzes zu diesem Zweck ebenso weltanschaulich motiviert."

4.2 Überwachungsbefugnisse im Überblick

Die Grafik zeigt überblicksmäßig eine – bei weitem nicht vollständige – Liste an Überwachungsmaßnahmen und deren formale Voraussetzungen. Oben stehen die Maßnahmen, die einfacher einzusetzen sind, weil sie als weniger eingriffsintensiv gesehen werden, weiter unten die, die als schwerwiegender gelten. Die formalen Voraussetzungen führen von Einsätzen durch die Polizei alleine, also von sich aus (links), bis zu einer Bewilligungspflicht durch das Gericht und die Rechtsschutzbeauftragten (rechts). Die Tabelle soll einen Eindruck davon geben, wie unterschiedlich die Voraussetzungen für einzelne Maßnahmen sein können. Dabei kann nicht die gesamte Komplexität abgebildet werden, und Voraussetzungen wie z.B. die Einschränkungen auf bestimmte Delikte nach Mindeststrafhöhen mussten weggelassen werden. Auch die horizontale Ebene kann keine definitive Bewertung des Rechtsschutzes z.B. zwischen Sicherheitspolizei und Verfassungsschutz oder zwischen Gericht und RSB sein, sondern soll Tendenzen anzeigen. Aus der Grafik wird ersichtlich, wo es möglicherweise zu Wertungswidersprüchen zwischen den verschiedenen Regelungsfeldern kommt. Es wird z.B. deutlich, dass zwar die Sicherheitspolizei und der Verfassungsschutz von sich aus Observationen mit technischen Mitteln und verdeckte Ermittlungen über einen längeren Zeitraum durchführen können, nicht aber die Kriminalpolizei allein.

Abb. 2, nächste Seite: Überwachungsbefugnisse im Überblick



4.3 Kontrolle und Aufsicht

Neben den subjektiven Rechten, die man selbst einklagen kann, z.B. durch Beschwerden, gibt es auch Aufsichts- und Kontrollorgane, deren Aufgabe es ist, die Rechtmäßigkeit der Überwachungsmaßnahmen sicherzustellen. Dies ist besonders dort relevant, wo Maßnahmen im Geheimen eingesetzt werden und wo es auch um die Überwachung politischer Gruppierungen geht.

➲ *Datenschutz/ Beschwerden 10.*

Rechtsschutzbeauftragte: Sowohl im SPG, in der StPO als auch im PStSG und im PNR-G ist ein_e Rechtsschutzbeauftragte_r (RSB) vorgesehen. Diese_r ist unabhängig und weisungsfrei, kann also nicht einfach entlassen oder gekündigt werden, wenn er_sie der Regierung unliebsam wird.

	Bestellung durch	Auf Vorschlag von
StPO	Justizminister_in	Vorschlag des_der Präsident_in des Verfassungsgerichtshofes, des_der Vorsitzende_n der Volksanwaltschaft und des_der Präsident_in des Österreichischen Rechtsanwaltskammertages
SPG	Bundespräsident_in	Bundesregierung nach Anhörung der Präsident_innen des Nationalrates sowie der Präsident_innen des Verfassungsgerichtshofes und des Verwaltungsgerichtshofes

Aufgaben des_der Rechtsschutzbeauftragten

Den Einsatz mancher Überwachungsmaßnahmen muss der_die RSB im Vorhinein genehmigen, z.B. die Depersonalisierung von PNR-Daten (wenn es um die Vorbeugung oder Verhinderung bestimmter Straftaten geht), oder bei Ermittlung gegen eine Person, die durch die geistliche Amtsverschwiegenheit geschützt ist nach der StPO. Nach dem PStSG müssen erweiterte Gefahrenerforschungen und Ermittlungen wegen verfassungsgefährdenden Angriffen im Vorhinein genehmigt werden, genauso wie der Einsatz von Ermittlungsmaßnahmen im Einzelnen, wie Observation, Einsatz von Bild- und Tonaufzeichnungsgeräten, der Einsatz von Kennzeichenerkennungsgeräten, etc. Diese Ermächtigung darf nur für den notwendigen Zeitraum erteilt werden, und maximal für 6 Monate, Verlängerungen sind aber zulässig.

Rechtsschutzsenat

Bestimmte Ermächtigungen nach dem PStSG kann nur ein Rechtsschutzsenat erteilen, der aus dem_derr RSB und zwei Stellvertreter_innen besteht. Darunter fallen verdeckte Ermittlungen und der Einsatz von Vertrauenspersonen und Auskünfte über Verkehrs- Zugangs- und Standortdaten.

➲ *5. Verdeckte Ermittlung, Standortdaten 7.1 Datenarten*

Die Videoüberwachung öffentlicher Orte nach dem SPG darf nur eingesetzt werden, wenn der_die RSB entweder zugestimmt hat, oder drei Tage nach einer Meldung an ihn_sie verstrichen sind. Ebenso ist es bei Datenbanken über Gruppierungen unter Beobachtung, die das BVT anlegt und bei bestimmten Verlängerungen von Speicherfristen durch das BVT, nicht aber bei Datenbanken über Vertrauenspersonen[16].

Überprüfung von Überwachungsmaßnahmen durch RSB

Andere Maßnahmen kann er_sie nur im Nachhinein überprüfen, z.B. nach dem SPG: Observation, verdeckte Ermittlungen (SPG), verdeckte Bild- und Tonaufzeichnungen, IMSI-Catcher usw. Der_die RSB muss über den Einsatz dieser Maßnahmen so früh wie möglich informiert werden. Nach der StPO prüft und kontrolliert er_sie die Anordnung, Genehmigung, Bewilligung und Durchführung von verdeckten Ermittlungen, Abschlüssen von Scheingeschäften, optischen und akustischen Überwachungen, und bestimmte Ermittlungsmaßnahmen, wenn sie sich gegen Personen richten, die im Strafprozess wegen ihres Naheverhältnisses zu dem_der Beschuldigten das Recht haben, die Aussage zu verweigern.

Berichte über Überwachungsmaßnahmen durch RSB

Außerdem gehört es zu den Aufgaben des_der RSB, über den Einsatz von Überwachungsmaßnahmen zu berichten (s.u.). Nach dem SPG hat der_die RSB die Pflicht, bei Datenschutzverletzungen Beschwerde bei der Datenschutzbe-

hörde zu erheben, und nach der StPO kann er_sie Einspruch bzw. Beschwerde bei der Staatsanwaltschaft erheben. Nach der StPO hat er_sie auch das Recht, die Löschung von Daten zu beaufsichtigen und sich von deren Vernichtung zu überzeugen, sowie diese zu beantragen.

Rechte von RSB

Die RSB haben nach SPG und PStSG das Recht auf Zutritt zu Räumen, Einblick in Unterlagen und Aufzeichnungen, um ihrer Kontrollfunktion gerecht werden zu können. Eine Ausnahme besteht bei Auskünften über die Identität von Personen, die im Strafprozess als Zeug_innen anonym bleiben dürfen, weil ihnen sonst Gefahr droht. Nach der StPO werden ihnen die relevanten Akten vorgelegt, auf deren Basis sie entscheiden. Die Aufgaben des_der RSB und deren Rechte und Pflichten nach dem SPG können nur mit einer Verfassungsmehrheit begrenzt werden.

Die Einrichtung der RSB wurde oft als nicht ausreichend für eine wirksame Kontrolle kritisiert.[17] Zuletzt hat auch der Verfassungsgerichtshof in seiner Entscheidung über den Bundestrojaner bestätigt, dass eine Bewilligung des_der RSB und die rechtliche Möglichkeit der Kontrolle für eine tatsächliche Kontrolle der Maßnahme nicht ausreichen. Vielmehr müsste durch persönliche und technische Ressourcen sichergestellt werden, dass die Kontrolle auch tatsächlich durchgeführt wird.[18]

Parlamentarischer Unterausschuss für innere Angelegenheiten: Zur Kontrolle über die nachrichtendienstlichen Maßnahmen des Verfassungsschutzes ist ein parlamentarischer Unterausschuss eingerichtet, der zum Ausschuss für Inneres gehört. Die Nationalratsabgeordneten in diesem Ausschuss sind befugt, von dem_der zuständigen Minister_in alle einschlägigen Auskünfte und Einsicht in Unterlagen zu erhalten, sofern dies nicht die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde.

Verletzung von Menschenrechten

Volksanwaltschaft: Die Volksanwaltschaft hat Kontrollrechte über die Verwaltung, um Missstände zu beseitigen. In den Bereich der Verwaltung fallen Überwachungsmaßnahmen nach dem SPG und PStSG, nicht aber nach der StPO, welche zur Justiz zählt (zur Unterscheidung s.o.). Betroffene Personen können sich mittels einer Beschwerde insbesondere wegen behaupteter Verletzung von Menschenrechten an die Volksanwaltschaft wenden. Die Volksanwaltschaft kann Behörden auch von Amts wegen prüfen, sie ist dabei von den Behörden zu unterstützen und ihr ist Akteneinsicht zu gewähren. Außerdem kann sie Beschwerde beim VfGH erheben. Die Volksanwaltschaft besteht aus drei Mitgliedern, die von den drei mandatsstärksten Parteien in Nationalrat bestellt werden. Teil der Volksanwaltschaft ist auch der Menschenrechtsbeirat, dessen Mitglieder zum Teil von NGOs vorgeschlagen werden. Dieser hat u.a. die Aufgabe, Befehls- und Zwangsakte der Polizei zu überprüfen, worunter z.B. Identitätsfeststellungen, Erkennungsdienstliche Behandlungen, oder der Einsatz von Bodycams fallen könnten.

Bodycams

Datenschutzbehörde: Die Datenschutzbehörde (DSB) überwacht als Aufsichtsbehörde die Einhaltung der Datenschutzgrundverordnung und der Polizei-DS-Richtlinie. Im Bereich der polizeilichen Datenverarbeitungen hat sie neben dem Bearbeiten von Beschwerden von Betroffenen außerdem folgende Aufgaben:

Aufgaben der Datenschutzbehörde

- Sensibilisierung der Öffentlichkeit für Risiken, Vorschriften, Garantien und Rechte
- Beratung von Parlament und Regierung über legislative und administrative Vorhaben
- Sensibilisierung von für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter_innen
- Informieren betroffener Personen über deren Rechte (auf Anfrage)
- Austausch mit den Aufsichtsbehörden anderer Länder und Amtshilfe diesen gegenüber
- Untersuchungen über die Anwendung der Polizei-DS-Richtlinie
- Überprüfung von Einschränkung von Informationen und Auskünften sowie die Verweigerung der Einschränkung oder Löschung
- Verfolgung maßgeblicher Entwicklungen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie
- Beratung vor der Anlage neuer Datenbanken mit personenbezogenen Daten
- Ausübung von Betroffenenrechten, bei Einschränkung von Informationen und Auskünften sowie die Verweigerung der Einschränkung oder Löschung

Dazu hat die DSB insbesondere die Befugnis, nach Verständigung die Räume, in denen Daten verarbeitet werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, Verarbeitungen durchzuführen und wenn erforderlich Kopien zu erstellen. Sie kann außerdem Warnungen aussprechen, Anweisungen gehen und konkrete Datenverarbeitungen auch verbieten. Der_die Leiter_in der DSB wird nach einer öffentlichen Ausschreibung von dem_der Bundespräsident_in auf Vorschlag der Bundesregierung für fünf Jahre bestellt.

Datenschutzrat: Der Datenschutzrat ist ein Gremium beim Justizministerium, das zu Fragen des Datenschutzes Stellung nimmt, die einheitliche Fortentwicklung des Datenschutzes fördert und die Bundesregierung in rechtspolitischer Hinsicht bei datenschutzrechtlich relevanten Vorhaben berät. Ihm gehören Vertreter_innen der im Nationalrat vertretenen Parteien, Vertreter der Arbeiterkammer, WKO, der Länder, des Gemeinde- und Städtebundes, des BMJ, der Datenschutzbeauftragten der anderen Ministerien und Expert_innen an.

Rechnungshof: Der Rechnungshof kontrolliert u.a. die Gebarung des Bundes auf Wirtschaftlichkeit und Zweckmäßigkeit. Er hat das Recht auf die Übersendung von Büchern sowie die Einschau an Ort und Stelle. Auch der Einsatz von Ermittlungsbefugnissen kann Gegenstand einer Überprüfung durch den Rechnungshof sein, siehe z.B. den Bericht über ausgewählte Ermittlungsmaßnahmen von 2008.[19]

4.4 Berufsgeheimnisträger_innen und Beweisverwertungsverbote

Um die Vertraulichkeit bestimmter Beziehungen, Ämter und Berufe zu wahren, dürfen Angehörige bestimmter Berufsgruppen nicht als Zeug_innen unter Wahrheitspflicht darüber vernommen werden, was ihnen im Zuge und wegen ihrer Tätigkeit anvertraut wurde.

Darunter fallen Geistliche, Beamt_innen und Personen mit klassifizierten Informationen des Nationalrates oder Bundesrates.

Bestimmte Personen haben außerdem das Recht, als Zeug_in die Aussage zu verweigern (Beschuldigte haben dieses Recht ohnehin). Dieses gilt für:

Recht auf Aussageverweigerung

- Angehörige des_der Beschuldigten

- Verteidiger_innen, Rechtsanwält_innen, Patentanwält_innen, Verfahrensanwält_innen in Untersuchungsausschüssen des Nationalrates, Notar_innen und Wirtschaftstreuhänder_innen darüber, was ihnen in dieser Eigenschaft bekannt geworden ist

- Fachärzt_innen für Psychiatrie, Psychotherapeut_innen, Psycholog_innen, Bewährungshelfer_innen, eingetragene Mediator_innen, und Mitarbeiter_innen anerkannter Einrichtungen zur psychosozialen Beratung und Betreuung darüber, was ihnen in dieser Eigenschaft bekannt geworden ist

- Medieninhaber_innen (Herausgeber_innen), Medienmitarbeiter_innen und Arbeitnehmer_innen eines Medienunternehmens oder Mediendienstes über Fragen, welche die Person der Verfasser_innen, Einsender_innen von Beiträgen und Unterlagen betreffen oder sich auf Mitteilungen beziehen, die ihnen im Hinblick auf ihre Tätigkeit gemacht wurden

- Wahlberechtigte darüber, wie sie ein gesetzlich für geheim erklärtes Wahl- oder Stimmrecht ausgeübt haben.

Beweisverwertungsverbot

Es ist im österreichischen Recht grundsätzlich nicht wie in manchen anderen Ländern verboten, Beweise in Gerichtsverfahren zu verwenden, deren Beschaffung rechtswidrig war. Ein solches Beweisverwertungsverbot verringert den Anreiz für die ermittelnden Behörden Gesetze zu umgehen, da die so erlangten Beweise bei festgestellter Rechtswidrigkeit schlichtweg unbrauchbar werden. Einzelne Umgehungen sind aber auch in Österreich mit Beweisverwertungsverboten belegt. So z.B. die geistliche Amtsverschwiegenheit und das Recht auf Aussageverweigerung (s.o.). Auch das Recht, die Aussage zu verweigern (s.o.), darf nicht durch andere Überwachungsmaßnahmen umgangen werden, insbesondere nicht durch die Überwachung von Kommunikation oder die Sicherstellung und Beschlagnahme von Datenträgern oder durch die Vernehmung von Mitarbeiter_innen und Auszubildenden. Jedenfalls unzulässig ist die Überwachung von Beichtstühlen. Besonders Maßnahmen der Massen-Kommunikationsüberwachung stellt in dieser Hinsicht den Rechtsstaat auf die Probe: So berichtet Justizminister Jabloner 2019, dass bei Sicherstellung riesiger Datenmengen die Feststellung von etwaigen Berufsgeheimnissen einen besonders großen Aufwand darstelle.[20] Geistliche dürfen dann überwacht werden, wenn sie selbst dringend verdächtig sind, und der_die RSB eine Ermächtigung dazu erteilt hat.

Redaktionsgeheimnis bei Online-Medien / Providern

Redaktionsgeheimnis: Durch das Recht auf freie Meinungsäußerungsfreiheit wird auch das Redaktionsgeheimnis gewährleistet. Auf dieses kann man sich selbst dann stützen, „wenn die verlangte Auskunft Aufschluss über schwere und schwerste Verbrechen geben könnte."[21] Der Schutz der Vertraulichkeit journalistischer Quellen ist außerdem „eine der Grundbedingungen der Pressefreiheit"[22] und dadurch auch ein wesentlicher Bestandteil der konventionsrechtlichen Garantie des Art 10 EMRK.
Mit dem Redaktionsgeheimnis hat sich der Oberste Gerichtshof (OGH) auch im Kontext von Online-Foren auseinander gesetzt. Darin bezog sich der OGH auf eine Entscheidung des Oberlandesgerichts (OLG) Wien, in der dieses entschieden hatte, dass ein Online-Medium, das gleichzeitig als Provider und als Anbieter von Inhalten auftrat, sich auch bezüglich der Foren-Beiträge von User_innen auf das Redaktionsgeheimnis berufen konnte und somit die Weitergabe von Daten an die Staatsanwaltschaft verweigern konnte. Der OGH schränkte dies aber folgendermaßen ein: „Eine Berufung auf das Redaktionsgeheimnis ist dann unzulässig, wenn ein Posting in keinerlei Zusammenhang mit einer journalistischen Tätigkeit steht. Es muss also zumindest irgendeine Tätigkeit, Kontrolle oder Kenntnisnahme eines Medienmitarbeiters intendiert sein, damit der Schutz des § 31 MedienG in Anspruch genommen werden kann." Laut OGH mangle es einem Posting an dem notwendigen Zusammenhang mit einer journalistischen Tätigkeit der in § 31 MedienG genannten Personen, wenn dieses völlig ohne journalistische Kontrolle und Bearbeitung, und allein aus dem eigenen Antrieb des_der Nutzer_in veröffentlicht wird. Allein die durch das Zurverfügungstellen des Online-Forums erklärte Absicht, alles zu veröffentlichen, was die Nutzer posten, reiche in dem Fall nicht aus, um den notwendigen Mindestzusammenhang zur Tätigkeit der Presse herzustellen.
In den Entscheidungsgründen zum obigen ersten Judikat schreibt das OLG Wien auch: „Die Betreiberin einer Onlinetageszeitung ist jedenfalls ein Medienunternehmen, sodass sie berechtigt ist, Antworten auf Fragen, welche die Person eines Einsenders von Beiträgen betreffen, zu verweigern. Dieses Verweigerungsrecht bezieht sich auch auf die Daten der Person eines Leserbriefschreibers und ist durch das Umgehungsverbot des § 31 Abs 2 MedienG zusätzlich abgesichert."
Und weiter: „Die Anwendbarkeit des § 18 ECG ist nämlich davon abhängig, ob der Provider zugleich Medieninhaber ist oder nicht, das heißt, dass sich nur der Provider, der zugleich Medieninhaber ist, auf das Redaktionsgeheimnis in Bezug auf die Person des Posters berufen kann und daher nicht nach § 18 ECG zur Herausgabe verpflichtet ist." Koukal argumentiert in einem Beitrag zu der Erkenntnis des OLG Wien (wie auch der OGH später entscheiden sollte), man müsse unterscheiden, ob Postings als Beiträge iSd § 1 MedienG gesehen werden können. Die Poster_innen teilen ihre Inhalte ja nicht primär nur den Journalist_innen mit, sondern auch anderen Nutzer_innen bzw. einer bestimmten Öffentlichkeit. In der Regel könnten Nutzer_innen auch ihre Postings selbstständig veröffentlichen und es gebe nur eine Nachkontrolle. Laut Koukal müsse man (auch im Einklang mit nunmehriger OGH-Judikatur) unterscheiden: Lediglich wenn es um den Schutz von Personen gehe, die Journalist_innen geheime Informationen und vertrauliche Hinweise geben, könnten Poster_innen in Online-Foren durch das Redaktionsgeheimnis geschützt werden.[23]

4.5 Finanztransaktionen und Bankgeheimnis

Der Bereich der Finanztransaktionen und der Banken ist für den Grundrechtsschutz vor allem deshalb höchst brisant, weil es sich um Maßnahmen handelt, die durch private Rechtsträger_innen wie Banken und Kreditinstitute vorgenommen werden müssen und mit Meldepflichten gegenüber den Strafverfolgungsbehörden verbunden sind. In Kombination mit Delikten, die im Zusammenhang mit Terrorismusbekämpfung immer weiter ins Vorfeld einer konkreten Tat reichen (z.B.: die terroristische Vereinigung nach § 278b StGB), besteht hier ein hohes Risiko, dass die Streubreite der Grundrechtseingriffe unverhältnismäßig wächst und völlig unbeteiligte und unbescholtene Menschen häufig von Grundrechtseingriffen betroffen sind.

Financial Action Task Force on Money Laundering FATF Geldwäscherichtlinien

Die im Juni 1989 von den Staatschefs der G7-Staaten und dem Präsidenten der Europäischen Kommission ins Leben gerufene (und demokratisch nicht legitimierte) Financial Action Task Force (on Money Laundering), FATF, (Arbeitsgruppe für finanzielle Maßnahmen gegen Geldwäsche), verabschiedete 40 „Empfehlungen" sowie nach dem 11. September 2001 noch neun „Sonderempfehlungen", die in den meisten Mitgliedsländern der FATF Grundlage für nationale Gesetze wurden.

Die Europäische Union, seit 2006 selbst Mitglied der FATF, verabschiedete auf Grundlage der Empfehlungen der FATF mittlerweile vier „Geldwäsche-Richtlinien". War Gegenstand der 1. Geldwäsche-Richtlinie noch die Bekämpfung der organisierten Kriminalität und hier insbesondere des internationalen Suchtgifthandels zentraler gewesen (mit der Konsequenz der Observation des bargeldlosen Zahlungsverkehrs durch Überwachungs- und Meldepflichten der Geldinstitute), dehnte die 3. Geldwäsche-Richtlinie den „Bekämpfungsauftrag" auf „besonders schwerwiegende Straftaten" aus. Eine Generalklausel umfasst zusätzlich alle Straftaten, die mit einer Freiheitsstrafe von mehr als einem Jahr

bedroht sind. Mitte 2015 wurde die 4. Geldwäsche-Richtlinie beschlossen, die bis Mitte 2017 von den Mitgliedstaaten umzusetzen war.

Die Gesetzgebung zur Überwachung von Finanztransaktionen weist einige Besonderheiten auf: die Ausarbeitung der grundlegenden Vorgaben in – zum Teil demokratisch nicht legitimierten – internationalen Gremien, die Verpflichtung von Privaten zur Mitwirkung, die intensive Automatisierung, Datensammlung und -auswertung, sowie die intensive internationale Kooperation und den internationalen Datenaustausch.

Die Bürger_innen selbst sollen als Überwacher_innen tätig werden, im – gesetzlich normierten – Auftrag des Staates ihre Mitmenschen kontrollieren und sie im Verdachtsfall melden. Seit der Umsetzung der 3. Geldwäsche-RL in Österreich in Verbindung mit der Novellierung der Rechtsanwaltsordnung (RAO) können selbst österreichische Rechtsanwält_innen in die Situation geraten, gemäß § 8c RAO hinter dem Rücken ihrer Mandant_innen Informationen über einen Verdacht auf Terrorismusfinanzierung oder Geldwäschehandlungen an das Bundesministerium für Inneres melden zu müssen.

Outsourcing von Überwachung auf Banken, Private usw.

Die Probleme dieser Art des „Outsourcings" der Überwachung auf Private sind mannigfach: Die Überwachung erfolgt nicht durch – mit hoheitlichen Befugnissen ausgestattete – Behörden, sondern durch Private, wie Banken, Unternehmen, Notar_innen und Rechtsanwält_innen. Die Bürger_innen werden bei Verdacht auf Geldwäsche und/oder Terrorismusfinanzierung gesetzlich zu Spitzeldiensten verpflichtet. Darüber hinaus handelt es sich dabei um verdachtsunabhängige Überwachung. Nicht nur wird also in der überwiegenden Mehrzahl der Fälle in die Rechte unbescholtener Bürger_innen eingegriffen, sondern die Untersuchungshandlungen und Ermittlungen erfolgen auch unterhalb der Schwelle eines „Anfangsverdachtes", unterliegen somit nicht den Regelungen und damit den Schutzmechanismen der Strafprozessordnung. Darüber hinaus haben die Betroffenen keinerlei Parteistellung und Prozessrechte.

Software zur Analyse und Watch Lists

Zur Unterstützung der Umsetzung der Pflichten der Kredit- und Finanzinstitute ist ein eigener Zweig der Softwarebranche entstanden, der die entsprechende Software zur Analyse von Finanztransaktionen entwickelt. Ebenso ist international eine Branche der Anbieter_innen von „Watch Lists" entstanden, welche von den Verpflichteten, insbesondere Kredit- und Finanzinstituten, erworben werden, um ihren Pflichten zur Bekämpfung der Geldwäsche und insbesondere der Terrorismusfinanzierung nachzukommen. Die Namen auf diesen Listen stammen zum Teil von öffentlichen internationalen Sanktionslisten und zum Teil aus eigenen Erhebungen durch die Anbieter_innen, wobei die Zahl der Betroffenen in die Millionen geht. Diese „Watch Lists" greifen in das Grundrecht auf Datenschutz, die Bewegungsfreiheit sowie die Eigentumsfreiheit der Betroffenen ein und der Rechtsschutz wird als mangelhaft beschrieben.[24]

Geldwäscherei ist zudem ein sehr weit gefasster Tatbestand. Sehr leicht kann man in die Situation kommen, das Tatbild zu erfüllen, wenn auch ohne jeglichen Vorsatz,[25] und auf diese Weise in den Fokus von Ermittlungen geraten. Ähnlich verhält es sich mit der Terrorismusfinanzierung, ein Tatbestand, der überdies sehr weit im Vorfeld der eigentlichen Tat angesiedelt ist.

Große Problematik durch Rechtsschutzdefizite bei Finanztransaktionen

Diese Umstände, also die immer weiter in das Vorfeld verschobenen Straftatbestände sowie die besondere Gefahr, leicht (unschuldig) in den Fokus von Ermittlungen zu geraten, und die schlechte Lage der Betroffenen, um sich rechtlich zu wehren, machen gerade in Kombination mit den beschriebenen Rechtsschutzdefiziten die große Problematik der derzeit üblichen Überwachung von Finanztransaktionen aus. Wie beschrieben ist die Überwachung von Finanztransaktionen in mehrerlei Hinsicht ein sehr isolierter Sektor der Überwachung: Sie unterliegt einem eigenständigen Regelungsregime, das jedoch die notwendigen Detailregelungen hinsichtlich Datenschutz, Datensicherheit und

Schnittstellen vermissen lässt, und ist ein sehr wenig untersuchter Sektor der Überwachung. Die Überwachung von Finanztransaktionen würde sich daher vornehmlich für eine sektorspezifische Bereichsevaluation der Überwachungsgesetze eignen.

Bankgeheimnis

Betreffend den Aspekt des Bankgeheimnisses hat der Gesetzgeber schließlich die Problematik erkannt und einen Rechtsschutzmechanismus eingeführt, der einen zweistufigen gerichtlichen Rechtsschutz mit der Bestellung eines Rechtsschutzbeauftragten kombiniert und sowohl in institutioneller als auch prozessualer Hinsicht als „Good Practice" erachtet werden kann: Nach den Verfassungsbestimmungen des § 9 Abs. 1 und 4 Kontenregister- und Kontoneinschaugesetz (KontRegG) entscheidet ein_e Einzelrichter_in am Bundesfinanzgericht über die Bewilligung einer Konteneinschau wobei gegen diese Entscheidung ein Rekurs möglich ist, über den ein Richtersenat am Bundesfinanzgericht entscheidet. Die §§ 8 und 9 Abs 2 leg cit sehen detaillierte Anforderungen an die Form eines diesbezüglichen Auskunftsverlangens und eine Begründungspflicht vor. Die §§ 10 f. regeln die Stellung des Rechtsschutzbeauftragen. Allerdings ist auch diese Regelung verbesserungswürdig; insbesondere enthält sie keine Bestimmungen zum besonderen Schutz von Berufsgeheimnisträgern, deren Kontobewegungen Einblick in geschützte Berufsgeheimnisse geben können.

4.6 Übersicht über die Quellenlage

Informationen über Überwachungsmaßnahmen, wie z.B. über ihre Häufigkeit, werden in Österreich relativ verstreut in verschiedenen Quellen erfasst. Im Rahmen dieses Handbuchs greifen wir vor allem auf die folgenden Quellen bzw. Quellengruppen zurück:

Der Bericht des_der Rechtsschutzbeauftragten des BMI (genauer: Zentrale Daten des_der Rechtsschutzbeauftragten) gibt einen Überblick über die Tätigkeit des_der Rechtsschutzbeauftragten (RSB) beim Bundesministerium für Inneres im vorvergangenen Jahr. Dieser Bericht muss bis zum 31. März des Folgejahres vorliegen. Dabei werden vor allem auch Einsätze, die der Genehmigung durch den RSB bedürfen, statistisch erfasst. Die Berichte erschienen zunächst in der Österreichischen-Juristen-Zeitung und im Journal für Strafrecht, seither aber im SIAK (=Sicherheitsakademie)-Journal „Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis") des BMI.

Die Sicherheitsberichte des BMI und BMJ und der Kriminalitätsbericht des BMI: Der Sicherheitsbericht des BMI behandelt Vorbeugung und Bekämpfung von Straftaten also Einschätzungen und Analysen von Bereichen wie organisierter Kriminalität oder Cyber-Sicherheit und auch Unterstützungen durch das Bundeskriminalamt sowie etwa Handlungsberichte des Einsatzkommandos Cobra und der Direktion für Spezialeinheiten. Der Kriminalitätsbericht hingegen liefert Statistiken über begangene Straftaten. Der Sicherheitsbericht des BMJ wiederum liefert unter Information über die Tätigkeit der Staatsanwaltschaft und der Strafgerichte, über Verurteilungen und auch Vollzugsmaßnahmen.

Der Bericht über besondere Ermittlungsmaßnahmen des BMJ beschäftigt sich mit bestimmten, eingriffsintensiven Ermittlungsmaßnahmen, nämlich verschiedenen Formen der optischen und akustischen Überwachung von Personen sowie dem automationsunterstützten Datenabgleich. Aufschlussreich kann auch der jährliche **Verfassungsschutzbericht** des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung sein (BVT). In diesem wird die vom BVT wahrgenommene Bedrohungslage durch Extremismus dargestellt (Islamistischer Extremismus und Terrorismus, Linksextremismus und Rechtsextremismus). Diese Berichte sind auf der Webseite des BVT abrufbar.

Abb. 3, zu 4.7 Überblick Strafdrohungen

Überblick Strafdrohungen

	Freiheits-entzug	Geld-strafe Tagessätze	An-gezeigt	Auf-geklärt
Diebstahl	6 Monate	360	121022	31322
Sachbeschädigung	6 Monate	360	58151	16022
Diebstahl durch Einbruch – Vergehen	3 Jahre	-	55915	7979
Körperverletzung	1 Jahr	72	35493	30323
Fahrlässige Körperverletzung im Straßenverkehr	3 Monate	180	29258	27570
Betrug	6 Monate	360	27440	15661
Gefährliche Drohung	1 Jahr	720	14842	13841
Diebstahl durch Einbruch in Wohnstätten oder mit Waffen – Verbrechen	6 Monate – 5 Jahre	-	13344	2191
Veruntreuung – Vergehen	6 Monate	360	2307	2124
Schwerer Diebstahl – Vergehen	3 Jahre	-	2069	594
Schwere Nötigung	6 Monate – 5 Jahre	-	1919	1778
Fortgesetzte Gewaltausübung – Vergehen	3 Jahre	-	1277	1271
Vergewaltigung	1 – 10 Jahre	-	817	653
Mord	10 – 20 Jahre	-	203	190

Parlamentarische Anfragen basieren auf dem verfassungsgesetzlich garantierten Fragerecht (auch Interpellationsrecht genannt) von Abgeordneten des österreichischen Nationalrates und Bundesrates gegenüber der Bundesregierung und den Minister_innen. Dabei geht es um Fragen der Vollziehung von Gesetzen, die befragten Minister_innen sind dabei zur wahrheitsgemäßen Beantwortung verpflichtet. In der Vergangenheit gab es im Bereich Überwachung zahlreiche Anfragen, unter anderem zu Observation mit Peilsendern, dem Einsatz von Videoüberwachung oder auch dem Stand der Fluggastdatenspeicherung in Österreich (siehe dazu genauer in den nachfolgenden Kapiteln).

Das **Transparenz-Tool fragdenstaat.at**, das unter anderem vom Forum Informationsfreiheit betrieben wird, stellt eine Eingabemaske bereit, mit der es leicht gemacht wird, eigene Anfragen an Behörden zu stellen. Auch die Fristen können einfach im Überblick behalten werden, und es gibt viele eingebaute praktische Features wie eingebautes PDF-Schwärzen sowie E-Mail Erinnerungen und Textvorschläge, um verspätete Anfragen zu urgieren.
Auf der **Webseite des Parlaments** (parlament.gv.at) und im **Rechtsinformationssystem des Bundes** (ris.bka.gv.at) können die Gesetzgebungsprozesse nachverfolgt werden. Es kann aufschlussreich sein, die Materialien, also Erläuterungen und Wirkungsfolgenabschätzungen, zu den Novellen, mit denen Überwachungsbefugnisse ausgeweitet oder eingeführt wurden, zu lesen. Dort wird z.B. die bisherige Praxis, die dabei angetroffenen Probleme und die gewünschte Anwendung der neuen Rechtslage beschrieben.
Die **Berichte des Rechnungshofes** können Aufschluss über Gesetzmäßigkeit, Häufigkeit und Kosten von Überwachungsmaßnahmen geben, insb. Im Abschnitt UG 11 Inneres. So gab es z.B. 2008 einen Bericht über ausgewählte Ermittlungsmaßnahmen.[26]

4.7 Überblick Strafdrohungen

Häufigkeit der Delikte und ihre Strafdrohung

Viele Überwachungsmaßnahmen dürfen nur für Ermittlungen von Straftaten mit bestimmten Strafdrohungen eingesetzt werden. Deswegen werden hier die häufigsten Delikte und ihre Strafdrohungen vorgestellt (alle Zahlen beziehen sich auf 2017). Die häufigsten Delikte, Diebstahl (121022 Anzeigen) und Sachbeschädigung (58151 Anzeigen), haben Strafdrohungen von bis zu 6 Monaten Freiheitsstrafe oder 360 Tagessätzen Geldstrafe, gefolgt von nicht erschwertem Einbruchsdiebstahl mit bis zu 3 Jahren Freiheitsstrafe. Das schwerste sehr häufige Delikt ist Einbruchsdiebstahl in Wohnstätten oder mit Waffen (13344 Anzeigen), der mit 6 Monaten bis 5 Jahren Freiheitsstrafe bedroht ist. Die häufigeren schwereren Delikte sind schwerer Diebstahl (2069 Anzeigen), schwere Nötigung (1919 Anzeigen) und fortgesetzte Gewaltausübung (1277 Anzeigen). Sehr schwere Delikte wie Mord (203 Anzeigen) und Vergewaltigung (817 Anzeigen) werden zum Vergleich angeführt, sind aber seltener – zumindest in der Anzeigenstatistik. (Grafik auf der linken Seite)
Nicht Teil der Anzeigenstatistik aber in den Verurteilungen am häufigsten sind Delikte nach dem Suchtmittelgesetz (im Jahr 2018 insgesamt 4954 Verurteilungen gegenüber 3030 wegen Körperverletzung und 2686 wegen einfachen Diebstahls). Hier reichen die Strafdrohungen von 6 Monaten Freiheitsstrafe für Erwerb, Besitz, etc. von Suchtgift zum eigenen Gebrauch bis zu 1–15 Jahren für Erwerb, Besitz, etc. von Suchtgift in größeren Mengen als Mitglied einer kriminellen Vereinigung.[27,28]

4.8 Polizeiliche Datenbanken

Oft liegt bei der Diskussion von Überwachung das Hauptaugenmerk auf den einzelnen Maßnahmen und der Beschaffung von Informationen. Wichtig ist daneben aber auch ein Blick auf die Datenbanken, die von der Polizei betrieben werden. Dort werden die Daten verschiedenen Ursprungs gespeichert und

analysiert. Wichtige Fragen für die Beurteilung, ob diese Datenbanken keine größeren Eingriffe als unbedingt notwendig darstellen, sind z.B., welche Personen und Organisationen darauf Zugriff haben, wie lange die Daten gespeichert werden, an wen die Daten übermittelt werden, und ob die Daten gut gesichert sind.
Beispiele für polizeiliche Datenbanken sind das „PAD – Protokollieren Anzeigen Daten“ und die „Erkennungsdienstlichen Evidenz – EDE“. Im Protokollierungssystem PAD werden Dokumentationen aller Amtshandlungen gespeichert. Diese Daten werden u.a. an Unternehmen wie IBM, Microsoft und RUBICON IT übermittelt.[29]
In der EDE werden erkennungsdienstliche Daten gespeichert. Diese sind Daten, die durch technische Verfahren zur Feststellung von biometrischen oder genetischen Daten, wie insbesondere die Abnahme von Papillarlinienabdrücken, die Vornahme von Mundhöhlenabstrichen, Fotografieren, die Vornahme von Messungen oder die Erhebung von Stimmproben, sowie die Feststellung äußerlicher körperlicher Merkmale und die Erhebung von Schriftproben eines Menschen zum Zweck der Wiedererkennung, erhoben worden sind. Dies ist u.a. zulässig, wenn eine Person im Verdacht steht, eine vorsätzliche Straftat begangen zu haben, wenn sie entweder dies im Rahmen einer kriminellen Verbindung getan hat, oder die erkennungsdienstliche Maßnahme der Vorbeugung gefährlicher Angriffe dient. Außerdem ist eine erkennungsdienstliche Maßnahme zulässig, wenn eine Identitätsfeststellung gerechtfertigt, aber auf andere Weise nicht möglich ist. Die Daten werden nach fünf Jahren gelöscht, wenn seit drei Jahren keine weitere erkennungsdienstliche Behandlung stattgefunden hat, oder wenn gegen die Person kein Verdacht mehr besteht. Auch diese Daten werden mit u.a. mit den Unternehmen IBM und Microsoft geteilt.[30]
Mit Stand 31.12.2018 waren in dieser Datenbank rund 604.000 Personen gespeichert, meistens mit drei Fotos des Kopfes bzw. des Gesichts aus unterschiedlichen Winkeln.[31]
Einen guten Überblick über polizeiliche Datenbanken, die personenbezogene Daten beinhalten gibt es auf der Webseite des BMI, wo datenschutzrechtliche Informationen gegeben werden: https://www.bmi.gv.at/402/information_datenschutz.aspx

4.9 Internationale Kooperationen

Gegenseitiger Datenzugriff

Es gibt eine große Anzahl an internationalen Abkommen, die den Austausch von personenbezogenen Daten im Rahmen der internationalen polizeilichen und justiziellen Kooperation regeln. Die Hauptinstrumente dieser Zusammenarbeit umfassen Datenbanken, die von zentralen Institutionen betrieben werden, genauso wie nationale Datenbanken, auf die gegenseitiger Zugriff besteht. Die verschiedenen Datenkategorien sind sehr umfassend und überschneiden sich zum Teil. Umso mehr zeigt sich die Notwendigkeit einer Evaluation der bestehenden Abkommen, insb. im Hinblick auf Rechtsschutzdefizite, wenn personenbezogene Daten den österreichischen Rechtsraum verlassen und die Rechteverfolgung (Auskunftsrechte, Anspruch auf Löschung unrichtiger Daten) von Betroffenen nicht gesichert ist oder den Betroffenen ungerechtfertigter Weise reale Nachteile drohen (No Fly Lists, Einreiseverweigerung, verstärkte Kontrollen etc.). Das Prinzip der Datensparsamkeit bei der Ermittlung personenbezogener Daten bekommt hier ein besonderes Gewicht.

Schengener Abkommen[32]
Nachdem 1985 das Schengener Abkommen von fünf EU-Mitgliedstaaten unterzeichnet wurde, um insb. stationäre Grenzkontrollen an den Binnengrenzen dieser Staaten abzuschaffen, wurde 1995 der Schengen-Raum durch Implementierung der beschlossenen Regelungen geschaffen. Die Kontrollen an den Außengrenzen der EU und das Visa-Regime wurden harmonisiert und die Koordination sowie Kooperation zwischen Polizei- und Justizbehörden wurden intensiviert. Heute ist das Schengen-Acquis Teil des EU-Acquis und alle EU- sowie EWR Mitgliedstaaten auch Schengen-Mitgliedstaaten (Schengener Durchführungsübereinkommen). Zentrales Instrument und technisches Herzstück der Polizeikooperation innerhalb des Schengen-Raums ist das „Schengener-Informationssystem“ (SIS). Das SIS ist ein elektronisches Personen- und Sachfahndungssystem, in dem Datenbanken u.a. in den Bereichen Festnahmeersuchen, Übergabe und Auslieferung, Gefahrenabwehr und Kfz-Fahndung enthalten sind. Als nationale Kontakt- und Anlaufstelle existiert in jedem Mitgliedstaat ein SIRENE (Supplementary Information Request at the National Entry)-Büro. Innerhalb des SIS kommt ein sog. „Hit / No Hit“-Verfahren zur Anwendung. Wenn eine Datenbank-Abfrage einen Treffer erzielt, wird der nachfolgende Informationsaustausch im Rahmen der Rechtshilfe zwischen den nationalen SIRENE-Büros bewerkstelligt. Das SIS besteht aus zwei Komponenten, einem Zentralrechner in Strasbourg (C-SIS) und nationalen Einheiten (N-SIS) in den Mitgliedstaaten. Die zweite Generation des Systems (SIS II) wurde nach langer Vorlaufzeit schließlich 2013 implementiert.

DNA Daten Fingerabdrücke, Zentrales Fahrzeugregister

Vertrag von Prüm, der Ratsbeschluss Prüm und das bilaterale „Prüm-like“ Abkommen zwischen Österreich und den USA[33]
Im Mai 2005 unterzeichneten sieben EU-Mitgliedstaaten den sog. Prümer Vertrag, dem seither mehrere andere EU-Mitgliedstaaten beigetreten sind. Mit diesem multilateralen Übereinkommen sollte die grenzüberschreitende Polizeikooperation, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration, verbessert und ausgeweitet werden. Der Vertrag regelt den automatisierten Austausch von DNA-Daten, Fingerabdruckdaten und Daten aus Kraftfahrzeugregistern zwischen den Staaten. Am 26. August 2008 ist der Ratsbeschluss Prüm in Kraft getreten. Hierdurch wurden die wesentlichen Inhalte des Prümer Vertrages in den Rechtsrahmen der Europäischen Union überführt und gelten damit für sämtliche EU-Mitgliedstaaten. Polizei- und Strafverfolgungsbehörden können danach direkt auf bestimmte Datenbanken zugreifen, die von den Behörden der anderen Mitgliedstaaten geführt werden (DNA- sowie Fingerabdruckdatenbanken und Zentrale Fahrzeugregister).
Der Prüm-Mechanismus verwirklicht ein Hit / No-Hit Verfahren. Wird in einer Datenbankabfrage ein Treffer erzielt, werden die Informationen im Rahmen der bilateralen Kooperation bzw. Rechtshilfe ausgetauscht. Österreich hat mit den USA daneben das bilaterale sog. Prüm-like Abkommen geschlossen. Das Prüm-like Abkommen übernimmt nicht sämtliche informationelle Kooperationsformen des Prümer Vertrages. Nicht Gegenstand des Abkommens sind insbesondere der Zugriff auf Fahrzeugregisterdaten oder der Massenabgleich von DNA-Profilen aus offenen Spuren. Auch eine Rechtshilfe in Form der Gewinnung bzw. Untersuchung von menschlicher DNA ist nicht vorgesehen.

Passwesen, Grenzkontrolle, Sicherheits-, Kriminal- u. Fremdenpolizeiliche Zwecke

Bundesgesetz über die internationale polizeiliche Kooperation (Polizeikooperationsgesetz - PolKG)
Das österreichische Polizeikooperationsgesetz (PolKG) gibt es seit 1997. Ziel des Gesetzes ist es, die einzelnen Bereiche der Kooperation, wie Interpol, Europol und Schengen, in einen gemeinsamen rechtlichen Rahmen einzufügen, der sowohl organisationsrechtliche Regelungen als auch allgemeine Grundsätze für die Mitwirkung österreichischer Sicherheitsbehörden an der internationalen polizeilichen Zusammenarbeit umfasst. Regelungsgegenstand des Polizeikooperationsgesetzes ist die internationale polizeiliche Amtshilfe, beschränkt auf sicherheits-, kriminal- und fremdenpolizeiliche Zwecke sowie auf Zwecke des Passwesens und der Grenzkontrolle. Unter Amtshilfe i.S.d PolKG ist einerseits die auf den Austausch von Daten gestützte Zusammenarbeit österreichischer Sicherheitsbehörden mit ausländischen Sicherheitsbehörden bzw. mit internationalen Sicherheitsorganisationen (Europol, Interpol) und andererseits die operative Kooperation zu verstehen.

Polizeiliche und Justizielle Zusammenarbeit (Lissabon-Vertrag)[34]
Durch den Vertrag von Lissabon wurde die vormals dritte Säule der Europäischen Gemeinschaft (Polizeiliche und Justizielle Zusammenarbeit in Strafsachen, PJZS) in das supranationale Unionsrecht überführt.[35] Dem EuGH ist die Kontrolle der mitgliedstaatlichen Maßnahmen innerhalb dieses Rahmens entzogen.

Statuten IKPO-Interpol[36]
Die Internationale Kriminalpolizeiliche Organisation (IKPO-Interpol) mit Hauptsitz in Lyon dient dem schnellen und sicheren Austausch über allgemeinpolizeiliche und fallbezogene Erkenntnisse zwischen den mehr als 190 Mitgliedsländern. IKPO-Interpol stellt dazu auf der rechtlichen Grundlage der Interpol-Statuten ein weltumspannendes, Informations- und Kommunikationsnetz zur Verfügung, führt Kriminalakten und Datenbanken und erstellt strategische sowie operative Kriminalitätsanalysen. Zudem gibt IKPO-Interpol Fahndungsnotierungen (*Notices*) heraus. Dabei haben die für das Generalsekretariat von Interpol tätigen Beamt_innen keine Exekutivbefugnisse zur Strafverfolgung. Ausschließlich das jeweilige nationale Recht in den Mitgliedstaaten bestimmt, welche exekutiven Maßnahmen zur Strafverfolgung von den eigenen nationalen Beamt_innen durchgeführt werden dürfen.

Europol-Übereinkommen (bzw. seit 2009 Europol-Ratsbeschluss)
Mit dem Europol-Ratsbeschluss wurde Europol zum 01.01.2010 in den Rechtsrahmen der EU überführt und ist seitdem eine EU-Agentur mit eigener Rechtspersönlichkeit. Europol hat zum Ziel, die Arbeit der zuständigen Behörden in den Mitgliedstaaten und deren Zusammenarbeit bei der Prävention und Bekämpfung von organisierter Kriminalität, Terrorismus und anderen Formen schwerer Kriminalität zu unterstützen und zu verstärken. Europol ist zuständig, wenn mindestens zwei Mitgliedstaaten betroffen sind.
Dazu speichert und analysiert Europol Informationen der Mitgliedstaaten und ermöglicht so deren Informationsaustausch. Die zuständigen Behörden in den Mitgliedstaaten können das Europol-Informationssystem abfragen, in dem von den Mitgliedstaaten gelieferte Daten zu Straftaten und -täter_innen gespeichert werden. Gegenseitige Bezüge von Ermittlungsverfahren, die in den einzelnen Mitgliedstaaten geführt werden, werden sichtbar. Durch sog. Analysedateien soll Europol Zusammenhänge zwischen Straftaten aufklären und den Mitgliedstaaten operative und strategische Analysen zur Verfügung stellen.

Leseempfehlung: Über die verschiedenen Datenbanken der EU gibt es hier einen Überblick: http://db.eurocrim.org/db/en/doc/2698.pdf (S. 3)

Endnoten

1 Vgl. *Zerbes*, Spitzeln, Spähen, Spionieren. Sprengung strafprozessualer Grenzen durch geheime Zugriffe auf Kommunikation (2010) 243.
2 Erläuterungen zur Regierungsvorlage 25 d. B. XXII. GP, 26. Vgl. auch *Adensamer/Klausner,* Ich weiß, was du nächsten Sommer getan haben wirst. Predictive Policing in Österreich, juridikum 3/2019, 419-431.
3 Vgl. *Ennöckl*, Der Rechtsschutz gegen sicherheitspolizeiliche Maßnahmen nach Inkrafttreten des Strafprozessreformgesetzes, Juristische Blätter 07/2008, 417.
4 *Heißl,* PStSG. Polizeiliches Staatsschutzgesetz (2016) 35 Rz 18.
5 *Adensamer/Sagmeister*, Das Polizeiliche Staatsschutzgesetz. Darstellung und Kritik, recht tolerant. RichterInnenwoche 2016 in Hermagor/Tröpolach 30. Mai – 3. Juni, Schriftenreihe des Bundesministeriums für Justiz – Band 164, 65 (72).
6 *Heißl*, PStSG. Polizeiliches Staatsschutzgesetz (2016) 31 Rz 1.
7 Ebd. 31 Rz 3.
8 Vgl. *Adensamer/Klausner*, Ich weiß, was du nächsten Sommer getan haben wirst, 419-431.
9 Erwägungsgrund 7, PNR-Richtlinie (EU) 2016/681.
10 Änderung BGBl I 2004/19, 16.12.2010, G 259/09 u.a., Gewaltentrennungsnovelle: BGBl I 2012/51. Vgl. auch *Öner/Walcher*, Zum Einspruch nach § 106 StPO, ÖJZ 2014/150, 999 ff, Vgl. auch *Ennöckl*, Der Rechtsschutz gegen sicherheitspolizeiliche Maßnahmen Jbl 7/2008.
11 Vgl. *Kretschmann*, Das Wuchern der Gefahr. Einige gesellschaftstheoretische Bemerkungen zur Novelle des Sicherheitspolizeigesetzes 2012, juridikum 3/2012, 320-333.
12 Vgl. *Rechtsschutzbeauftragter des Innenministeriums*, Stellungnahme 6 zu ME/110 XXIV. GP, 9. (https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_03454/imfname_408709.pdf)
13 *Heißl*, PStSG. Polizeiliches Staatsschutzgesetz (2016) 36 Rz 21.
14 Vgl. mit weiteren Nachweisen *Heißl*, PStSG. Polizeiliches Staatsschutzgesetz (2016) 34 Rz 14.
15 Vgl. *Adensamer/Sagmeister*, Die umkämpfte Verfassung. Kommentar zum Polizeilichen Staatsschutzgesetz, juridikum 3/2015, 305.
16 Dazu kritisch *Heißl*, PStSG, Polizeiliches Staatsschutzgesetz, Kurzkommentar (2016) 136 Rz 12.
17 Vgl. und siehe für weitere Nachweise *Adensamer/Sagmeister,* Das Polizeiliche Staatsschutzgesetz. Darstellung und Kritik, recht tolerant, 12.
18 VfGH G 72-74/2019, G 181-182/2019, vom 11.12.2019, (https://www.vfgh.gv.at/downloads/VfGH_Verkuendung_11.12.2019_G_72_2019.pdf, 13f.)
19 Rechnungshof, Wirkungsbereich des Bundesministerien Inneres und Justiz. Ausgewählte Ermittlungsmaßnahmen, Bund 2008/10, https://www.rechnungshof.gv.at/rh/home/home/Ausgewaehlte_Ermittlungsmassnahmen_1 (09.01.2020).
20 Vgl. *Bundesministerium Verfassung, Reformen, Deregulierung und Justiz*, Wahrnehmungsbericht des Bundesministers für Verfassung, Reformen, Deregulierung und Justiz Dr. Clemens Jabloner. Befund. Maßnahmen für eine moderne und qualitätsvolle Justiz. 11. November 2019, 32f. (https://www.justiz.gv.at/file/2c94848b6d50e800016e6a285abf00ed.de.0/wahrnehmungsbericht_hbm%20jabloner.pdf)
21 OGH, 16.12.2010, 13Os130/10g (13Os136/10i).
22 *Gahleitner/Windhager,* Redaktionsgeheimnis 2.0 – Sind Userdaten von § 31 MedienG geschützt? Medien und Recht 3/2013, 108.
23 ZIR 2013/3, 187 (https://h-i-p.at/Content/uploads/2018/04/ZIR3_Koukal.pdf) und MR 2013/3, 107, (http://weberling.de/images/Beitraege/windhager-mr-2013-3-107.pdf)
24 Vgl. *Böszörmenyi/Schweighofer*, Tracking of Financial Movements, in *Schweighofer/Kummer/Hötzendorfer* (Hrsg), Transparenz. Tagungsband des 17. Internationalen Rechtsinformatik Symposions IRIS 2014 (2014) 617-624. Siehe insb. auch EuGH 18.07.2013, C584/10 P, C593/10 P und C595/10 P, Kadi.
25 Vgl. die grundsätzliche Kritik von *Fischer,* Bundesrichter in Karlsruhe: Woher haben Sie dieses Geld?, Zeit Online, 13.10.2015, http://www.zeit.de/gesellschaft/zeitgeschehen/2015-10/geldwaesche-fischer-im-recht/komplettansicht (01.07.2016).
26 Vgl.Bericht: https://www.rechnungshof.gv.at/rh/home/home/Ausgewaehlte_Ermittlungsmassnahmen_1 (09.01.2020)
27 Vgl. Kriminalitätsbericht des BMI 2017: https://www.bmi.gv.at/508/files/SIB_2017/03_SIB_2017-Kriminalitasetsbericht_web.pdf
28 Vgl. Statistik Austria: https://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/soziales/kriminalitaet/index.html (09.01.2020)

29 Zu PAD siehe: https://www.bmi.gv.at/402/files/Informationen/Sektion_II/BF_PAD-Protkollieren_Anzeigen_Daten_V2.pdf.
30 Zu EDE siehe: https://www.bmi.gv.at/402/files/Informationen/Sektion_II/BF_Erkennungsdienstliche_Evidenz-EDE_V2.pdf.
31 https://fragdenstaat.at/anfrage/gesichtserkennung/4519/anhang/Beantwortung-GFE_AuskPflG_2019_09_21_Ranftl_geschwaerzt.pdf.
32 Dazu: *Lachmayer*, Die Wirkung von „Schengen" nach innen – Polizeiliche Informationsnetzwerke ohne Grenzen? juridikum 2/2009, 104.
33 *Kunnert*, „Tausche Visafreiheit gegen Datenschutz" - Die neue Polizeikooperation auf Basis des US-Österreichischen „Prüm-like" Abkommens, Jahrbuch Datenschutzrecht und E-Governmen t 2012, 193.
34 *Rieser-Angulo García/Bauer*, Polizeiliche und justizielle Zusammenarbeit in der EU (Teil II) Polizeilicher Informationsaustausch und Datenschutz, SIAK-Journal 2013 Heft 3, 4.
35 Vgl. http://www.europarl.europa.eu/aboutparliament/de/displayFtu.html?ftuId=FTU_5.12.7.html (01.07.2016) bzw. http://www.europarl.europa.eu/aboutparliament/de/displayFtu.html?ftuId=FTU_5.12.6.html (01.07.2016).
36 Vgl. http://www.interpol.int/About-INTERPOL/Legal-materials/The-Constitution (01.07.2016).

5 Die verdeckte Ermittlung

Definition

Die verdeckte Ermittlung ist das Einholen von Auskünften durch Polizeibeamt_innen, die sich aber nicht als solche zu erkennen geben.[1] Dabei sind die Beamt_innen aktiv ins Geschehen eingebunden und erlangen Informationen im Gespräch und durch Befragung. Diese aktive Rolle einerseits und die Täuschung über die wahre Identität von Beamt_innen andererseits sind die Kernpunkte der verdeckten Ermittlung. Da Eingriffe grundsätzlich als schwerwiegender gesehen werden, wenn sie heimlich geschehen, war schon in den Grundrechtskodifikationen des 19. Jahrhunderts dafür besonderer Schutz vorgesehen.[2]

§ 54 Abs. 3 SPG

Dies wird unter anderem im Sicherheitspolizeigesetz (SPG) klargestellt, wo für die verdeckte Ermittlung der sonst bei Ermittlungsmaßnahmen notwendige Hinweis auf den amtlichen Charakter nicht vorgesehen ist. Im Rahmen der Sicherheitspolizei soll die verdeckte Ermittlung laut Erläuterungen vor allem zur Bekämpfung bandenmäßiger und organisierter Kriminalität eingesetzt werden, aber auch zur Aufklärung von Entführungen. Die Befugnis zur verdeckten Ermittlung umfasst darüber hinaus „selbstverständlich auch die Befugnis zur Observation“.[3]

§ 54a SPG

Neben diesem Einsatz von Beamt_innen erlaubt das SPG außerdem auch den Einsatz von sogenannten Vertrauenspersonen, also Privatpersonen, die in bestimmten, als gefährlich eingeschätzten Gruppen im Auftrag der Sicherheitsbehörde ermitteln sollen.[4]

Scheinidentität

Auch der Aufbau einer umfassenden Scheinidentität, einer sogenannten „Legende“[5], durch die Herstellung offizieller Ausweise, die eine falsche Identität für Beamt_innen ausgeben, ist im Rahmen der verdeckten Ermittlung möglich (nicht aber für Vertrauenspersonen). Dies sei notwendig, weil in kriminellen Organisationen oftmals „Überprüfungen“ üblich seien, ohne die man in deren Strukturen nicht eindringen könne.[6] Zu diesem Zweck gebe es „verschiedenste legendenunterstützte Maßnahmen, umfangreiche Legendenmodule und Tarnpapiere“.[7]

§ 131 StPO

Auch die Kriminalpolizei darf verdeckt ermitteln, hier ist die verdeckte Ermittlung aber nicht beschränkt auf das Einholen von Auskünften, sondern umfasst jeden kriminalpolizeilichen Einsatz. Die Materialien zur StPO führen

§ 5 Abs. 3, § 25 StPO

dazu aus: „Das ‚Verlocken‘ zu einem Geständnis ist in jedem Fall unstatthaft.“[8] Wie die Abgrenzung zum Verlocken passieren soll, wird nicht näher ausgeführt. Dass Beschuldigte nicht zu einem Geständnis verlockt werden dürfen, entspricht dem Prinzip der Selbstbelastungsfreiheit (Nemo Tenetur Prinzip), das auch durch das Recht auf ein faires Verfahren geschützt ist.

➲ *9.5 Faires Verfahren*

5.1 Voraussetzungen

Die verdeckte Ermittlung ist im Rahmen der Sicherheitspolizei, der Kriminalpolizei und im Bereich des Verfassungsschutzes nach unterschiedlichen Voraussetzungen erlaubt.[9]

§ 54 Abs. 3ff, § 54a SPG

Nach dem Sicherheitspolizeigesetz: Für den Einsatz von verdeckter Ermittlung nach dem SPG muss ein Aufgabenbereich des SPG vorliegen und ohne die verdeckte Ermittlung die Abwehr gefährlicher Angriffe oder einer kriminellen Verbindung gefährdet bzw. erheblich erschwert sein. Da jede vorsätzliche Straftat nach dem Strafgesetzbuch ein gefährlicher Angriff sein kann, ist die Voraussetzung der Verfolgung krimineller Verbindungen leicht umgehbar. Das Betreten von Wohnungen oder anderen vom Hausrecht geschützten Räumen (z.B. Privatordination von Ärzt_innen, Geschäftsräume, Betriebsräume, Kellerabteile oder geschlossene Fahrzeuge[10]) ist dabei nur mit Einverständnis des_der Inhaber_in und nicht durch Täuschung über eine Zutrittsberechtigung erlaubt.

Die verdeckte Ermittlung mit Ton- und Bildaufzeichnungsgeräten ist zur Abwehr einer kriminellen Verbindung nur zulässig, wenn eine Handlung mit mehr als einem Jahr Freiheitsstrafe als Strafdrohung zu erwarten ist. Es ist nur erlaubt, Äußerungen oder Verhalten aufzuzeichnen, wenn diese öffentlich stattfinden oder in Anwesenheit eine_r Beamt_in erfolgen.

Scheinidentität
§ 54a SPG

Legenden, also Ausweise mit falscher Identität, können auf Verlangen des_der Innenminister_in von Behörden ausgestellt werden, die generell zur Ausstellung von Urkunden berechtigt sind. Sie können nur für Polizeibeamt_innen ausgestellt werden, nicht für Vertrauenspersonen.[11] Die Ausweise dürfen nur für Zwecke der verdeckten Ermittlung verwendet werden und müssen eingezogen werden, wenn sie nicht mehr benötigt werden. Jeder einzelne Anwendungsfall muss von den Beamt_innen dokumentiert werden.

§ 131 StPO

Nach der Strafprozessordnung: Voraussetzung für verdeckte Ermittlungen nach der StPO ist, dass sie zur Aufklärung von Straftaten erforderlich erscheinen. Das Betreten von Wohnungen oder anderen vom Hausrecht geschützten Räumen (z.B. Privatordinationen von Ärzt_innen, Geschäftsräume, Betriebsräume, Kellerabteile, geschlossene Fahrzeuge[12]) ist nur mit Einverständnis der Inhaber_innen und nicht durch Täuschung über eine Zutrittsberechtigung zulässig.

Systematische, über längere Zeit durchgeführte verdeckte Ermittlungen sind nur unter besonderen Voraussetzungen möglich. Was „systematisch und längerfristig“ bedeutet, geht aus den Erläuterungen nicht hervor.[13] Generell „wurden bisher wenig brauchbare Hinweise geliefert“, abgesehen davon, dass die Ermittlung sowohl längerfristig als auch systematisch sein muss, und dass es sich dabei um „planmäßiges, gezieltes, gegliedertes Vorgehen“ handelt.[14] Die Voraussetzungen sind:

- Aufklärung einer vorsätzlichen Straftat mit mehr als einem Jahr Strafdrohung sonst wesentlich erschwert

  ODER

- Verhinderung einer im Rahmen einer kriminellen/terroristischen Vereinigung bzw. kriminellen Organisation geplanten Straftat sonst wesentlich erschwert

  UND

- Anordnung durch die Staatsanwaltschaft

Legenden, also Ausweise mit falscher Identität für Beamt_innen, auszustellen ist dann zulässig, wenn es für Aufklärung oder Verhinderung einer Straftat/eines verfassungsgefährdenden Angriffs unerlässlich ist.

§ 11 Abs. 1 Z 2 PStSG

Voraussetzungen nach dem Polizeilichen Staatsschutzgesetz (Verfassungsschutz):

➲ *4.1.3 Die erweiterte Gefahrenerforschung und der verfassungsgefährdende Angriff*

- Aufgabenbereich des PStSG (erweiterte Gefahrenerforschung oder vorbeugender Schutz vor verfassungsgefährdenden Angriffen) liegt vor
- Erfüllung der Aufgabe wäre sonst aussichtslos oder erheblich erschwert
- Ermächtigung des Rechtsschutzbeauftragten

5.2 Geschichte

BGBl 1991/566

Im Bereich der Sicherheitspolizei war die verdeckte Ermittlung bereits in der ursprünglichen Fassung des Sicherheitspolizeigesetzes aus dem Jahr 1993 enthalten und wurde seither mehrere Male geändert. Auch die „Ermittlung personenbezogener Daten mit Bild- und Tonaufzeichnungsgeräten“ durfte unter den Voraussetzungen für die verdeckte Ermittlung bereits 1993 verdeckt erfolgen. 1998 wurde die gesetzliche Möglichkeit geschaffen, eine Legende aufzubauen, also falsche Ausweise einzusetzen, da dies laut Erläuterungen „vielfach unabdingbare Voraussetzung erfolgreicher Tätigkeit“ sei und außerdem dem „Schutz verdeckt ermittelnder Beamter“ diene. Im Jahr 2000 trat eine Novelle in Kraft, die die verdeckte Ermittlung nicht mehr nur bei „bandenmäßiger“ und „organisierter“ Kriminalität sondern – niederschwelliger also – nun auch bei Ermittlungen zu „kriminellen Verbindungen“ zuließ. Außerdem wurden von dem verdeckten Einsatz von Ton- und Bildaufzeichnungsgeräten nichtöffentliche, nicht in Anwesenheit der oder außerhalb des Wahrnehmungsbereiches von Ermittlungsbeamt_innen erfolgende Äußerungen oder Verhalten ausgenommen. Auch die Einschränkung auf die Gefahr von mit mehr als einjährige Strafe bedrohten Handlungen für verdeckte Ermittlungen bei kriminellen Verbindungen wurde eingeführt. 2006 wurde der Einsatz der verdeckten Ermittlung außerdem auf den Bereich der erweiterten Gefahrenerforschung ausgedehnt, also die Beobachtung einer Gruppe, in deren Umfeld mit Kriminalität, die mit schwerer Gefahr für die öffentliche Sicherheit verbunden ist, zu rechnen ist. Von 2012 bis 2016 war diese erweiterte Gefahrenerforschung auch für Ermittlungen über Einzelpersonen vorgesehen, dann aber bei Einführung des PStSG wieder aufgehoben (inhaltlich aber bloß in den Aufgabenbereich des vorbeugenden Schutzes von Rechtsgütern verschoben).[15]

➲ *4. Überwachungsbefugnisse im Überblick*

BGBl I 2000/85

BGBl I 2005/158

➲ *4.1.3 Die erweiterte Gefahrenerforschung*

BGBl I 2016/5

2016 trat dann jene Novelle in Kraft, die den Einsatz von Vertrauenspersonen zur verdeckten Ermittlung ermöglichte. Schon 2002 wurde mit § 54b SPG die sogenannte Vertrauenspersonenevidenz eingerichtet, die den_die Innenminister_in ermächtigte, Daten über Informant_innen, „die den Sicherheitsbehörden gegen Belohnung Informationen über gefährliche Angriffe weitergeben, in einer eigenen Datenbank zu verarbeiten“[16]. Diese Evidenz-Datenbank sollte Auskünfte darüber geben, welche Menschen für welche Sicherheitsbehörden Informationen anliefern, und Vertrauenswürdigkeit und Schutz der Informant_innen fördern.[17] Nicht erfasst werden sollten laut damaligen Erläuterungen aber „Menschen, die den Sicherheitsbehörden sicherheitspolizeilich relevante Informationen ohne Gegenleistung weitergeben oder die von Gesetzes wegen zur Anzeige verpflichtet sind“.[18] In unbedingt erforderlichen Fällen sollten darin auch sensible und strafrechtsbezogene Daten über Betroffene verarbeitet werden dürfen, Auskünfte aus der Evidenz sollten nur Sicherheitsbehörden erhalten.[19] Die verdeckte Ermittlung durch Vertrauenspersonen, also nicht nur der Kauf von Informationen im Nachhinein sondern die Beauftragung zur Informationsbeschaffung im Vorhinein, war dadurch aber nach herrschender Lehre noch nicht erlaubt. Laut abweichender Meinung in der Lehre war aber auch dieser Einsatz von Vertrauenspersonen schon davor zulässig.[20] Zumindest im Bereich der Kriminalpolizei wurde dies laut Zerbes schon vor einer expliziten Ermächtigung so gehandhabt, siehe den Abschnitt zur Strafprozessordnung in diesem Kapitel. Erst die erwähnte Novelle im Jahr 2016 ließ aber ausdrücklich die verdeckte Ermittlung durch Vertrauenspersonen zu und führte dementsprechend bestimmte Führungs-, Überwachungs- und Dokumentationspflichten ein.[21]

§ 54b SPG BGBl I 2002/104

Einführung des Einsatzes von Vertrauenspersonen

§ 11 Abs. 1 Z 2 PStSG

Zeitgleich wurde auch das Polizeiliche Staatsschutzgesetz (PStSG) eingeführt, in dem die verdeckte Ermittlung, inklusive des Einsatzes von Vertrauenspersonen, von Beginn an normiert war, und im Wesentlichen die Befugnisse aus dem SPG übernommen wurden, allerdings in Verbindung mit den dem PStSG eigenen Aufgaben, die auf wesentlich vageren Verdachten beruhen: Als Aufgabe geht es hierbei nämlich (wie generell im PStSG) um die erweiterte Gefahrenerforschung, also die Beobachtung von Gruppierungen, bevor sie kriminelle Handlungen setzen, und um den vorbeugenden Schutz vor verfassungsgefährdenden Angriffen, also etwa terroristische Straftaten nach den §§ 278b bis 278f StGB[22].

Bis 1974 waren im Strafprozessrecht „weder Täuschungen noch Tarnungen“ erlaubt.[23] Erst 2008 erhielt die Polizei die ausdrückliche Befugnis zur verdeckten Ermittlung, inklusive des Einsatzes von Vertrauenspersonen. Laut Zerbes ließ sich die Befugnis zur verdeckten Ermittlung aber auch schon aus der früheren Fassung der StPO ableiten, nämlich aus dem kleinen Lausch- und Spähangriff, der allerdings, anders als die aktuelle explizite Befugnis zur verdeckten Ermittlung, ohne technische Hilfsmittel eine richterliche Genehmigung benötigt.[24] Dennoch waren aber bereits damals Observation, verdeckte Ermittlung und auch Scheingeschäfte Routine in der polizeilichen Arbeit, laut Zerbes legte man dem eine „überdehnte Auslegung“ des früheren § 24 StPO zugrunde. Dadurch hätten in den 70er und 80er Jahren bereits verdeckte Ermittler_innen und Vertrauenspersonen „Kontakte geknüpft [und] Zeugen sowie verdächtig scheinende Personen befragt“.[25] Auch das Parlament billigte dies 1980 nach heftigen Diskussionen.[26]

BGBl I 2009/52

§ 136 Abs. 1 Z 2

➲ *4.2 Überwachungsbefugnisse im Überblick*

6. Videoüberwachung

5.3 Beispiele aus der Praxis

Die verdeckte Ermittlung und der Einsatz von Vertrauenspersonen waren schon mehrmals im Zuge aufsehenerregender Fälle Thema öffentlicher Debatten. Ein prominentes Beispiel aus Österreich waren die Ermittlungen im sogenannten Tierschützer-Prozess, bei dem Tierrechtsaktivist_innen wegen des Verdachts der Gründung einer kriminellen Organisation gem. § 278a StGB angeklagt wurden. Dabei war eine Beamtin mit dem Decknamen Danielle Durand von 2007 bis 2008 verdeckt ermittelnd tätig. Der zuständige Beamte sprach von einem Einsatz ausschließlich „zur Gefahrenabwehr laut Sicherheitspolizeigesetz“, laut seinen Aussagen befand man sich also nicht im Bereich der StPO.[27] Besonders kritisch gesehen wurde, dass die verdeckte Ermittlerin sexuelle Beziehungen mit einer beobachteten Person unterhielt, und diese auch noch in der Untersuchungshaft besuchte, zu einem Zeitpunkt also, wo die Verhinderung gefährlicher Angriffe als Befugnisgrundlage zumindest fraglich erscheint. Noch problematischer ist, dass die Betroffenen erst aufgrund eines Hinweises und mithilfe eines Detektivs die Information erlangen konnten, dass es überhaupt zu dieser verdeckten Ermittlung gekommen war, was in Bezug auf das Recht auf volle Akteneinsicht äußerst problematisch ist.[28] Da die verdeckte Ermittlung nach Eröffnung strafrechtlicher Ermittlungen die Voraussetzungen der StPO erfüllen müsste, hätte es dafür eine staatsanwaltliche Genehmigung benötigt, diese wurde aber nie erteilt.[29]

Tierschützerprozess

Im Endeffekt wurde die verdeckte Ermittlung vor dem Verwaltungsgericht als rechtskonform erkannt. Da die Ermittlung unter das SPG subsumiert wurde, sei keine Ermächtigung durch die Staatsanwaltschaft notwendig, und würde man die Ermittlung als im Bereich der StPO angesiedelt betrachten, sei das Verwaltungsgericht nicht zuständig, war die damalige Argumentation des Richters.[30] Im Zuge des BVT-Untersuchungsausschusses gerieten die Ermittlungen um die Tierrechtsaktivist_innen auch in Bezug auf eventuelle politische Einflussnahme Jahre später wieder in Diskussion.[31]

In Deutschland war in Bezug auf den Nationalsozialistischen Untergrund die Praxis, Vertrauenspersonen in rechtsextreme Kreise einzuschleusen, stark in die Kritik gekommen, da dadurch nicht zuletzt neonazistische Strukturen mittelbar von staatlicher Seite mitfinanziert wurden, da das Vertrauen der Gruppen nur durch aktive Mithilfe erlangt werden konnte und außerdem die tatsächliche Vertrauenswürdigkeit der beauftragten Personen stark zweifelhaft war. Aber auch der Umgang des Verfassungsschutzes mit den erlangten Informationen war äußerst fragwürdig. So sollen V-Leute direkten Kontakt mit den Terrorist_innen gehabt haben, was bedeuten würde, dass sie Informationen nicht weitergeleitet haben (ein „mutmaßlicher Terrorhelfer in Staatsdiensten“[32], schrieb etwa der Spiegel), außerdem sollen auch die Ermittlungsbehörden unterein-

ander Informationen nicht rechtzeitig weitergegeben haben.[33] In Großbritannien wurde sogar über Polizeibeamte berichtet, die im Rahmen von verdeckten Ermittlungen und unter falscher Identität Kinder zeugten.[34]

Schutz vor Enttarnung der Ermittler_innen

Für die Ermittler_innen selbst kann es gefährlich sein, enttarnt zu werden. Daher haben sie ein besonderes Interesse daran, dass Bildaufnahmen von ihnen nicht veröffentlicht werden.[35] Im Zuge der Hausdurchsuchung am 28.02.2018 im BVT, die im Nachhinein als rechtswidrig erkannt wurde[36], wurden unter anderem Informationen über verdeckte Ermittler_innen im rechtsextremen Milieu durch FPÖ-nahe Beamt_innen beschlagnahmt. Goldgruber hatte als Generalsekräter der FPÖ im Innenministerium schon zuvor versucht, von BVT-Chef Gridling Informationen über in Burschenschaften ermittelnde Beamt_innen zu erlangen, welche dieser aber nicht herausgab.[37] Diese Vorgänge waren Teil des Grundes für die Einsetzung des BVT-Untersuchungsausschusses am 24.04.2018. Im Zuge dessen wurden Personalakten aus dem BVT an den Ausschuss geliefert, inklusive einer Liste von Ermittler_innen im Extremismusbereich. Das Bekanntwerden ihrer Identitäten hätte laut Gridling Lebensgefahr für die betroffenen Ermittler_innen nach sich ziehen können.[38]

5.4 Häufigkeit

Wie auch bei anderen Überwachungsmaßnahmen ist hier die Datenlage dünn. Das klarste Bild liefern parlamentarische Anfragen und Anfragen über das Portal fragdenstaat.at sowie der Bericht des Rechtsschutzbeauftragten.

Verdeckte Ermittlungen nach SPG und PStSG 2013-2018

Die untenstehende Graphik zeigt, dass es zwischen 2013 und 2018 zwischen 40 und 70 verdeckte Ermittlungen nach dem SPG und dem PStSG gab. Davon umfasst sind sowohl Einsätze von verdeckten Ermittler_innen als auch der verdeckte Einsatz von Ton- und Bildaufzeichnungsgeräten. Vor 2013 sind keine Daten über verdeckte Ermittlungen nach dem SPG verfügbar.[39] Die Zahlen für das Jahr 2013 sind allerdings mit Vorsicht zu lesen, da es in einer Anfragebeantwortung von 2017 hieß, diese seien erst ab Juni 2013 erfasst worden.[40]

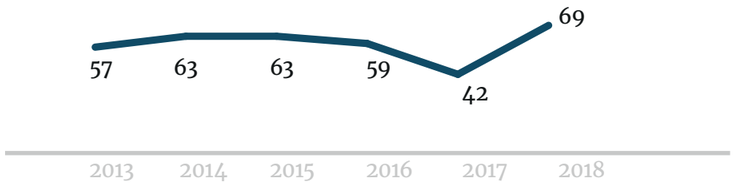


Abb. 4.: Verdeckte Ermittlungen nach SPG und PStSG 2013-2018
Quelle: Bundesministerium, Anfragebeantwortung auf Fragdenstaat.at vom 12.11.2019

Abb. 5, nächste Seite: Verdeckte Ermittlung im Sicherheitsbericht Zeitraum 2009
Quelle: Bundesministerium für Inneres, Sicherheitsbericht 2009

Sicherheitsbericht 2009: Die Sicherheitsberichte der letzten Jahre sind wenig aufschlussreich, lediglich der Bericht über das Jahr 2009 gibt eine Momentaufnahme über verdeckte Ermittlungen.

Verdeckte Ermittlung im Sicherheitsbericht Zeitraum 2009

VE-Einsätze SPG	1.504
VE-Einsätze StPO	637
Scheinkäufe	203
Festnahmen	404
Bearbeitete Legendierungsfälle	273
Beantrage Tarndokumente	58
Neue Legenden	24
Auflösung von Legenden	15

2009 lagen die Schwerpunkte der verdeckten Ermittlungen bei Bekämpfung von Eigentumskriminalität, Suchtmitteldelikte (in dem Jahr kam es zu 203 Scheinkäufen) und der Verbreitung von Falschgeld.[41] Auch in jüngeren Jahren waren Suchtmitteldelikte laut dem Rechtsschutzbeauftragten die häufigsten Einsatzbereiche von verdeckten Ermittlungen.[42] Es gab 861 Vertrauenspersonen, von denen 105 neu registriert waren. Heute wird die Anzahl von Vertrauenspersonen nicht mehr veröffentlicht. Diese Information könnten, wie auch Informationen über Bezahlung und die Voraussetzung von Auszahlungen, „aufgrund der dadurch bewirkten erheblichen Gefährdung der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit nicht öffentlich bekanntgegeben werden“, so das Innenministerium in einer Anfragebeantwortung.[43] Die Informationen könnten missbraucht werden, um sich ungerechtfertigte finanzielle Vorteil zu verschaffen.[44] Die Zunahme von Legendierungsfällen von 2006-2009 von 149 auf 273 deutet darauf hin, dass diese Maßnahme häufiger eingesetzt wurde.

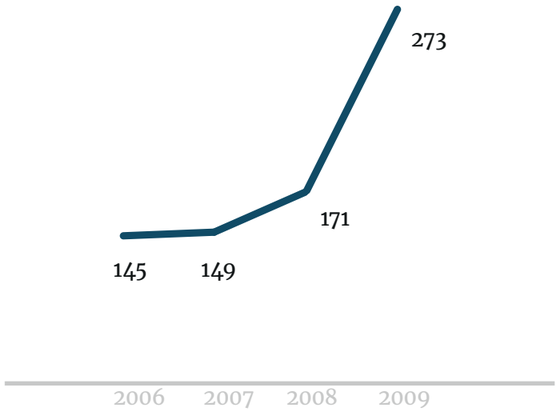


Abb. 6: Legendierungsfälle 2006-2009
Quelle: Sicherheitsbericht BMI

Kommentar zur Tätigkeit des_der Rechtsschutzbeauftragten (RSB) des Innenministeriums

§ 14 Abs. 2 PStSG

§ 91c Abs 1 SPG

Der Bericht des_der RSB des Innenministeriums (merke: Der_die RSB des Justizministeriums verfasst einen eigenen Bericht) zeigt die Tendenz, dass ab Einführung des PStSG die Einsätze von Überwachungsmaßnahmen in den ersten zwei Jahren im Vergleich zum SPG extrem hoch waren. Dabei muss der RSB bei derartigen Maßnahmen zustimmen (wohingegen im Rahmen des SPG dem RSB verdeckte Ermittlungen bloß gemeldet werden müssen und dieser nur im Einzelfall und im Nachhinein die Ermittlung verbieten kann), diese Zustimmung wird aber nur selten verweigert, wie die Berichte zeigen: Für ein Aktivwerden der Behörden im Rahmen des PStSG benötigt es zunächst eine sogenannte Basisermächtigung durch den RSB und in Folge eine Befugnisermächtigung für die spezifische Überwachungsbefugnis (wie z.B. Observation oder eben verdeckte Ermittlung)[45]. In der obenstehenden Tabelle (wie auch im Bericht des RSB) werden zwar nur Ersuchen aufgelistet (und nicht etwa Bestätigungen). Diese sind aber durchaus aussagekräftig, da etwa der RSB-Bericht des Jahres 2016 erläutert, dass in diesem Jahr keine einzige der 43 begehrten Basisermächtigungen „schlechthin verweigert" wurde. Im selben Zeitraum hat der RSB für 51 Meldungen (die genannten 43 Erstmeldungen und Fortsetzungsmeldungen + 8 Zwischenmeldungen), in denen wiederum Ersuchen für 124 einzelne Befugnisse enthalten war, in 42 Fällen davon für alle darin gewünschten Befugnisse eine uneingeschränkte Ermächtigung erteilt, in 5 Fällen wurde sie eingeschränkt erteilt und lediglich in 3 Fällen wurden Befugnisse verweigert.

Genehmigung der Vertrauenspersonen

Auch in Bezug auf den Einsatz von Vertrauenspersonen scheint (diesfalls im Rechtsschutzsenat) großes Vertrauen vorzuherrschen: „Die Ersuchen zum Einsatz einer Vertrauensperson wurden im Berichtsjahr allesamt uneingeschränkt positiv erledigt. Dies lässt sich ganz einfach damit erklären, dass die Staatsschutzbehörden – der Sensibilität der Materie bewusst – Befugnisersuchen im erörterten Bereich nur dann stellten, wenn sie sie wirklich überzeugend zu begründen vermochten", steht im RSB-Bericht 2017.

Resumée

Die verdeckte Ermittlung als (unter anderem von Vertrauenspersonen ausgeführte) Überwachungsmaßnahme kann äußerst invasives Potential entfalten. Umso kritischer ist es zu betrachten, dass, wie oben dargestellt, der Umfang der Befugnisse umstritten ist (etwa in Bezug auf Ton- und Bildaufzeichnung), dass laut Vermutung des RSB die Befugnisse von Beamt_innen willkürlich unter dem Regime der StPO oder unter jenem des SPG eingesetzt werden[46] und außerdem, dass die Datenlage für eine derart eingriffsintensive Maßnahme äußerst dürftig ist und eine Evaluierung der Eingriffe durch die verdeckte Ermittlung gar nicht zulässt.

Endnoten

1 Vgl. Erläuterungen zur Regierungsvorlage, 148 d. B. XVIII. GP, 44. https://www.parlament.gv.at/PAKT/VHG/XVIII/I/I_00148/imfname_260305.pdf.
2 Siehe *Zerbes*, Spitzeln, Spähen, Spionieren (2010) 1.
3 Erläuterungen zur Regierungsvorlage, 148 d. B. XVIII. GP, 44.
4 Vgl. *Heißl*, Überwachungen und Ermittlungen im Internet (2017) 56ff.
5 *Zerbes*, WK-StPO 2017, § 131, Rz 8.
6 *Bundeministerium für Inneres*, Sicherheitsbericht 2009, 356. https://www.parlament.gv.at/PAKT/VHG/XXIV/III/III_00186/index.shtml (30.11.2019).
7 Ebd.
8 Erläuterungen zur Regierungsvorlage, 25 d. B. XXII. GP, 183. https://www.parlament.gv.at/PAKT/VHG/XXII/I/I_00025/imfname_001986.pdf.
9 Vgl. *Heißl*, Überwachungen und Ermittlungen im Internet (2017) 87f.
10 Vgl. *Adamovich/Funk/Holzinger/Frank*, Österreichisches Staatsrecht. Band 3: Grundrechte2 2015, Rz 42.057.
11 Vgl. *Zerbes*, WK-StPO 2017, § 131, Rz 8: „Nur verdeckte Ermittler ieS – kriminalpolizeiliche Organe – können diese Unterstützung bekommen, Vertrauenspersonen nicht."
12 *Adamovich/Funk/Holzinger/Frank*, Österreichisches Staatsrecht. Band 3: Grundrechte2 2015, Rz 42.057.
13 Erläuterungen zur Regierungsvorlage, 25 d. B. XXII. GP, 181.
14 *Zerbes*, WK-StPO 2017, § 131, Rz 3.
15 Erläuterungen zur Regierungsvorlage 763 d. B. XXIV. GP, 4.
16 Erläuterungen zur Regierungsvorlage 1138 d. B. XXI. GP, 21.
17 Vgl. ebd.
18 Ebd. 30.
19 Vgl. ebd.
20 Vgl. *Zerbes*, WK-StPO § 129 Rz 27ff, 46f.
21 Vgl. Erläuterungen zur Regierungsvorlage 763 d. B. XXV GP, 13f.
22 *Heißl*, PStSG Kurzkommentar, Wien 2016, § 6 Rz 1ff, § 11 Rz 23ff.
23 *Zerbes*, Spitzeln, Spähen, Spionieren (2010) 1.
24 Vgl. *Zerbes*, WK-StPO, § 129-133, Rz 1.
25 Ebd. Rz 2.
26 Vgl. *Zerbes*, Spitzeln, Spähen, Spionieren (2010) 2.
27 Zit. nach *Brickner*, Heikle Fragen an „Danielle Durands" Führer, derstandard.at 13.12.2010, https://www.derstandard.at/story/1291455024561/heikle-fragen-an-danielle-durands-fuehrer (30.08.2019).
28 Vgl. *Seeh*, Tierschützer: Sexspionin hat nichts Strafbares gefunden, diepresse.com 13.12.2010 https://diepresse.com/home/panorama/oesterreich/618217/Tierschuetzer_Sexspionin-hat-nichts-Strafbares-gefunden (30.08.2019);
Brickner, Heikle Fragen an „Danielle Durands" Führer, derstandard.at 13.12.2010, https://www.derstandard.at/story/1291455024561/heikle-fragen-an-danielle-durands-fuehrer (30.08.2019). Siehe auch Bericht des Untersuchungsausschusses betreffend die Einflussnahme auf das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT-Untersuchungsausschuss) (3/US) (695 d. B.) 288, https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00695/index.shtml (29.11.2019).
29 Vgl. *APA/NN*, Freispruch für Tierschützer: „Sternstunde der Justiz", diepresse.com, https://diepresse.com/home/panorama/oesterreich/654688/Freisprueche-fuer-Tierschuetzer_Sternstunde-der-Justiz (30.08.2019).
30 Vgl. *Möseneder*, Spitzeleinsatz gegen Tierrechtler war zulässig, derstandard.at 03.04.2014, https://www.derstandard.at/story/1395364216625/tierschuetzer-verdeckte-ermittlung-war-zulaessig (30.08.2019); *Möseneder*, Tierschutzprozess: Lizenz zum Spitzeln, derstandard.at 03.04.2014, https://www.derstandard.at/story/1395364235487/tierschuetzerprozess-lizenz-zum-spitzeln (30.08.2019).
31 Vgl. *Simettinger*, Balluch sieht BVT von ÖVP beeinflusst, orf.at 06.03.2019, https://orf.at/stories/3114035/ (30.08.2019).
32 *Gebauer/Roebel/Stark*, NSU-Sprengstofflieferant war V-Mann der Berliner Polizei, derspiegel.de 13.09.2012, https://www.spiegel.de/panorama/justiz/nsu-sprengstofflieferant-war-v-mann-der-berline-rpolizei-a-855719.html (30.08.2019).
33 Vgl. ua *NN*, Ex-V-Mann spendete Teil seines Honorars an den NSU, zeit.de 19.02.2018,

https://www.zeit.de/gesellschaft/zeitgeschehen/2018-02/nsu-ausschuss-stuttgart-verfassungsschutz-finanzierung-rechtsterrorismus (30.08.2019);
Aust/Büchel/Laabs, Spuren, die keine sein dürfen, welt.de 24.04.2018, https://www.welt.de/politik/deutschland/article163970309/Spuren-die-keine-sein-duerfen.html (30.08.2019);
Gebauer/Roebel/Stark, NSU-Sprengstofflieferant war V-Mann der Berliner Polizei, derspiegel.de 13.09.2012, https://www.spiegel.de/panorama/justiz/nsu-sprengstofflieferant-war-v-mann-der-berliner-polizei-a-855719.html (30.08.2019).

34 Vgl. *Evans/Lewis*, Undercover police had children with activists, theguardian.com 20.01.2012, https://www.theguardian.com/uk/2012/jan/20/undercover-police-children-activists (30.08.2019).

35 Vgl. *Rieß*, „Darf ich Polizist_innen fotografieren?". Zulässigkeit von Bildaufnahme und Veröffentlichung polizeilichen Handelns, juridikum 3/2019, 412.

36 Bericht des Untersuchungsausschusses betreffend die Einflussnahme auf das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT-Untersuchungsausschuss) (3/US) (695 d. B.) 177, https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00695/index.shtml (29.11.2019).

37 Ebd. 242ff.

38 Siehe auch ebd. 247.

39 *Bundeministerium für Inneres*, Anfragebeantwortung „Verdeckte Ermittlung", 12.11.2019 https://fragdenstaat.at/anfrage/verdeckte-ermittlung/ (28.11.2019) 2.

40 Vgl. *Bundesministerium für Inneres*, Anfragebeantwortung 13139/AB, XXV. GP vom 29.09.2017 zur Anfrage 13961/J, XXV. GP vom 27.9.2017, https://www.parlament.gv.at/PAKT/VHG/XXV/AB/AB_13139/index.shtml (28.11.2019);
Siehe auch *Adensamer/Steinhauser,* SPG Ermittlungsmaßnahmen nach 2013, in: Die Grünen, Nie mehr allein… Überwachungsbericht 2017, 13.

41 Vgl. *Bundesministerium für Inneres*, Sicherheitsbericht 2009, 354.

42 Vgl. *Burgstaller u.a.*, Zentrale Daten des Rechtsschutzbeauftragen 2017, SIAK-Journal 3/2018, 7f, https://www.bmi.gv.at/104/Wissenschaft_und_Forschung/SIAK-Journal/SIAK-Journal-Ausgaben/Jahrgang_2018/files/Burgstaller_3_2018.pdf.

43 Vgl. Bundesministerium für Inneres, Anfragebeantwortung vom 25.11.2019, https://fragdenstaat.at/anfrage/verdeckte-ermittlung/4645/anhang/Erledigung_BMI_extern_geschwaerzt.pdf, 5.

44 Ebd.

45 Vgl. *Burgstaller/Goliasch/Kubarth*, Zentrale Daten des Rechtsschutzbeauftragten 2016, SIAK-Journal 3/2017, 4 (13f).

46 Vgl. *Burgstaller/Goliasch/Zotter*, Zentrale Daten des Rechtsschutzbeauftragten 2017, SIAK-Journal 3/2018, 7f.

6 Videoüberwachung

Eine offene, das heißt nicht geheime, Videoüberwachung (die Aufnahme von Bild und/oder Ton) kann aufgrund diverser Bestimmungen durchgeführt werden. Das Sicherheitspolizeigesetz (SPG) sieht eine gesetzliche Grundlage für die Überwachung öffentlicher Orte, eine Überwachung von Zusammenkünften zahlreicher Menschen und die Verwendung von Body Worn Cameras durch Polizist_innen vor. Im Sicherheitspolizeigesetz finden sich auch noch zwei Bestimmungen, welche Videoüberwachung vor allem zur Erfüllung internationaler Verpflichtungen gestatten: Die Videoüberwachung des öffentlichen Raumes zum Schutz von Vertreter_innen anderer Staaten oder Internationaler Organisationen und Überwachung des öffentlichen Raumes zum Schutz bestimmter Objekte, insbesondere zum Schutz von Botschaften. Offene Videoüberwachung kann aber auch auf der Grundlage des polizeilichen Staatsschutzgesetzes durch die Geheimdienste (bspw. Filmen auf Demonstrationen, um Personen identifizieren zu können) durchgeführt werden.

§ 54 Abs. 6 SPG, § 54 Abs. 5 SPG und § 13a Abs. 3 SPG

§ 54 Abs. 7 SPG und § 54 Abs. 7a SPG

§ 11 Abs. 1 Z 3 PStSG

Weiters gestattet das SPG den Sicherheitsbehörden Videoüberwachung auch durch die Inanspruchnahme Dritter (also bspw. durch die Verwendung von Videokameras von Spitälern, öffentlichen Verkehrsbetrieben, der ASFINAG). Im sog. Sicherheitspaket 2018 wurde sogar eine Bestimmung eingeführt, die es der Polizei erlaubt, Dritte zu verpflichten, das von ihnen aufgenommene Material bis zu vier Wochen zu speichern. Diese Art der staatlichen Überwachung wird in einem eigenen Kapitel behandelt, da sie eine Stufe zwischen offener und verdeckter Überwachung darstellt. Zum Sonderfall der Kfz-Überwachung siehe Kapitel 8.3 Zwar sind die Kameras von Privaten oder Gemeinden im Normalfall erkennbar aufgestellt, dass das aufgenommene Material jedoch länger gespeichert wird und ein Zugriff von Sicherheitsbehörden leicht möglich ist, muss nicht gekennzeichnet werden. Insofern handelt es sich hierbei zwar nicht um eine verdeckte Aufnahme der Sicherheitsbehörden, wohl aber um einen verdeckten Zugriff auf Videomaterial durch eben diese. Unabhängig davon darf nicht vergessen werden, dass auf Grundlage der Strafprozessordnung (StPO) von der Polizei Videomaterial jedenfalls sichergestellt (d.h. kopiert) werden darf, wenn es aus Beweisgründen zur Aufklärung einer gerichtlichen Straftat erforderlich erscheint. Dafür ist keine gerichtliche Bewilligung oder Anordnung der Staatsanwaltschaft notwendig.

§ 52 Abs. 5 und § 93a SPG Inanspruchnahme Dritter

§ 110 Abs. 1 Z 1 i.V.m. § 111 Abs. 2 StPO

📖 *Sicherheitspaket 2018*

Geheime Videoüberwachung

Schließlich gibt es noch einige Bestimmungen, die den staatlichen Behörden eine geheime Videoüberwachung (Bild und/oder Ton) gestatten. Diese finden sich im SPG, im PStSG und in der StPO („Großer und kleiner Lauschangriff“ 6.5.1; 6.5.2). Diese Bestimmungen sind unten genauer dargestellt.

📖 *Lauschangriff, großer und kleiner*

§§ 54 Abs. 4 SPG, § 11 Abs. 1 Z 3 PStSG, § 136 StPO

6.1 Offene Videoüberwachung durch die Polizei

Offen ist eine Videoüberwachung, wenn sie angekündigt wird, oder auf andere Weise für die Betroffenen erkennbar ist, z.B. durch eine Tafel. Dies ist weniger eingriffsintensiv als eine geheime Überwachung, weil es möglich ist, die Überwachung zu vermeiden, bzw. Auskunft zu verlangen oder sich zu beschweren, wenn die Überwachung nicht rechtmäßig war. Prinzipiell besteht die Pflicht zur Offenlegung, Ausnahmen müssen gesetzlich ausdrücklich geregelt sein.

6.1.1 Body Worn Cameras

Die Polizei kann mit an ihrer Uniform angebrachten Kameras (Body Worn Cameras, oder auch Body-Cams) Aufnahmen von Amtshandlungen machen. Diese Befugnis wurde 2016 beschlossen und hätte Ende 2019 außer Kraft treten sollen. Im Gewaltschutzpaket 2019 wurde der sunset-clause jedoch ohne Debatte aufgehoben. Derzeit sind 140 Body-Cams in Betrieb und für die kommenden Jahre hatte Ex-Innenminister Herbert Kickl (FPÖ) eine Aufstockung auf 300 Body-Cams angekündigt.[1] Nach Probebetrieben in Salzburg und Graz sind Body Worn Cameras seit Frühling 2019 bundesweit im Betrieb.[2] Es gibt keine Dokumentation darüber, wie oft die Body-Cams jährlich im Einsatz sind, also wie oft diese tatsächlich aktiviert wurden.

§ 13a Abs. 3 SPG

📖 *Body Worn Cameras*

Die Voraussetzungen für den legitimierten Einsatz dieser Kameras sind u.a. das Vorliegen einer Amtshandlung, bei welcher Befehls- oder Zwangsgewalt ausgeübt werden soll, und die Ankündigung des Einsatzes der Kamera gegenüber der Betroffenen, sodass er diesen auch bekannt wird. De facto bedeutet das, dass jede_r Polizist_in bei Erfüllung dieser Voraussetzungen autonom darüber entscheiden kann, ob er oder sie diese Maßnahme anwendet oder nicht. Die Rechtsschutzbeauftragten (RSB) müssen vom Einsatz der Body-Cams nicht informiert werden. Es ist als problematisch zu bewerten, dass der_die kameraführende Polizist_in vollkommen selbständig darüber entscheidet, wann die Kamera ein- bzw. ausgeschalten ist: Es besteht die Möglichkeit, dass der eigentliche Dokumentationszweck dadurch verfehlt wird. Zumindest müssten die Polizist_innen mit sichtbaren Dienstnummern ausgestattet sein, um sie im Nachhinein identifizieren zu können.

Das auf diese Weise angefertigte Videomaterial darf nur zur Verfolgung von strafbaren Handlungen, die sich während der Amtshandlung ereignet haben, und zur Kontrolle der Rechtmäßigkeit der Amtshandlung ausgewertet werden. Diese Bestimmung enthält zwei Kontrollregelungen, die Aufbewahrung betreffend: Die Videoaufzeichnungen werden nach 6 Monaten gelöscht, es sei denn, es ist noch ein Verfahren anhängig. Die Daten müssen verschlüsselt aufbewahrt werden und jeder Zugriff muss protokolliert werden.

Kontrollregelungen

6.1.2 Überwachung von Zusammenkünften zahlreicher Menschen

Die öffentlich angekündigte Ermittlung personenbezogener Daten mit Bild- und Tonaufzeichnungsgeräten ist auch zur Vorbeugung gefährlicher Angriffe erlaubt. Voraussetzung ist eine Zusammenkunft zahlreicher Menschen und die Befürchtung, dass es dabei zu gefährlichen Angriffen gegen Leben, Gesundheit oder Eigentum von Menschen kommen wird. Bei einer Zusammenkunft kann es sich um eine Versammlung (Kundgebung, Demonstration, etc.) oder z.B. um eine Sport- oder Theaterveranstaltung handeln. Die Streubreite des Grundrechtseingriffs ist enorm hoch, nachdem sich die Ermittlungsbefugnis auf alle Anwesenden bezieht, gleichgültig, ob diese an der Zusammenkunft aktiv und bewusst teilnehmen oder sich nur zufällig am Ort der Zusammenkunft aufhalten. Die ermittelten Daten dürfen auch zur Abwehr gefährlicher Angriffe, die sich im Zusammenhang mit oder während der Zusammenkunft ereignen, sowie zu deren Aufklärung bzw. Verfolgung (auf Grundlage der StPO oder im Rahmen der Sicherheitsverwaltung) verwendet werden, bspw. also zur Aufklärung bzw. Verfolgung von Verwaltungsübertretungen nach dem Pyrotechnikgesetz.

§ 54 Abs. 5 SPG

§ 16 Abs. 2 SPG

6.1.3 Videoüberwachung von öffentlichen Orten

§ 54 Abs. 6 SPG

Gem. § 54 Abs. 6 SPG dürfen nach öffentlicher Ankündigung personenbezogene Daten mit Bild- und Tonaufzeichnungsgeräten zur Vorbeugung gefährlicher Angriffe an öffentlichen Orten ermittelt werden. Voraussetzung der Ermittlungsmaßnahme ist eine Prognoseentscheidung, dass es an dem zu überwachenden öffentlichen Ort sonst zu gefährlichen Angriffen gegen Leben, Gesundheit oder Eigentum von Menschen kommen werde. Gemeint sind sog. Kriminalitätsbrennpunkte oder Hot-Spots wie z.B. Plätze, Passagen oder Parkgaragen, die erfahrungsgemäß besonders kriminalitätsgefährdet sind. Die ermittelten Bild- und Tondaten dürfen 48 Stunden aufbewahrt werden, wobei sie während dieser Zeit auch zur Abwehr gefährlicher Angriffe oder deren Aufklärung oder zur Fahndung verwendet werden dürfen. Sind die Aufzeichnungen zur weiteren Verfolgung strafbarer Handlungen erforderlich (z.B. wenn sie einen identifizierbaren Tatverdächtigen zeigen), dürfen sie auch über die 48-Stunden-Frist hinaus aufbewahrt werden (zur Strafverfolgung bzw. zur Übermittlung in ein anderes Aufgabengebiet der Sicherheitsbehörden). Die geplante Maßnahme ist dem_der Rechtsschutzbeauftragten mitzuteilen und darf erst nach Ablauf der Drei-Tages-Frist nach der Meldung bzw. bei Vorliegen einer entsprechenden Äußerung des_der Rechtsschutzbeauftragten vorgenommen werden. Laut einer Anfragebeantwortung[3] des BMI gibt es 17 solcher Standorte mit Videoüberwachung (Stand 03.09.2019, Grafik links)

Bundesland	Ort	aktiv seit
Kärnten	Klagenfurt Pfarrplatz	27.08.2007
Kärnten	Villach Lederergasse	03.04.2006
Niederösterreich	Flughafen Schwechat	30.07.2005
Niederösterreich	SCS	03.03.2005
Niederösterreich	Wr. Neustadt	22.09.2006
Oberösterreich	Linz – Altstadt	14.03.2006
Oberösterreich	Linz – Hinsenkampplatz	30.08.2006
Oberösterreich	Ried im Innkreis	15.03.2010
Salzburg	Salzburg – Rudolfskai	27.06.2006
Salzburg	Salzburg – Südtirolerplatz	04.02.2006
Steiermark	Graz – Jakomini	30.09.2009
Tirol	Innsbruck - Rapoldi/ Bogenmeile	12.08.2005
Tirol	Reutte	14.07.2010
Wien	Karlsplatz	08.08.2005
Wien	Praterstern	20.05.2016

Abb. 7: Standorte polizeilicher Videoüberwachung im öffentlichen Raum. Die Tabelle zeigt, welche 17 Standorte aufgrund des § 54 Abs. 6 SPG unter ständiger Videoüberwachung stehen.

6.2 Videoüberwachung durch die Einbindung Dritter

Die oben genannten Kameras betreibt die Polizei selbst, ebenso wie z.B. Kennzeichenerkennungssysteme. Mit der immer weiteren Verbreitung privater Videoüberwachung (z.B. auf Bahnhöfen, Krankenhäusern, Banken, etc.), wurden aber auch Zugriffsmöglichkeiten für die Polizei auf diese geschaffen. Dies führt zu einem potentiell sehr engen Netz polizeilicher Videoüberwachung im öffentlichen Raum und ist daher stark umstritten. Hier zeigt sich auch, dass private und polizeiliche Überwachung nicht getrennt voneinander betrachtet werden können, wenn eine reale Einschätzung der Lage das Ziel der Betrachtung ist.

6.2.1 Informationspflicht und Speicherverpflichtung für Dritte

§ 93a SPG

Wenn öffentliche Rechtsträger_innen und private Rechtsträger_innen, denen ein öffentlicher Versorgungsauftrag zukommt (bspw. Betreibende öffentlicher Verkehrsunternehmen, Gemeinden und Spitäler), den öffentlichen Raum mittels Videokamera überwachen, sind sie verpflichtet, die Sicherheitsbehörden darüber zu informieren. Unter bestimmten, sehr weit gefassten, Voraussetzungen können die Sicherheitsbehörden diese Rechtsträger_innen sogar dazu verpflichten, das Videomaterial bis zu vier Wochen zu speichern. Kommen sie diesen Verpflichtungen nicht nach, droht eine Verwaltungsstrafe. Dadurch werden private und öffentliche Unternehmen dazu gedrängt, ihre Kamerasysteme entgegen der Grundsätze Privacy by Design und Privacy by Default einzurichten. Diese Bestimmung wurde 2018 im Rahmen des Überwachungspakets eingeführt. Die ASFINAG, betreffend Bilddaten diverser Autobahn-Teilstücke sowie Rastplätze, wurde bisher als Einzige seit Einführung der Befugnis per Bescheid zur vier Wochen langen Speicherung verpflichtet.[4] Die ASFINAG hatte schon in ihrer Stellungnahme zum Gesetzesentwurf bemerkt, dass sie damit dazu verpflichtet würde, Daten zur Verfügung zu stellen, deren Sammlung aufgrund anderer Gesetze für sie verboten sei. Eine Änderung der betreffenden Gesetze oder eine Spezifizierung im Gesetzestext erfolgte jedoch nicht. Dazu kommt, dass die von der ASFINAG betriebenen Systeme technisch so ausgelegt sind, dass sie den gesetzlichen Anforderungen entsprechen (z.B. lediglich Speicherung von ausgewählten Einzelbildern im Rahmen des Mautsystems) und daher für eine allfällige generelle Speicherverpflichtung nicht geeignet sind.“[5]

Rechtsträger_innen

z.B. Speicherverbot gemäß § 98f StVO oder § 19a BStMG

Voraussetzung für die Auferlegung der Speicherverpflichtung ist die Erfüllung von mindestens einem der nachfolgenden Punkte:

Vorraussetzungen Speicherverpflichtung

- Es erscheint aus Gründen der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit erforderlich. Damit könnte beinahe jeder öffentliche Platz überwacht werden.
- Es erscheint zur Strafverfolgung erforderlich.
- Eine ortsbezogene Risikoanalyse hat ergeben, dass die Aufbewahrungsverpflichtung notwendig ist.

6.2.2 Verwendung von Videomaterial von Dritten durch die Sicherheitsbehörden

§ 53 Abs. 5 SPG

Die Sicherheitsbehörden dürfen auch Videomaterial verwenden, das nicht von ihnen selbst angefertigt wurde. Diese Befugnis wurde im Zuge des Überwachungspakets 2018 novelliert. Es gibt dabei zwei Unterfälle: In einem Anwendungsfall (bei der freiwilligen Zurverfügungstellung des Videomaterials durch Dritte) wurden die Voraussetzungen erheblich gelockert und der zweite Anwendungsfall wurde zur Gänze neu eingeführt.

Erzwingen der Herausgabe von Videomaterial

Der zweite Anwendungsfall sieht eine gänzlich neue Befugnis im Sicherheitspolizeigesetz vor. Die Sicherheitsbehörden dürfen nach dieser Bestimmung die Herausgabe von Videomaterial, welches von dritter Seite angefertigt wurde, erzwingen. Sobald die Polizei den_die Verarbeiter_in des Videomaterials darüber in Kenntnis gesetzt hat, darf diese_r es nicht mehr löschen. Das bedeutet, dass theoretisch eine Reihe von technischen Systemen umgestellt werden müssten. Somit ist erstmals eine Herausgabeverpflichtung für Zwecke der Sicherheitspolizei gesetzlich verankert worden. Bisher war eine Sicherstellung bzw. Beschlagnahme von Videomaterial Dritter nur im Rahmen der Strafverfolgung nach den §§ 110 und 115 StPO zulässig. Nach den Erläuterungen sind die Rechtsträger_innen sogar verpflichtet, einen Livestream zur Verfügung zu stellen.

Videomaterial ist von der Herausgabepflicht betroffen, wenn die folgenden Voraussetzungen vorliegen:

- Das Videomaterial wird von öffentlichen oder privaten Rechtsträger_innen, sofern letzteren ein öffentlicher Versorgungsauftrag zukommt (z.B. öffentliche Verkehrsbetriebe, Bahnhofs- oder Flughafenbetreiber, die ASFINAG oder Spitäler) angefertigt.
- Die Überwachung betrifft einen öffentlichen Ort.
- Die Überwachung dient einem der folgenden Zwecke:
  - Vorbeugung eines gefährlichen Angriffs
  - Abwehr eines gefährlichen Angriffs
  - Abwehr einer kriminellen Verbindung: Der Begriff der „kriminellen Verbindung“ in diesem Zusammenhang ist sehr weit gefasst. Sobald sich drei oder mehr Personen zu dem Zweck verbinden, fortgesetzt gerichtlich strafbare Handlungen zu begehen (§ 16 Abs. 1 Z 2 SPG) liegt eine kriminelle Verbindung im Sinne des Sicherheitspolizeigesetzes vor.
  - Fahndung

§ 84 Abs. 1 Z 7 SPG

Diese Bestimmung der Herausgabepflicht muss in Zusammenhang mit der Speicherverpflichtung und Informationsverpflichtung (s.o.) für bereits genannte Rechtsträger_innen gesehen werden. Kommen Rechtsträger_innen einer Herausgabeverpflichtung nicht nach, droht eine Verwaltungsstrafe. Rechtsträger_innen haben die Möglichkeit, bei Verpflichtung durch Sicherheitsbehörden zur Herausgabe von Videomaterial ein Rechtsmittel einzulegen; der ohnehin dürftige Rechtsschutz (Information der RSB) für die am Video aufgezeichnete Person wurde jedoch – in wohl verfassungswidriger Weise – ausgeschlossen. Es muss den RSB keine Meldung mehr erstattet werden, wenn von dieser Befugnis Gebrauch gemacht wird. Das Wegfallen einer Dokumentation durch die RSB bedeutet auch, dass es für die Öffentlichkeit sehr schwierig wird, nachzuvollziehen, wie oft diese Befugnis zum Einsatz kommt. In den ersten Monaten der Geltung der neuen Bestimmung wurden schon über 350 Rechtsträger von den Landespolizeidirektionen aufgefordert, Auskunft über von ihnen betriebene Aufnahmesysteme zu geben.[6]

§ 53 Abs. 5 SPG

Die Voraussetzungen, unter welchen die Sicherheitsbehörde Videomaterial verwenden darf, das ihr freiwillig zur Verfügung gestellt wird, haben sich erheblich gelockert. Sofern darauf nur öffentliches Verhalten aufgezeichnet wird, darf dieses unter sehr weit gefassten Voraussetzungen von der Polizei verwendet werden.

Die Verwendung des Videomaterials durch die Behörde muss einen der folgenden Zwecke verfolgen:

Zweck der Verwendung des Materials muss definiert sein

- Erfüllung der ersten allgemeinen Hilfeleistung
- Abwehr krimineller Verbindungen
- Abwehr eines gefährlichen Angriffs und zur Gefahrenerforschung
- Vorbeugung wahrscheinlicher gefährlicher Angriffe (siehe genauer § 53 Abs. 1 Z 4 SPG)
- Fahndung
- Aufrechterhaltung der öffentlichen Ordnung bei einem bestimmten Ereignis: Alle größeren Ereignisse (Fußballspiele, Silvester, Versammlungen, etc.) fallen unter diesen Zweck. Die Beurteilung des Vorliegens dieses Zwecks ist besonders problematisch.

Die Rechtsschutzbeauftragten müssen informiert werden, wenn Videomaterial auf Grund dieser Bestimmung durch die Sicherheitsbehörden verwendet wird. Die RSB haben auch die Möglichkeit ein Rechtsmittel anstelle des Betroffenen einzulegen.

Häufigkeit

Da die RSB einen jährlichen Bericht veröffentlichen, ist bekannt, wie häufig diese Bestimmung unter den alten Voraussetzungen eingesetzt wurde: Im Jahr 2017 wurden bloß 8 Meldungen erstattet.[7] Es ist zu erwarten, dass durch die Ausdehnung der Voraussetzungen diese Überwachungsmaßnahme zukünftig häufiger eingesetzt wird.
Im ersten Halbjahr 2019 wurden in fünf Fällen ein Eisenbahnunternehmen und ein städtischer Verkehrsbetrieb von der Polizei verpflichtet, Ton- und Videomaterial herauszugeben. Ein Eisenbahnunternehmen, ein Amt einer Landesregierung, ein Einkaufszentrum sowie zwei Privatpersonen haben freiwillig Bild- und Tondaten übermittelt.[8]

6.3 Verdeckte Ermittlung mit Bild- und Tonaufzeichnungsgeräten

Verschiedene gesetzliche Bestimmungen erlauben den verdeckten, also geheimen, Einsatz von Bild- und/oder Tonüberwachung zu verschiedenen Zwecken:

§ 54 Abs. 3, Abs. 4a und Abs. 4 SPG

- Zur Abwehr eines gefährlichen Angriffs oder zur Abwehr einer kriminellen Verbindung, wenn zu erwarten ist, dass diese kriminelle Verbindung Straftaten begehen werde, die mit mehr als einjähriger Freiheitsstrafe bedroht sind. Nach dieser Bestimmung darf die Aufzeichnung in Räumlichkeiten, die vom Hausrecht geschützt sind (z.B. Wohnungen), nur mit Einverständnis des_der Inhaber_in geschehen. Hier geht es also vor allem um die Aufnahme von Gesprächen durch eine_n verdeckte_n Ermittler_in oder eine Vertrauensperson. 2017 wurden den RSB 87[9] und 2018 122[10] verdeckte Einsätze mittels Bild- und Tonaufzeichnungsgeräten auf Grundlage dieser Bestimmung gemeldet.

➲ *5. Verdeckte Ermittlung*

§ 11 Abs. 1 Z 3 PStSG

- Das Polizeiliche Staatsschutzgesetz wurde 2016 eingeführt und erlaubt den geheimen Einsatz von Bild- und Tonaufzeichnungsgeräten zur „erweiterten Gefahrenforschung". Damit ist die Beobachtung von Gruppen gemeint, „wenn im Hinblick auf deren bestehende Strukturen und auf zu gegenwärtige Entwicklungen in deren Umfeld damit zu rechnen ist, dass es zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität, insbesondere zu ideologisch oder religiös motivierter Gewalt kommt". Die Überwachung nach dieser Bestimmung ist auch zulässig zur Vorbeugung von „verfassungsgefährdenden Angriffen". Die Formulierungen des Gesetzes sind vage und weit. Politisch engagierte Personen sind daher rasch der Gefahr ausgesetzt, von einer der geheimen Ermittlungsbefugnisse des PStSG betroffen zu sein. 2017 wurden den RSB 97[11] und 2018 113[12] verdeckte Ermittlungen mittels Bild- und Tonaufzeichnungsgeräten auf Grundlage dieser Bestimmung gemeldet.

➲ *4.1.3 Erweiterte Gefahrenforschung*

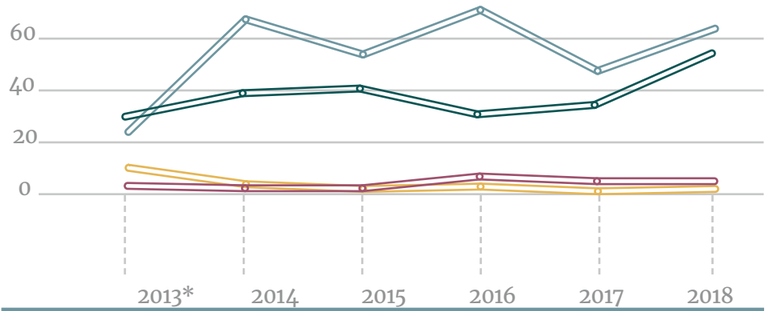
§ 6 Abs 1 Z 1 PStSG

- Der verdeckte Einsatz von Bild- und Tonaufzeichnungsgeräten kann auch auf Grundlage der StPO geschehen. Es dürfen unter bestimmten Umständen auch Räumlichkeiten (z.B. Wohnungen) überwacht werden (s.u.).

6.4 Häufigkeit der Videoüberwachung nach dem Sicherheitspolizeigesetz

Insgesamt ist die Überwachung zur Unterstützung von Observation häufiger, als die zur Unterstützung der verdeckten Ermittlung, welche auch nur unter strengeren Voraussetzungen zulässig ist. Auch die Überwachung von Zusammenkünften zahlreicher Menschen wurde laut dem Bundesministerium für Inneres im Jahr 2018 nur drei Mal angewendet.[13] Die Entwicklung der Videoüberwachungen lassen keinen klaren Trend erkennen, der Anstieg im Jahr 2018 des § 54 Abs. 4 SPG sollte im Auge behalten werden; er kann zwar ein Ausreißer sein, kann aber auch Beginn eines Trends sein.
(siehe Grafik auf nächster Seite)

Videoüberwachung nach § 54 SPG



	2013*	2014	2015	2016	2017	2018
§ 54 Abs. 2a SPG	23	71	56	75	49	67
§ 54 Abs. 3 SPG	10	3	1	2	0	1
§ 54 Abs. 4 SPG	31	41	43	32	36	58
§ 53 Abs. 5 SPG	1	0	0	5	3	3

Abb. 8: Juni 2013 - 2018 Videoüberwachung nach § 54 SPG.
**Die Zahlen für 2013 sind nur für das halbe Jahr vorhanden, und wurden für diese Darstellung hochgerechnet.*

6.5 Videoüberwachung nach der Strafprozessordnung

Auch nach der Strafprozessordnung (StPO) ist Videoüberwachung zulässig. Hier dient sie zur Aufklärung von Straftaten und ist ab einem konkreten Tatverdacht möglich. Im Folgenden werden die verschiedenen Befugnisse nach der StPO im Einzelnen dargestellt.

➲ *4.2 Überwachungsbefugnisse*

6.5.1 Großer Späh- und Lauschangriff

§ 136 Abs. 1 Z 3 StPO

Der Große Späh- und Lauschangriff erlaubt die Installation von Videokameras und Mikrofonen in Räumlichkeiten, die vom Hausrecht geschützt sind (z.B. in Wohnungen), in Pkws, etc. Dies kann zur Überwachung von Tatverdächtigen sowie von Personen, die mit Tatverdächtigen Kontakt haben geschehen. Im Jahr 2018 wurden aufgrund dieser Bestimmung in 7 verschiedenen Objekten (Wohnungen oder Pkws) optische oder akustische Überwachungen durchgeführt.[14]

🕮 *Lauschangriff, großer*

Der Große Späh- und Lauschangriff darf eingesetzt werden:

- Zur Aufklärung einer Straftat, die mit mehr als zehn Jahren Freiheitsstrafe bedroht ist.

- Zur Aufklärung bestimmter Organisationsdelikte: Mitgliedschaft in einer kriminellen Organisation, Mitgliedschaft in einer terroristischen Vereinigung, Begehung einer terroristischen Straftat, Terrorismusfinanzierung oder Ausbildung für terroristische Zwecke. Die niedrigste Strafdrohung beginnt hier schon bei sechs Monaten.

- Zur Verhinderung bestimmter Organisationsdelikte: Hier greift die Befugnis bereits, bevor überhaupt eine Straftat begangen wurde. In Zusammenhang mit einer (zukünftigen) Straftat, welche mit mehr als dreijähriger Freiheitsstrafe bedroht ist und entweder im Rahmen einer kriminellen Organisation oder im Rahmen einer terroristischen Vereinigung geplant ist, darf diese Überwachungsmethode auch zur Verhinderung dieser Straftat eingesetzt werden.

- Zur Ermittlung des Aufenthaltsortes einer Person, wenn diese Person verdächtig ist, eine der oben genannten Organisationsdelikte oder einer Straftat, die mit mehr als zehnjähriger Freiheitsstrafe bedroht ist, begangen zu haben.

Jedenfalls wird eine gerichtliche Bewilligung auf Antrag der Staatsanwaltschaft benötigt. Der Einsatz des großen Lauschangriffs stieg von 3 Einsätzen in 2010 auf 6 Fälle in 2018.[15] Die Variation dazwischen ist relativ stark, dass man maximal von einem leichten linearen Aufwärtstrend ausgehen kann.

6.5.2 Kleiner Späh- und Lauschangriff

Wird ein_e verdeckte_r Ermittler_in oder eine Vertrauensperson eingesetzt, darf diese_r Bild und/oder Ton geheim aufnehmen, wenn dies zur Aufklärung einer Straftat, die mit bis zu drei Jahren Freiheitsstrafe bedroht ist, erforderlich erscheint. Es darf nur Verhalten aufgenommen werden, das zur Kenntnisnahme der Person gedacht ist, die verdeckt ermittelt. Im Jahr 2018 wurden acht optische oder akustische Überwachungen nach dieser Bestimmung durch das Gericht bewilligt.[16]

§ 136 Abs. 1 Z 2 StPO

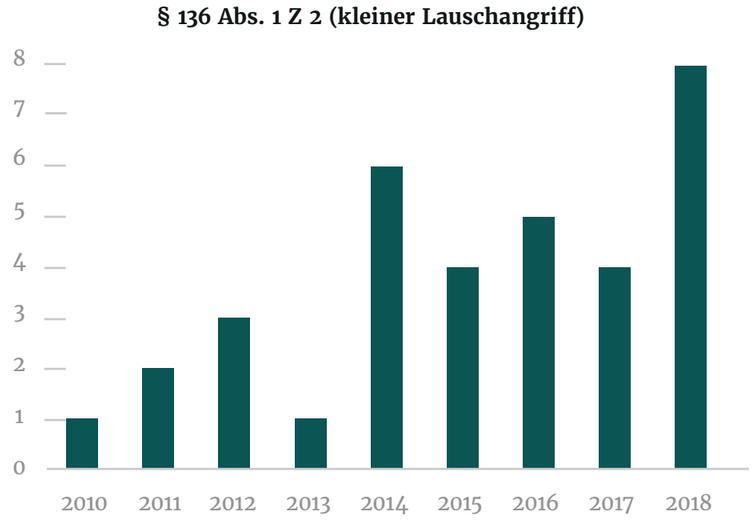


Abb. 9: Kleiner Lauschangriff

Der Einsatz des Kleinen Lauschangriffs ist in den letzten Jahren von einem Fall in 2010 auf acht Fälle in 2018 gestiegen. Ein linearer Aufwärtstrend ist eindeutig erkennbar.

6.5.3 Sonstige geheime Bild- und/oder Tonüberwachung nach der Strafprozessordnung

Neben den oben angeführten Fällen ist eine geheime Bild- und/oder Tonüberwachung nach der Strafprozessordnung auch im Fall einer Entführung zulässig, solange diese andauert. In diesem Fall ist keine gerichtliche Bewilligung auf Antrag der Staatsanwaltschaft notwendig. *§ 136 Abs. 1 Z 1 StPO*

Schließlich besteht auch die Befugnis zur Objektüberwachung zur Aufklärung von Straftaten, wonach bestimmte Gegenstände, Örtlichkeiten oder Räume überwacht werden können, um zu beobachten, welche Personen mit bzw. an diesen in Kontakt treten. Es dürfen nur Vorgänge aufgenommen werden, die außerhalb von Wohnungen geschehen. Eine gerichtliche Bewilligung auf Antrag der Staatsanwaltschat ist nötig. Im Jahr 2018 wurde in 112 Fällen eine derartige Überwachung genehmigt.[17] Mit Zustimmung des_der Inhaber_in einer Wohnung (bzw. anderen vom Hausrecht geschützten Räumen) darf diese Objektüberwachung auch in Wohnungen stattfinden. Allerdings nur zur Aufklärung von Straftaten, die mit mehr als einem Jahr Freiheitsstrafe bedroht sind. Auch hier ist eine gerichtliche Bewilligung auf Antrag der Staatsanwaltschaft notwendig. Im Jahr 2018 erfolgten 42 Überwachungen innerhalb von Räumlichkeiten.[18] *§ 136 Abs. 3 Z 1 und Z 2 StPO*

Endnoten

1 Kurier: Erste 140 Bodycams der Polizei bald offiziell im Einsatz, 01.03.2019, https://kurier.at/chronik/oesterreich/erste-140-bodycams-der-polizei-bald-offiziell-im-einsatz/400422785, 20.12.2019).
2 *Bundesministerium für Inneres*, Anfragebeantwortung vom 01.10.2019, 6, https://fragdenstaat.at/anfrage/polizeiliche-videouberwachung/4534/anhang/Erledigung_BMI_extern_geschwaerzt.pdf.
3 Ebd. 4.
4 Vgl. Ebd. 7.
5 Vgl. *ASFINAG*, Stellungnahme 59 zu 15 d. B. XXVI. GP, 3. (https://www.parlament.gv.at/PAKT/VHG/XXVI/SN/SN_00059/imfname_687573.pdf)
6 Vgl. Bundesministerium für Inneres, Anfragebeantwortung 1793/AB, XXVI. GP vom 13.11.2018 zur Anfrage 1773/J, XXVI. GP vom 26.09.2018. (https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_01793/imfname_723599.pdf)
7 Vgl. *Burgstaller/Goliasch/Zotter,* Zentrale Daten des Rechtsschutzbeauftragten 2017, SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis 3/2018, 7. (https://www.bmi.gv.at/104/Wissenschaft_und_Forschung/SIAK-Journal/SIAK-Journal-Ausgaben/Jahrgang_2018/files/Burgstaller_3_2018.pdf)
8 Vgl. *Bundesministerium für Inneres,* Anfragebeantwortung 3824/AB XXVI. GP vom 30.08.2019 zur Anfrage 3811/J vom 01.07.2019. (https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_03824/imfname_764668.pdf)
9 Vgl. *Burgstaller/Goliasch/Zotter*, Zentrale Daten des Rechtsschutzbeauftragten 2017, SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis 3/2018, 6.
10 Vgl. *Burgstaller/Stricker/Zotter*, Zentrale Daten des Rechtsschutzbeauftragten 2017, SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis 3/2019, 7.
11 Vgl. Ebd., 14.
12 Vgl. Ebd.
13 *Bundesministerium für Inneres,* Anfragebeantwortung vom 01.10.2019, 3, https://fragdenstaat.at/anfrage/polizeiliche-videouberwachung/4534/anhang/Erledigung_BMI_extern_geschwaerzt.pdf.
14 *Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz*, Gesamtbericht 2018. Einsatz besonderer Ermittlungsmaßnahmen (2018) 7. (https://www.parlament.gv.at/PAKT/VHG/XXVI/III/III_00317/imfname_763732.pdf)
15 Vgl. die Berichte Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz, Gesamtbericht 2018. Einsatz besonderer Ermittlungsmaßnahmen (2018) und Bundesministerium für Justiz, Gesamtbericht über den Einsatz besonderer Ermittlungsmaßnahmen in den Jahren 2010 und 2011 (III-373 der Beilagen XXIV. GP)
16 Vgl. *Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz*, Gesamtbericht 2018. Einsatz besonderer Ermittlungsmaßnahmen (2018) 9. (https://www.parlament.gv.at/PAKT/VHG/XXVI/III/III_00317/imfname_763732.pdf)
17 Vgl. Ebd. 12.
18 Vgl. Ebd.

7 Telekommunikationsüberwachung

Die Überwachung von Nachrichten, die Auskunftspflicht über Telekommunikationsdaten und die Anlassdatenspeicherung (auch Quick Freeze genannt) betreffen Daten, die über ein öffentliches Netz oder einen Dienst der Informationsgesellschaft ausgetauscht oder weitergeleitet werden. Davon sind gewerbliche Dienstleistungen umfasst, die ganz oder überwiegend in der Übertragung von Signalen in Kommunikationsnetzen bestehen. Betroffen sind hiervon also typischerweise Telefon- oder Internetanbieter_innen. Zusätzlich zählen hierzu Dienste der Informationsgesellschaft. Das sind jene Dienste, die – in der Regel gegen Entgelt, elektronisch im Fernabsatz, ohne gleichzeitige physische Anwesenheit der Parteien – und auf individuellen Abruf eine_r Empfänger_in erbracht werden, wie zum Beispiel Online-Shops.[1] Die Auskunft von Daten einer Nachrichtenübermittlung betrifft all jene Daten, über die Netzbetreiber_innen oder Diensteanbieter_innen verfügen. Grundsätzlich ist dabei der Daten- und Geheimnisschutz zu beachten. Verkehrsdaten (zu den Definitionen der Datenarten s.u.) etwa dürfen nur gespeichert werden, wenn sie zur Verrechnung von Leistungen benötigt werden – wozu auch eine gesetzliche Verpflichtung besteht. Auch Stammdaten dürfen nur zur Vertragsabwicklung verarbeitet werden. In beiden Fällen bestehen Löschungs- beziehungsweise Anonymisierungsverpflichtungen, sobald die Daten nicht mehr zur Vertragserfüllung bzw. zur Fakturierung benötigt werden. Verfügen Telekommunikationsanbieter_innen als Vertragspartner_innen der Teilnehmer_innen über gewisse Daten, sind sie staatlichen Behörden in bestimmten Fällen zur Auskunft verpflichtet.

Anlassdatenspeicherung

Betroffene Daten und Dienstleistende

§§ 97, 99 TKG

➲ *9. 2 Datenschutz*

Von Anlassdatenspeicherung spricht man, wenn diese Daten auf Anordnung der Staatsanwaltschaft länger gespeichert werden müssen, als es im Regelfall erlaubt ist. Die grundsätzliche Löschungsverpflichtung des Telekommunikationsgesetzes wird somit durchkreuzt. Diese Bestimmung ist am 01.06.2018 in Kraft getreten und sieht vor, dass Daten aus einem bestimmten Anlass bis zu einem Jahr gespeichert werden müssen. Dafür genügt ein bloßer Anfangsverdacht.

§ 135 Abs. 2b StPO

Bei der Auskunft von Daten einer Nachrichtenübermittlung und der Anlassdatenspeicherung werden Standort-, Verkehrs- oder Stammdaten erfasst, während die Überwachung von Nachrichten den Inhalt von Kommunikation betrifft. Die einschlägigen Gesetze sind u.a. das polizeiliche Staatsschutzgesetz (PStSG), das Sicherheitspolizeigesetz (SPG), die Strafprozessordnung (StPO) sowie das Telekommunikationsgesetz (TKG).

Manche dieser Gesetze ergänzen einander, andere haben getrennte Anwendungsbereiche. Eine wichtige Abgrenzung ist die zwischen Sicherheitspolizeigesetz und Strafprozessordnung: Ersteres ist immer dann anwendbar, wenn ein gefährlicher Angriff verübt wurde oder ein solcher bevorsteht. Ein gefährlicher Angriff ist die Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung einer Straftat nach dem Strafgesetzbuch (StGB)[2] oder nach bestimmten Straftatbeständen des sog. „Nebenstrafrechts“, z.B. nach dem Fremdenpolizeigesetz oder dem Suchtmittelgesetz mit spezifischen Ausnahmen. Für das Verständnis ist wichtig, dass für die Anwendbarkeit des SPG noch keine Straftat verwirklicht sein muss, die Bedrohung der geschützten Rechtsgüter ist ausreichend. Die Beendigung tatsächlicher Angriffe ist natürlich auch von der sicherheitspolizeilichen Aufgabe „Gefahrenabwehr“ erfasst. Die Sicherheitsbehörden

➲ *4.1 Rechtsgrundlagen*

§ 16 SPG Anwendungsbereiche

haben die maßgeblichen Umstände und die Identität des_der Angreifer_in zu klären, wenn dies zur Vorbeugung weiterer gefährlicher Angriffe erforderlich ist. Sobald jedoch eine Person einer bestimmten Straftat verdächtig ist, ist ausschließlich die Strafprozessordnung anzuwenden. Die Abgrenzung kann im Einzelfall mitunter schwierig zu ziehen sein, was – im schlimmsten Fall – zur missbräuchlichen Anwendung von Befugnissen führen kann.

7.1 Definition der Datenarten

Verkehrsdaten werden auch Verbindungsdaten, äußere Gesprächsdaten oder Rufdaten genannt. Sie werden immer dann verarbeitet, wenn eine Nachricht an ein Kommunikationsnetz weitergeleitet wird, oder dieser Vorgang fakturiert, also in Rechnung gestellt, wird. Beispiele sind etwa die aktive und passive Teilnehmer_innennummer. Die aktive Teilnehmer_innennummer ist die, von der aus die Verbindung aufgebaut wird, die passive ist die, die angewählt wird. Auch Zeitpunkt und Dauer der Verbindung zählen zu den Verkehrsdaten. *§ 92 Abs. 3 Z 4 TKG*

Zugangsdaten sind jene Daten, die beim Zugang von Teilnehmer_innen zu einem öffentlichen Kommunikationsnetz bei den Betreiber_innen entstehen, und zählen ebenfalls zu den Verkehrsdaten. Sie sind zur Identifikation von Teilnehmer_innen einer Internetkommunikation notwendig. *§ 92 Abs. 3 Z 4a TKG*

Standortdaten beziehen sich auf die geografische Position der Telekommunikationsendeinrichtung von Nutzer_innen eines öffentlichen Kommunikationsdienstes. Sie werden in einem Kommunikationsnetz verarbeitet und umfassen jedenfalls jene Standortdaten, die während der von den Überwachten bewusst geführten Kommunikation anfallen. *§ 92 Abs. 3 Z 6 TKG*

Stammdaten sind Daten, die zur Vertragserfüllung notwendig sind: der Name, der akademische Grad, die Anschrift (Wohnadresse bei natürlichen Personen bzw. die Rechnungsadresse bei juristischen Personen), Teilnehmer_innennummer und sonstige Kontaktinformationen, Informationen über Art und Inhalt des Vertragsverhältnisses und die Bonität des_der Vertragspartner_in. *§ 92 Abs. 3 Z 3 TKG*

Inhaltsdaten beziehen sich auf den Inhalt von Kommunikation – beispielsweise Bilder oder den Text einer E-Mail oder einer SMS. *§ 92 Abs. 3 Z 5 TKG*

Viele Daten sind doppelfunktional und fallen in mehrere der oben genannten Kategorien, etwa die durch IMEI-Rasterung ermittelte Rufnummer. Die IMEI (International Mobile Equipment Identification) ist die fix mit einem Gerät verbundene Kennnummer. Bei der IMEI-Rasterung werden Netzbetreiber_innen aufgefordert, ihre Netzdaten danach durchzusehen, ob eine bestimmte IMEI darin aufscheint. Ist dies der Fall, ist die dazugehörige Rufnummer bekannt zu geben. Die Rufnummer ist einerseits Stammdatum, da sie als Teilnehmer_innennummer eine_r Nutzer_in fix zugewiesen ist. Andererseits kann sie auch Verkehrsdatum sein – der Auswertungskontext spielt hier die entscheidende Rolle. Wenn die Rufnummer also nicht durch einen bloßen Blick in die Kund_innendatei, sondern erst durch die Auswertung von Verkehrsdaten erhoben werden kann, ist sie selbst Verkehrsdatum. Anderes gilt, wenn Netzbetreiber_innen oder Diensteanbieter_innen zwar Verbindungsdaten auswerten, letztlich aber nur andere – nicht doppelfunktionale – Stammdaten (z.B. Name, Postadresse) der ermittelten Benutzer_innen bekannt geben. Dann sind diese Daten der Rechtsprechung zufolge Stammdaten.[3]

Sonderfall IP-Adressen: IP-Adressen stellen einen Sonderfall dar.[4] In § 92 Abs. 3 Z 16 TKG ist der Unterschied zwischen statischen und dynamischen IP-Adressen festgeschrieben: Während zweitere nur Zugangsdaten, also Verkehrsdaten sind, sind erstere zugleich auch Stammdaten. Das Interesse der Sicherheitsbehörden an einer Auskunft über eine_n – hinter einer IP-Adresse stehenden – Teilnehmer_in besteht darin, einen bereits bekannten Inhalt (z.B. die Nutzung eines Online-Dienstes, den Zugriff auf eine Website oder den Eintrag in einem Online-Forum) einer bestimmten Person zuordnen zu können. Der Inhalt ist also schon vorher bekannt, bleibt aber ohne die Verkehrsdaten-

auskunft ohne Personenbezug. Die Information darüber, wem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, stellt sozusagen den „missing link“ her, um öffentlich bekannte oder bei einem Dienstanbieter ausgeforschte Kommunikationsinhalte mit einer bestimmten Person zu verbinden. Zwar dürfen Internet-Zugangsanbieter_innen nicht aufzeichnen, welche Internetseiten von dem_der Teilnehmer_in aufgerufen wurden, viele Internetseiten bzw. -dienste sind allerdings technisch so konzipiert, dass bei Zugriffen auf diese Seiten oder Dienste die IP-Adresse des_der Teilnehmer_in sowie der Zeitpunkt des Zugriffs durch den Host-Provider protokolliert und bei manchen Anwendungen auch mit bestimmten Inhalten verknüpft wird (z.B. bei Einträgen in einem Online-Forum). Bei vielen Online-Diensten existieren auch Aufzeichnungen über das konkrete Nutzungsverhalten (z.B. Einkäufe bei Amazon.com, Ebay oder Suchanfragen bei Google). Gleichzeitig lässt sich daraus noch nicht ableiten, ob der_die Anschlussinhaber_in auch mit dem_der Urheber_in der Kommunikation ident ist. Die Information ist vielmehr bloß ein erster Ermittlungsansatz. Die Zuordnung von Verbindungsdaten (insbesondere IP-Adressen) zu einer bestimmten Person lässt selbst keine Rückschlüsse darüber zu, ob diese Person auch tatsächlich am fraglichen Kommunikationsvorgang beteiligt war. Hierzu bedarf es weiterer konkretisierender Indizien, welche gerade bei der Erforschung von Kommunikationsvorgängen im Internet häufig schwer fassbar sind. Anschaulich lässt sich eine IP-Adresse als eine Art Kfz-Kennzeichen auf dem „Datenhighway“ beschreiben. Vielfach wird daher eine Art „IT-Lenker_innenerhebung“ erforderlich sein, um Aussagekraft und Zuverlässigkeit der ermittelten Daten beurteilen zu können; denn eine reine Gefährdungshaftung für Inhaber_innen von Internet- oder Telefonanschlüssen ist der österreichischen Rechtsordnung bislang nicht bekannt.

Host-Provider

Die Judikatur des Obersten Gerichtshofes (OGH) in Strafsachen behandelte Auskünfte über Name und Anschrift zu einer bestimmten, bereits bekannten IP-Adresse lange als Stammdatenabfrage nach § 103 Abs. 4 TKG. Dass der_die Anbieter_in im Falle von dynamischen IP-Adressen für die Auskunft intern die Aufzeichnung der Zugangsdaten (also Verkehrsdaten) auswerten muss, wurde nach dieser sogenannten „ergebnisorientierten“ Sichtweise für unbeachtlich erklärt. Damit bestanden in Bezug auf IP-Adressen keine materiellen Einschränkungen auf bestimmte schwerere Delikte. Richter_innenvorbehalt oder sonstige Formerfordernisse mit Rechtsschutzcharakter gab es bei Stammdatenauskünften ebenso keine, vielmehr war sogar die Kriminalpolizei ohne Anordnung der Staatsanwaltschaft auskunftsberechtigt. Diese Auslegung verkannte völlig, dass diese Ermittlungsbefugnisse eigentlich eher in der Nähe einer Inhaltsüberwachung anzusiedeln sind. Mit der Legaldefinition der öffentlichen IP-Adresse in Verbindung mit der ausdrücklichen Rechtsgrundlage für Stammdatenauskünfte an Justizbehörden in § 90 Abs. 7 TKG löste der Gesetzgeber diese Widersprüche in der Judikatur auf und beschränkte die Stammdatenauskunft auf die Fälle, in denen keine Verkehrsdaten für die Auskunft ausgewertet werden müssen.[5] Sachlich besteht das Problem auf Grund der weiten Ausnahmen (s.u.) aber fast unverändert weiter. Eine Auskunftserteilung zu Name und Anschrift einer IP-Adresse ist im Rahmen eines zivilgerichtlichen Verfahrens (etwa in Zusammenhang mit Urheberrechtsverletzungen) nicht möglich.[6]

Auslegung des OGH GZ 11 Os 57/05z

§ 92 Abs. 3 Z 16 TKG

§ 99 Abs. 5 TKG iVm § 76a Abs. 2 StPO

7.2 Relevante Bestimmungen des Telekommunikationsgesetzes

Das Telekommunikationsgesetz (TKG) hat zum Ziel „durch Förderung des Wettbewerbes im Bereich der elektronischen Kommunikation die Versorgung der Bevölkerung und der Wirtschaft mit zuverlässigen, preiswerten, hochwertigen und innovativen Kommunikationsdienstleistungen zu gewährleisten.“ Darin werden die Rechte und Pflichten von Telekommunikationsanbieter_innen d.h. von Bereitsteller_innen eines Kommunikationsnetzes oder Betreiber_innen eines Kommunikationsdienstes oder -netzes normiert. Das Gesetz wurde im Rahmen der Umsetzungspflicht der Telekom-Datenschutzrichtlinie beschlossen.

§ 1 TKG

Richtlinie 2002/58/EG

Herausgabe von personenbezogenen Daten

Der 12. Abschnitt des TKG enthält detaillierte Bestimmungen zum Daten- und Geheimnisschutz im Bereich der Telekommunikation. Grundsätzlich gilt dabei, dass von Anbieter_innen von Kommunikationsdiensten Stammdaten nur für die Vertragsabwicklung und nur für die Dauer eines Rechtsverhältnisses verarbeitet werden dürfen, auch Verkehrsdaten sind nach dem Ende der Verbindung bzw. nach Abschluss der Übertragung zu löschen oder zu anonymisieren. Inhaltsdaten wiederum dürfen gar nicht erst gespeichert werden, außer diese Speicherung ist Teil des Dienstes, etwa bei Mailboxen oder Cloud-Services.

§§ 92 bis 107 TKG

§ 92 TKG, § 99 TKG, § 101 TKG

Anbieter_innen von Kommunikationsdiensten müssen in zwei Fällen auf schriftliches Verlangen von Verwaltungsbehörden, Gerichten, Staatsanwaltschaften und Kriminalpolizei Stammdaten an diese herausgeben:

§ 90 Abs. 6 und Abs. 7

1. Stammdaten von Personen, die in Verdacht stehen, durch eine über ein öffentliches Telekommunikationsnetz gesetzte Handlung eine Verwaltungsübertretung begangen zu haben, soweit die Herausgabe ohne Verarbeitung von Verkehrsdaten möglich ist. Die Ausnahme für Verkehrsdaten wurde eingefügt, damit nicht eine Verkehrsdatenauskunft als Stammdatenauskunft getarnt werden kann, indem z.B. statt den Stammdaten einer bestimmten verdächtigen Person die Stammdaten aller Personen, mit denen die verdächtige Kontakt hatte, verlangt werden.[7] Beispiele für derartige Handlungen, die eine Herausgabepflicht begründen, sind etwa: Die Zusendung unerwünschter SMS oder auch die Belästigung oder Verängstigung anderer Benützer_innen von Telekommunikationsendeinrichtungen.[8]

§ 107 TKG

§ 78 TKG

2. Zur Aufklärung und Verfolgung des konkreten Verdachts einer Straftat, an Gerichte, Staatsanwaltschaften, Kriminalpolizei, aber auch Sicherheitsbehörden und Finanzstrafbehörden. Letztere dürfen nach dieser Bestimmung nur die in § 53 Abs. 3a Z 1 SPG aufgezählten Stammdaten herausverlangen, das sind Name, Anschrift und Telefonnummer wenn diese zur Erfüllung ihrer Aufgaben notwendig ist, außerdem auch zur erweiterten Gefahrenforschung und zum Schutz vor verfassungsgefährdenden Angriffen, Finanzstrafbehörden nur wenn der Wertbetrag eines Finanzvergehens eine bestimmte Höhe überschreitet. In dringenden Fällen können solche Auskünfte außerdem vorläufig auch mündlich übermittelt werden. In diesen Fällen muss aber eine Nachschau in den Vertragsdaten ausreichen und es dürfen keine Verkehrsdaten, insbesondere keine IP-Adressen ausgewertet werden. Nur dann genügt ein schriftliches Verlangen der Kriminalpolizei oder der Staatsanwaltschaft ohne richterliche Genehmigung.[9]

§ 11 Abs. 1 Z 5 PStSG und § 99 Abs. 3a FinStrG

Somit können Behörden, unter anderem die Kriminalpolizei, bei einem Verdacht Daten wie Namen, Anschriften und sogar Informationen wie die Bonität und Geburtsdaten erhalten. Mangels Formulierungen, die darauf hindeuten würden („insbesondere“, „speziell“,...) müssen diese beiden Fälle als abschließende Aufzählung gelesen werden, aus anderen Gründen heraus dürfen Daten also nicht herausverlangt werden. Das bedeutet auch, dass etwaige neue Normen, die diese Kompetenzen ausweiten würden, zumindest in Konflikt mit dem TKG treten würden.

In § 93 TKG ist das Kommunikationsgeheimnis geregelt, dem Inhalts-, Verkehrs- und Standortdaten sowie Daten im Zuge erfolgloser Verbindungsversuche unterliegen. Alle Betreiber_innen sind zur Wahrung des Kommunikationsgeheimnisses verpflichtet. Sein Kern ist das Verbot von „Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige[m] Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie [der] Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer.“ Ausnahmen davon sind allerdings wiederum

Kommunikationsgeheimnis

- die Aufzeichnung und Rückverfolgung von Notrufen
- Fälle von Fangschaltung

- die polizeiliche Überwachung von Nachrichten
- die polizeiliche Auskunft über Daten einer Nachrichtenübermittlung
- Datenauskünfte nach § 99 Abs. 3a Finanzstrafgesetz, also Auskünfte über Namen, Anschrift oder Teilnehmernummer (also z.B. die identifizierenden Ziffern einer Telefonnummer, die auf eine Vorwahl wie 0699 oder 0676 folgen) die Auskunft über Daten nach § 11 Abs. 1 Z 7 PStSG, also Auskünfte über Verkehrsdaten, Zugangsdaten, Standortdaten von Betreiber_innen von Telekommunikationsdiensten und Diensteanbieter_innen (von Diensten der Informationsgesellschaft), eine technische Speicherung, die für die Weiterleitung erforderlich ist.

§ 3 Z 32 Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung 2009

Überdies wird auch in diesem Rahmen das Redaktionsgeheimnis (s.u.), das im Mediengesetz näher geregelt ist, hervorgehoben.

7.3 Überwachung von Nachrichten

§ 135 Abs. 3 StPO

Die Überwachung von Nachrichten betrifft Inhaltsdaten (s.o.), die Definition von Nachrichten wurde im Zuge des Überwachungspakets 2018 ausgeweitet: Nicht nur klassische Kommunikations-Informationen (wie WhatsApp-Nachrichten oder E-Mails) dürfen nun ausgelesen werden, sondern auch jegliche Informationen, die von einer Person über ein Computersystem verschickt oder empfangen werden (bspw. welche Webseiten eine Person aufruft), fallen darunter. Lediglich das Auslesen der gesamten Festplatte („Online-Durchsuchung“) oder automatische Backups sollen nicht zulässig sein. Die Tatsache, dass der Nachrichtenbegriff derart weit ist, erscheint problematisch. Es führt dazu, dass auch Daten über das Internetnutzungs-Verhalten, zum Beispiel eine Liste von aufgerufenen Webseiten ermittelt werden könnten. Häufig weiß man im Vorhinein nicht, welcher Inhalt sich konkret auf einer Webseite befindet, oder ob man einen Artikel gut oder schlecht finden wird, bevor man ihn liest. Über die tatsächliche Meinung der beschuldigten Person zu den aufgerufenen Inhalten kann nur gemutmaßt werden. Trotzdem sind diese Beweismittel dazu geeignet, eine Person in einem bestimmten Licht darzustellen. Daher werden sich angeklagte Personen dazu gezwungen sehen, sich zu den aufgerufenen Inhalten zu äußern. Es besteht daher die Gefahr, dass im Rahmen von Gerichtsverhandlungen vermehrt Meinungsbildungsprozesse kontrolliert werden.

Rechtshistorisch betrachtet handelt es sich bei der Nachrichtenüberwachung um den „Prototyp des geheimen Eingriffs in das Fernmelde- und Datengeheimnis sowie die geschützte Privatsphäre“[10], weshalb mancher Ansicht zufolge die Auskunft von Daten einer Nachrichtenübermittlung im Vergleich zur Überwachung von Nachrichten grundrechtlich weniger eingriffsintensiv sei. Diese Ansicht ist jedoch nicht mehr zeitgemäß, da je nach Intensität gewisser Auskunftsbegehren auch das Gegenteil der Fall sein kann. Die Überwachung von Nachrichten unterliegt dem Richtervorbehalt: Sie ist aufgrund einer gerichtlichen Bewilligung von der Staatsanwaltschaft anzuordnen.

§ 137 Abs. 1 StPO

7.3.1 Überwachung mit Zustimmung

Gibt der_die Inhaber_in eines Teilnehmer_innenanschlusses (die Person, die faktisch entscheiden kann, wer beispielsweise ihr Telefon wann benützen darf) seine_ihre Zustimmung zur Überwachung, darf bei einer Straftat von mehr als sechs Monaten Freiheitsstrafe bereits eine Überwachung von Nachrichten durchgeführt werden. Voraussetzung ist, dass dadurch die Aufklärung dieser Straftat gefördert werden kann und ein konkreter Verdacht in Bezug auf die begangene Straftat vorliegt.[11] Bei Unternehmen kann die Inhaberschaft beim Unternehmen oder bei dem_der Dienstnehmer_in liegen, wobei immer im Einzelfall zu prüfen ist, „wer darüber entscheidet, wann welche Einrichtungen von wem und zu welchen Zwecken (nur dienstlich oder auch privat) genutzt werden dürfen.“[12] Bei Internet-Cafés gestaltet sich die Sache komplizierter: Gäste nutzen die PCs nur kurzfristig und der_die Betreiber_in kann die Nutzung jederzeit beenden, weshalb ihm oder ihr die Inhaberschaft zukommt. Die Überwachung der IP-Adresse erfordert daher die Zustimmung der Café-Betreiber_innen. Setzt die Überwachung aber an der E-Mail-Adresse an, bei der der_die Nutzer_in Verfügungsberechtigte_r ist, genügt die Zustimmung des_der Betreiber_in des Cafés nicht.[13] Bei Zustimmung des_der Inhaber_in muss die Überwachung zwar verhältnismäßig sein, es ist aber nicht notwendig, dass die Daten anders nicht erhoben werden können.[14] Wie der Verfassungsgerichtshof (VfGH) jedoch erst jüngst zum geplanten Bundestrojaner urteilte, vermag die Tatsache, dass der_die Inhaber_in eines überwachten Computersystems dieser Maßnahme zustimmen muss, bloß die Überwachung der Privatsphäre des Zustimmenden zu rechtfertigen. Dass eine solche Maßnahme aber auch einen Eingriff in die Rechtssphäre dritter Personen bedeutet, die von der Überwachung betroffen sind und auf die Integrität der Kommunikation mit anderen vertrauen können, ließ der Gesetzgeber hier außer Acht.

Internet-Cafés

VfGH G 72-74/2019 G 181-182/2019

7.3.2 Überwachung ohne Zustimmung

Bei der Überwachung von Nachrichten ohne Zustimmung – dies stellt die weitaus höhere Anzahl der Fälle dar – sind die Voraussetzungen strenger. Die Verhältnismäßigkeit muss gegeben sein: Dabei wird im Wesentlichen das Interesse an der Aufklärung der Straftat gegen die Nachteile einer solchen Überwachungsmaßnahme abgewogen. Nachteile stellen etwa auch Eingriffe in die Grundrechte unbeteiligter Personen dar, die aufgrund der Streuwirkung mitüberwacht werden, was in die Verhältnismäßigkeitsprüfung einzubeziehen ist. Es gibt mehrere Fälle, in denen eine Überwachung ohne Zustimmung des_der Inhaber_in der technischen Einrichtung durchgeführt werden kann.

Bundestrojaner

➲ *9.1.3 Verhältnismäßigkeitsprüfung*

Der klassische Fall: Überwachung zu Aufklärungszwecken

Der klassische Fall ist die Überwachung zu Aufklärungszwecken, bei der eine mit mehr als einjähriger Freiheitsstrafe bedrohte Straftat aufgeklärt werden soll. Hierfür ist das Vorliegen eines dringenden Tatverdachts Voraussetzung, es muss also „ein höherer Grad von Wahrscheinlichkeit [vorliegen], dass der Beschuldigte die ihm angelastete Straftat begangen hat.“[15] Die Überwachung zu Aufklärungszwecken darf angewendet werden, wenn der_die Inhaber_in der Einrichtung selbst dringend im Verdacht steht, die Straftat begangen zu haben, oder bestimmte Tatsachen für die Annahme sprechen, dass ein_e dringend Verdächtige_r die technische Einrichtung nützen oder eine Verbindung mit ihr herstellen[16], also aktiv tätig werden wird.

Überwachung bei Organisationsdelikten

Organisationsdelikte sind strafbare Handlungen, die im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation begangen oder geplant werden. Voraussetzung für die Telekommunikationsüberwachung ist hier, dass die Aufklärung dieser Delikte bei Nichtdurchführung der Überwachung wesentlich erschwert wäre, wie z.B. durch erhebliche zeitliche Verzögerungen oder finanzielle Aufwendungen. Auch die Überwachung bei Organisationsdelikten setzt voraus, dass entweder der_die Inhaber_in der Einrichtung selbst in einem dringenden Verdacht steht, oder die Annahme besteht, dass eine andere dringend verdächtigte Person die technische Einrichtung nützt oder eine Verbindung mit ihr herstellen wird. Es muss sich um die Aufklärung einer Straftat handeln, die mit mehr als einem Jahr Freiheitsstrafe bedroht ist. Das kann auch das Organisationsdelikt selbst sein, also etwa die Mitgliedschaft in einer einschlägigen Gruppe. Auch geplante oder begangene strafbare Handlungen im Rahmen dieser Gruppierung sind einer Überwachung zugänglich, selbst wenn sie nicht mit mehr als einem Jahr Freiheitsstrafe bedroht sind oder es sich um Fahrlässigkeitsdelikte handelt. Bei

§ 135 Abs. 3 Z 2

§ 135 Abs. 3 Z 3 StPO

weniger schwerwiegenden Delikten (oder gar Fahrlässigkeitsdelikten) wird eine Überwachungsmaßnahme jedoch an einer Verhältnismäßigkeitsprüfung scheitern.[17]

Überwachung bei Geiselnahme

§ 136 Abs. 1 Z 1 StPO

Diese Konstellation deckt sich überwiegend mit dem Wortlaut der optischen und akustischen Überwachung von Personen. Die einschlägigen Entführungsdelikte sind Straftaten, die durchwegs mit mehr als einjähriger Freiheitsstrafe bedroht sind, weshalb die Einführung dieser Bestimmung redundant war – eine Überwachung wäre davor auch nach den übrigen, oben dargestellten Überwachungsbefugnissen möglich gewesen.[18] Es genügt nämlich gerade nicht eine einfache Freiheitsentziehung, sondern die Bestimmung setzt schwerwiegendere Fälle von Geiselnahmen wie erpresserische Entführungen voraus. Zudem muss ein dringender Verdacht des Vorliegens einer solchen Entführung bestehen. Die Überwachung muss sich auf Nachrichten des Beschuldigten beschränken, womit die Streuwirkung einer solchen Maßnahme begrenzt werden soll. Eine zusätzliche Voraussetzung – die sich nicht aus dem Gesetzestext zur Befugnis, jedoch aus dem Grundsatz der Verhältnismäßigkeit ergibt – ist, dass zu erwarten ist, dass die Überwachung zur Beendigung der Geiselnahme beitragen kann.[19]

Überwachung zur Aufenthaltsermittlung

Diese Bestimmung umfasst jene Fälle, in denen ein_e Beschuldigte_r einer strafbaren Handlung dringend verdächtig ist, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, deckt sich also insofern mit den übrigen Fällen. Der Zweck der Maßnahme ist jedoch ein anderer: Er muss der Ermittlung des Aufenthaltsortes der dringend verdächtigten beschuldigten Person dienen, wenn diese flüchtig oder abwesend ist. Nach dem Wortlaut dieser Bestimmung gibt es keine Beschränkung auf bestimmte Kommunikationsanlagen. Aus dem Verhältnismäßigkeitsgrundsatz ergibt sich jedoch, dass eine Überwachung nur jener Kommunikationsmittel möglich ist, die entweder der_die Beschuldigte selbst oder eine Kontaktperson innehat, bei der davon auszugehen ist, dass der_die Beschuldigte sie kontaktieren wird. Die Überwachung einer Telekommunikationsanlage, bei der nur zwischen an der Straftat unbeteiligten Dritten kommuniziert wird, ist – entgegen dem Wortlaut der Bestimmung – nicht zulässig.[20]

§ 135 Abs. 3 StPO

Die Voraussetzungen einer Nachrichtenüberwachung sind also folgende:

- Es besteht ein dringender Verdacht, dass eine Person eine andere entführt hat oder sich „sonst ihrer bemächtigt hat“

  UND

- die Auskunft beschränkt sich auf Daten einer Nachricht, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung von dem_der Beschuldigten empfangen oder gesendet wird;

ODER

- Erwartungsgemäß kann dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden

  UND

- der_die Inhaber_in der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, stimmt der Überwachung ausdrücklich zu;

ODER

Strafprozessordnung (StPO)

- Die Überwachung erscheint zur Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einem Jahr Freiheitstrafe bedroht ist, erforderlich

  ODER

- die Aufklärung oder Verhinderung von im Rahmen einer terroristischen oder kriminellen Vereinigung oder Organisation begangenen oder geplanten Straftaten wäre ansonsten wesentlich erschwert

  Zustimmung d. Inhaber_in

  UND

- der_die Inhaber_in der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, ist einer vorsätzlich begangenen Straftat, die mit mehr als einem Jahr Freiheitsstrafe bedroht ist, oder einer Straftat gemäß §§ 278 bis 278b StGB dringend verdächtig

  Mitgliedschaft in einer kriminellen Vereinigung, kriminellen Organisation oder terroristischen Vereinigung

  ODER

- aufgrund bestimmter Tatsachen ist anzunehmen, dass eine der oben genannten Tat dringend verdächtige Person die technische Einrichtung benützen oder mit ihr eine Verbindung herstellen werde

ODER

- aufgrund bestimmter Tatsachen ist anzunehmen, dass dadurch der Aufenthalt eine_r flüchtigen oder abwesenden Beschuldigten, der_die einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.

Häufigkeit

§ 135 Abs. 3 StPO

Seit 2008 haben sich die Einsätze der Nachrichtenüberwachung verdreifacht.[21] Die Überwachung von Nachrichten wird oft angewandt: Allein im ersten Halbjahr 2019 wurden 1.878 Überwachungen durchgeführt, es gab 109 Anklagen und 38 Verurteilungen in diesem Zeitraum.[22] Die Zahl der Bewilligungen einer Nachrichtenüberwachung ist im Steigen begriffen, während die danach erfolgenden Anklagen und Verurteilungen zurückgehen.[23] Diese Divergenz ist aus der Grafik auf nächster Seite gut sichtbar.

7.4 Auskunft von Telekommunikationsdaten

Bei der Überwachung von Nachrichten, wie im vorherigen Kapitel, handelt es sich also um das direkte Abrufen („Anzapfen“) von Kommunikationsvorgängen und Inhaltsdaten. Wird ein Telefonat überwacht, bedeutet dies, dass das Gespräch durch die Behörde mitgehört wird. Bei der Auskunft von Telekommunikationsdaten hingegen werden Daten, die der_die Telekommunikationsanbieter_in gespeichert hat, an die Behörde weitergegeben.
Die österreichische Rechtsordnung kennt kein Gesetz, in dem alle behördlichen Befugnisse zur Auskunft von Telekommunikationsdaten festgesetzt sind. Vielmehr handelt es sich um eine Vielzahl an Bestimmungen in unterschiedlichen Gesetzen, die aufeinander verweisen oder einander ergänzen. Die ISPA (Internet Service Providers Austria) haben hierzu eine umfassende Übersicht zusammengestellt, aus der die Rechtsnormen, die zu beauskunftenden Datenarten, die Art der Anfrage (schriftlich oder mündlich), die Pflicht zur Nutzung der dafür vorgesehenen „Durchlaufstelle“ (DLS) zur Datenübertragung und die

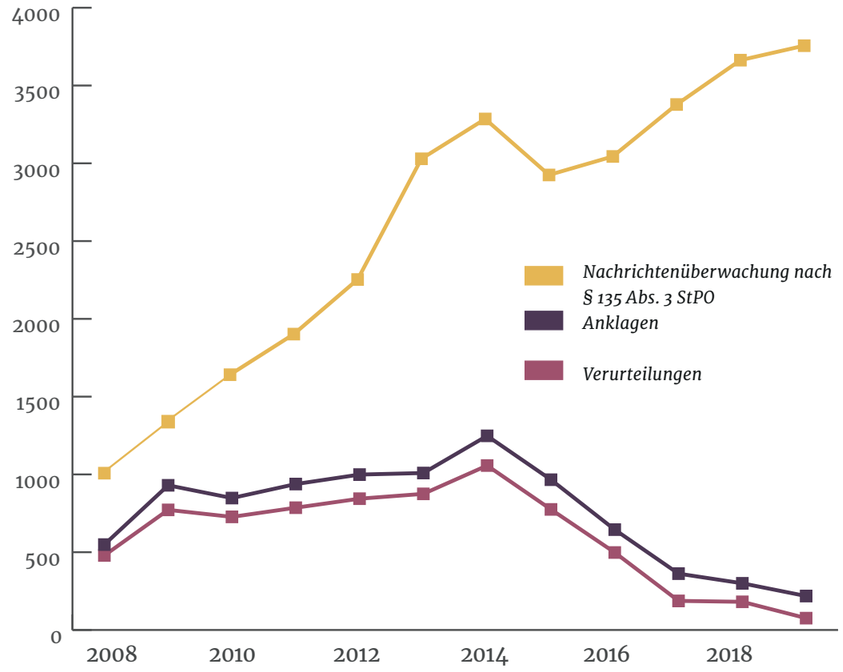


Abb. 10 Nachrichtenüberwachung nach § 135 Abs. 3 StPO, Anklagen und Verurteilungen 2008–2019

anfrageberechtigte Stelle (Polizei, Staatsanwaltschaft oder Gericht) hervorgehen.[24] Die für die Auskunft von Telekommunikationsdaten anzuwendenden Gesetze sind u.a. das polizeiliche Staatsschutzgesetz (PStSG), das Sicherheitspolizeigesetz (SPG), die Strafprozessordnung (StPO) sowie das Telekommunikationsgesetz (TKG).

Gefährlicher Angriff

Das SPG ist immer dann anwendbar, wenn ein gefährlicher Angriff verübt wurde. Dann haben die Sicherheitsbehörden die maßgeblichen Umstände und die Identität des Angreifers oder der Angreiferin zu klären, wenn dies zur Vorbeugung weiterer gefährlicher Angriffe erforderlich ist. Sobald jedoch eine Person einer bestimmten Straftat verdächtig ist, ist zur Ermittlung ausschließlich die StPO anzuwenden. Das PStSG hingegen kann parallel zur StPO angewendet werden, weil eine Subsidiaritätsklausel wie im SPG fehlt. Es kommen somit unter Umständen beide Gesetze parallel zur Anwendung[25], was freilich für Verwirrung sorgen kann.

➲ *4.1 Rechtsgrundlagen § 22 Abs. 3 Satz 2 SPG*

Für diese Ermittlungen im sicherheits- und kriminalpolizeilichen Bereich sowie auf dem Gebiet des polizeilichen Staatsschutzes müssen jedoch nicht nur die Voraussetzungen des SPG, der StPO oder des PStSG erfüllt sein – es muss immer auch eine korrelierende Bestimmung im Telekommunikationsgesetz (TKG) bestehen, um Telekommunikationsanbieter_innen zu dieser Auskunft überhaupt erst zu ermächtigten oder zu verpflichten.

7.4.1 Auskunft von Telekommunikationsdaten nach der Strafprozessordnung (StPO)

§ 135 Abs. 2 StPO, § 99 Abs. 5 Z 1 TKG

In der StPO sind mehrere Fälle normiert, in denen Behörden eine Auskunft von Telekommunikationsdaten durch Betreiber_innen und Diensteanbieter_innen verlangen können. Diese decken sich teilweise mit den Fällen, in denen auch

eine Nachrichtenüberwachung möglich ist. Diese Bestimmungen betreffen Verkehrsdaten, Zugangsdaten (z.B. IMSI, IMEI) und Standortdaten.

Die Möglichkeit der Auskunft von Daten besteht zum einen bei Zustimmung des_der Inhaber_in der technischen Einrichtung, zum anderen bei einer Entführung oder einer sonstigen Bemächtigung – diese Fälle sind im Detail bei den Ausführungen über die Nachrichtenüberwachung nachzulesen. Auch die Auskunft zur Aufenthaltsermittlung entspricht der Überwachung von Nachrichten zur Aufenthaltsermittlung.

§ 135 Abs. 3 StPO

Schließlich gibt es in der StPO einen weiteren Fall, der von der Überwachung von Nachrichten insofern abweicht, als durch die Auskunft die Aufklärung der Tat lediglich gefördert werden muss, also sie mit einer gewissen Wahrscheinlichkeit zu zweckdienlichen Ermittlungsergebnissen führen muss.[26] (Im Vergleich dazu muss bei der Überwachung von Nachrichten diese Maßnahme zur Aufklärung erforderlich sein.) Weiters weicht der Fall dahingehend ab, dass kein dringender Tatverdacht notwendig ist – bereits ein hinreichender Tatverdacht genügt. Schließlich ist hier nicht erforderlich, dass sich die Auskunft nur auf einen Anschluss bezieht, deren Inhaber_in selbst (dringend) verdächtig ist, es muss lediglich anzunehmen sein, dass dadurch Daten des Beschuldigten ermittelt werden können. Die Voraussetzungen sind daher weit weniger streng. Grund dafür ist, dass diese Maßnahme als weniger eingriffsintensiv gesehen wird, da sie keine Inhaltsdaten betrifft. Diese Ansicht entspricht allerdings nicht der Realität. Punktuelle und zeitlich (sehr) beschränkte Datenerhebungen mögen nicht so schwerwiegend sein, allerdings ist die Erstellung kompletter Profile ein sehr gewichtiger Eingriff, der in seiner Intensität durchaus mit der Überwachung von Inhaltsdaten auf einer Stufe steht.[27]

Die Voraussetzungen einer Weitergabe an die Behörde von Telekommunikationsdaten sind folgende:

- dringender Verdacht, dass eine Person eine andere entführt hat oder sich „sonst ihrer bemächtigt hat“

UND

- die Auskunft beschränkt sich auf Daten einer Nachricht, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten empfangen oder gesendet wird;

ODER

- erwartungsgemäß kann dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden

UND

- Der_die Inhaber_in der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, stimmt der Auskunft ausdrücklich zu;

ODER

- erwartungsgemäß kann dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einem Jahr Freiheitsstrafe bedroht ist, gefördert werden

UND

- auf Grund bestimmter Tatsachen ist anzunehmen, dass dadurch die Daten des_der Beschuldigten ermittelt werden können.

ODER

- Auf Grund bestimmter Tatsachen ist anzunehmen, dass dadurch der Aufenthalt eine_r flüchtigen oder abwesenden Beschuldigten, der_die einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.

§ 137 Abs. 1StPO

Auch diese Ermittlungsmaßnahme unterliegt dem Richter_innenvorbehalt. Sie wird also von der Staatsanwaltschaft aufgrund einer gerichtlichen Bewilligung angeordnet.

Häufigkeit

Die Anwendung dieses Paragraphen ist im Steigen begriffen, während die infolge einer solchen Auskunft erfolgenden Anklagen und Verurteilungen stark zurückgehen, was aus folgender Grafik sehr anschaulich hervorgeht:

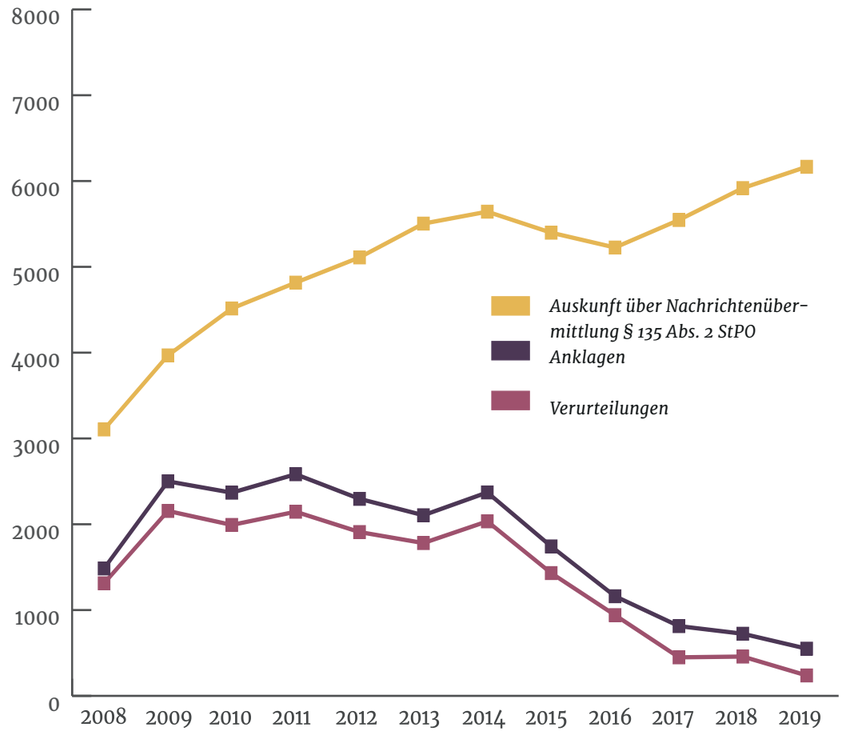


Abb. 11
Datenauskunft nach § 135 Abs. 2 StPO

Der Schutz besonderer Geheimnisse und die Überwachung von Nachrichten und die Auskunft von Telekommunikationsdaten

➲ *4.4 Berufsgeheimnisträger_innen und Beweisverwertungsverbote*
Amtsverschwiegenheit

§ 144 StPO

In der StPO werden Berufsgeheimnisse besonders geschützt – zum einen die geistliche Amtsverschwiegenheit, und zum anderen jene Geheimnisse, die durch ein Aussageverweigerungsrecht geschützt sind. Davon sind Berufsgruppen umfasst, die von einem Vertrauensverhältnis abhängen, etwa Rechtsanwält_innen, Psychiater_innen, Psychotherapeut_innen und Psycholog_innen oder Mitarbeiter_innen von Medienunternehmen. Das bedeutet zum Beispiel, dass ein_e Psychotherapeut_in die Aussage stets verweigern darf, selbst wenn ihm_ihr im Zusammenhang mit seiner_ihrer beruflichen Tätigkeit zur Aufklärung einer Straftat bedeutsame Informationen zugekommen sind – etwa, weil er_sie eine verdächtige Person behandelt. Das in diesem Zusammenhang bestehende Umgehungsverbot ist stets zu beachten: Das Berufsgeheimnis darf nicht dadurch umgangen werden, dass ein von dieser Person beruflich genutzter Anschluss überwacht wird, um die Ergebnisse dann im Verfahren zu verwerten. Allerdings ist dieses Umgehungsverbot keinesfalls absolut: Zum einen besteht es nicht, wenn die betreffende Person – also der_die Berufsgeheimnisträger_in – selbst der Tat dringend verdächtig ist. Sehr wohl ist aber trotz des Umgehungsverbots die Überwachung von Nachrichten möglich, wenn sie das Telefon (oder andere Kommunikationseinrichtungen) der beschuldigten Person oder einer dritten Kontaktperson betrifft, von dem aus die Kommunikation mit eine_r Berufsgeheimnisträgerin passiert. Ein Telefongespräch mit einer Psychotherapeutin kann also im Zuge der Überwachung des Handys des_der Tatverdächtigen durchaus überwacht werden: Dieses Handy ist nicht für die Kommunikation mit der Psychotherapeutin ausgelegt. Jedoch darf das entsprechende Gespräch nicht verwertet werden und ist zu löschen.[28]

Berufsgeheimnis und Umgehungsverbot

In der Praxis stellt dies ein Problem dar, da elektronische Daten oftmals in riesigen Mengen sichergestellt werden. Vorab erfolgt keine Überprüfung ihrer Relevanz für das jeweilige Verfahren. Diese Datenmengen müssen anschließend von Staatsanwaltschaften, aber auch Gerichten im Hinblick auf die Betroffenheit von Berufsgeheimnissen, durchforstet werden. Sicherstellungen bei Berufsgeheimnissen erzeugen somit große Unsicherheiten, zum Beispiel im Widerspruchverfahren.[29]

§ 112 StPO

7.4.2 Auskunft von Stamm- und Zugangsdaten nach der Strafprozessordnung (StPO)

Stammdaten

Zur Auskunft über Stammdaten sind Anbieter_innen von Kommunikationsdiensten, also auf jeden Fall Access-Provider verpflichtet; unklar ist, ob auch Host-Provider dazu verpflichtet sind. Notwendig ist dafür der konkrete Verdacht auf eine Straftat, der sich auch auf eine konkret bestimmte Person beziehen muss. Auskünfte über Stammdaten können über Teilnehmer_innen verlangt werden, also über Personen, die mit Kommmunikationsdienstleister_innen einen Vertrag haben. Begründung ist dafür keine notwendig. Das Auskunftsersuchen ist schriftlich zu stellen, ausgenommen sind „dringende Fälle“, bei denen das schriftliche Ersuchen aber zumindest nachgeliefert werden muss.

§ 76a StPO iVm
§ 90 Abs. 7 TKG

📖 *Host-Provider*

Gefahr in Verzug Regelung

Zugangsdaten

Für eine Auskunft über Zugangsdaten ist nach der StPO jedenfalls eine Anordnung durch die Staatsanwaltschaft notwendig, im Gegensatz zu einer Auskunft über Stammdaten kann die Polizei Zugangsdaten also nicht von sich aus herausverlangen. Eine Anordnung auf Stammdatenauskunft muss außerdem Beschuldigten und sonstigen Betroffenen unverzüglich zugestellt werden. Verpflichtet sind auf jeden Fall Access-Provider und zwar solche, die zusätzlich dazu eine E-Mail-Adresse bereitstellen. Reine Host-Provider, zumindest nach Heißl, sind nicht dazu verpflichtet.
§ 76a StPO sieht also eine Auskunft von Stamm- und Zugangsdaten zur Aufklärung des konkreten Verdachts einer Straftat einer bestimmten Person über Stammdaten eine_r Teilnehmer_in vor; es ist der konkrete Verdacht auf eine Straftat notwendig, der sich auf eine konkret bestimmte Person beziehen muss. Es sind nicht alle Arten von Zugangsdaten durch § 76a StPO erfragbar. Über folgende Daten muss Auskunft gegeben werden:

- Name, Anschrift und Teilnehmer_innenkennung eine_r Teilnehmer_in, dem_der zu einem bestimmten Zeitpunkt eine öffentliche IP-Adresse zugewiesen (Auskunft bei „dynamischer IP-Adresse“). Es sei denn, diese Zuordnung würde eine größere

Zahl von Teilnehmer_innen erfassen (z.B. bei Network-Adress-Translation (NAT))

ODER

- bei der Verwendung von E-Mail-Diensten die dem_der Teilnehmer_in zugewiesene Teilnehmer_innenerkennung

ODER

- Name und Anschrift des_der Teilnehmer_in, dem_der eine E-Mail-Adresse zu einem bestimmten Zeitpunkt zugewiesen war

ODER

- die E-Mail-Adresse und die öffentliche IP-Adresse des_der Absender_in einer E-Mail.[30]

Auskunftsanordnungen nach § 76a StPO erfolgten im ersten Halbjahr 2019 499 Mal.[31] Es erfolgten sechs Anklagen und zwei Verurteilungen.[32] Im Jahr 2018 waren es insgesamt 1081 Auskunftsbegehren, 32 Anklagen und 15 Verurteilungen.[33] 2017 waren es 927 Fälle, worauf 23 Anklagen und 10 Verurteilungen erfolgten.[34]

7.4.3 Auskunft von Telekommunikationsdaten nach dem Sicherheitspolizeigesetz (SPG)

§ 53 Abs. 3a / 3b SPG iVm § 90 Abs. 7 TKG

Nach dem SPG können Auskünfte zur Gefahrenabwehr oder zur ersten allgemeinen Hilfeleistungspflicht eingeholt werden. Diese Auskunftsbefugnisse unterliegen keinem Richter_innenvorbehalt. Die Auskunft nach dem SPG umfasst Stammdaten, aber auch IP-Adressen, Stammdaten zu IP-Adressen, passive Rufdaten, IMSI- und Standortdaten.

das Sicherheitspolizeigesetz (SPG)

Diese Auskunft ist möglich bei Vorliegen folgender Voraussetzungen	**Über folgende Daten**
Die Daten sind zur Erfüllung der nach dem SPG übertragenen Aufgaben erforderlich	Name, Anschrift, Teilnehmer_innennummer eines bestimmten Anschlusses
Die Daten sind wesentliche Voraussetzung zur Abwehr einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht ODER eines gefährlichen Angriffs ODER einer kriminellen Verbindung	IP-Adressen zu einer bestimmten Nachricht sowie Zeitpunkt ihrer Übermittlung Namen und Anschrift eine_r Benutzer_in, dem_der eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war
Die Daten sind zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht ODER zur Abwehr gefährlicher Angriffe erforderlich	Name, Anschrift, Teilnehmer_innennummer eines bestimmten Anschlusses durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmer_innennummer
Die Daten sind zur Abwehr einer gegenwärtigen Gefahr erforderlich ODER zur Abwehr gefährlicher Angriffe erforderlich	Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem_der Gefährder_in oder von dem gefährdeten oder diesen begleitenden Menschen mitgeführten Endeinrichtungen – dabei wird es sich vornehmlich um Mobiltelefone handeln –, sowie technische Mittel zur Lokalisierung der Endeinrichtung zum Einsatz zu bringen.

7.4.4 Auskunft von Telekommunikationsdaten nach dem polizeilichen Staatsschutzgesetz (PStSG)

Nach dem PStSG können Auskünfte über bestimmte Gruppierungen und Betroffene sowie zu deren Kontakt- oder Begleitpersonen verlangt werden. Davon sind Gruppierungen erfasst, von denen zu erwarten ist, dass von ihnen Straftaten ausgehen, die eine schwere Gefahr für die öffentliche Sicherheit darstellen, weil ihre Strukturen oder zu erwartende Entwicklungen in deren Umfeld dies nahelegen. Hierunter fällt „insbesondere ideologische oder religiös motivierte Gewalt“, so der schwammige O-Ton des Gesetzes. Betroffene Person ist hier, wer unter begründetem Verdacht steht, in Zukunft einen verfassungsgefährdenden Angriff zu verüben.

PStSG
➲ *4.1 Rechtsgrundlagen*

Die Auskunft von Telekommunikationsdaten nach § 11 Abs. 1 Z 5 PStSG

§ 11 Abs. 1 Z 5 PStSG

Zum Zweck der erweiterten Gefahrenerforschung und des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen kann der Verfassungsschutz Telekommunkationsdaten herausverlangen, wie nach dem SPG (s.o.). Hierbei handelt es sich um die Auskunft über Stammdaten, IP-Adressen, IMSI und Standort-Daten. Es gibt also mehrere Konstellationen: Zum einen ist eine Auskunft über Namen, Anschrift und Teilnehmer_innennummer eines bestimmten Anschlusses möglich. Zum zweiten kann eine Auskunft über eine IP-Adresse erteilt werden, wenn eine bestimmte Nachricht und der Zeitpunkt ihrer Übermittlung bekannt sind. Ein Anschluss umfasst in diesem Zusammenhang Telefon- und Handynummer, aber nicht IP-Adressen.[35] Als dritter Fall können Namen und Anschrift eine_r Benutzer_in erfragt werden, dem_der eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war. Diese Bestimmung kommt z.B. bei anonymen Postings im Internet zum Tragen.[36] Standortdaten und IMSI von Endeinrichtungen können ebenso erfragt werden. Dazu zählen Mobiltelefone, aber auch Laptops oder Tablets, die über W-LAN-Netzwerke oder SIM-Karten geortet werden können.[37] Die hier beschriebenen Auskunftsbefugnisse beziehen sich auch auf Kontakt- oder Begleitpersonen der Verdächtigen.

Die Auskunft von Telekommunikationsdaten nach § 11 Abs. 1 Z 7 PStSG

§ 6 Abs. 1 Z 2 PStSG

Auch diese Bestimmung bezieht sich auf oben beschriebene Gruppierungen – in der Rechtsanwendung bleibt dieser Passus aber ohne Bedeutung, da der verfassungsgefährdende Angriff sich nur auf Einzelpersonen bezieht. Einen solchen Angriff, der von einer Gruppierung verübt wird, gibt es also gar nicht – es handelt sich um eine normative Unstimmigkeit.[38] Zur Vorbeugung verfassungsgefährdender Angriffe, deren Verwirklichung mit mehr als einem Jahr Freiheitsstrafe bedroht ist, ist das Einholen von Auskünften über Verkehrsdaten, Zugangsdaten und gewisser Standortdaten zulässig, wenn die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre.

§ 94 TKG

Diese verschiedenen Datenkategorien können ein umfassendes Persönlichkeitsbild liefern, was potentiell sehr eingriffsintensiv sein kann: Sämtliche sozialen Kontakte werden ebenso erfasst wie die Intensität der Kommunikationsbeziehungen. Zusätzlich kann ein Bewegungsprofil erstellt werden, das jede Ortsveränderung aufzeichnen kann. Der Eingriff ist somit durch die verschiedenen Datenstränge und deren Beziehung zueinander potentiell ein durchaus tiefgehender.[39]

Ein richterlicher Befehl ist für keine der Ermittlungsbefugnisse des PStSG – ebenso wie im SPG – vorgesehen. Bedenken zum Gesetzesentwurf ob der Eingriffsintensität mancher Maßnahmen gab es einige.[40] Auf die Kritik an der fehlenden richterlichen Anordnung im PStSG reagierte der Gesetzgeber mit Einführung des Rechtsschutzsenates – ein_e Rechtsschutzbeauftragte_r und zwei Stellvertreter_innen –, der mit Stimmenmehrheit seine Zustimmung zur Durchführung der Ermittlungsmaßnahme etwa zu § 11 Abs. 1 Z 7 PStSG gibt.

RSB

7.5 Anlassdatenspeicherung

Anlassdatenspeicherung §§ 135 Abs. 2b, 134 Z 2b StPO

Die Anlassdatenspeicherung besteht im Verbot der Löschung von bereits gespeicherten Verkehrsdaten durch den_die Telekommunikationsanbieter_in, insbesondere Daten, die für die Verrechnung von Leistungen benötigt werden. Sie sind grundsätzlich zu löschen, sobald dies nicht mehr der Fall ist. Diese Daten müssen nun auf Anordnung gespeichert bleiben. Es handelt sich also um das Einfrieren von bereits gespeicherten Verkehrsdaten (*Quick-Freeze*). Die Anlassdatenspeicherung wurde als Teil des Überwachungspakets eingeführt und ist seit 01.06.2018 in Kraft.

Sicherheitspaket

Die Anlassdatenspeicherung setzt voraus:

§ 135 Abs. 2b StPO

- einen Anfangsverdacht

  UND

- dass die Sicherung einer Auskunft über Daten einer Nachrichtenübermittlung dient

  UND

- dass dadurch erwartungsgemäß die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann

  UND

- dass der_die Inhaber_in der technischen Einrichtung, der_die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt,

  ODER

- dass dadurch erwartungsgemäß die Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einem Jahr Freiheitsstrafe bedroht ist, gefördert werden kann

  UND

- auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch die Daten des_der Beschuldigten ermittelt werden können,

  ODER

- dass auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch der Aufenthalt einer flüchtigen oder abwesenden beschuldigten Person, die einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.

Die Speicherung der Daten kann von der Staatsanwaltschaft allein angeordnet werden. Hier ist keine gerichtliche Bewilligung notwendig. Verhärtet sich der Verdacht in Folge und wird er zu einem „konkreten Tatverdacht", wird neben der Speicherverpflichtung auch der Zugriff auf die Daten möglich. In Fällen des § 135 Abs. 2 StPO bedarf der Zugriff auf die gespeicherten Daten einer gerichtlichen Bewilligung. Nach § 76a StPO haben kriminalpolizeiliche Behörden und Staatsanwaltschaften aber auch ohne gerichtliche Bewilligung das Recht auf Auskunft über Stamm- und Zugangsdaten (s.o.). Dieses Recht gilt auch bei Auskunft über Daten, die nur aufgrund einer Anlassdatenspeicherung nicht gelöscht wurden.[41] In den Erläuterungen wird die Rechtsauffassung vertreten, die Regelung würde im Einklang mit der Rechtsprechung des EuGH stehen, weil der Zugriff auf die gespeicherten Daten einer gerichtlichen Bewilligung unterliegt. Dies entspricht jedoch nicht der Realität[42], weil der EuGH bereits in Digital Rights Ireland urteilte, dass schon die Speicherpflicht selbst einen Grundrechtseingriff in das Recht auf Achtung des Privat- und Familienlebens darstellt. Der Zugriff der Behörden wird vom EuGH als nachstehender zusätzlicher Grundrechtseingriff beurteilt.

Speicherpflicht als Grundrechtseingriff

Art. 7 GRC
EuGH Digital Rights Ireland, Rn 34

Einerseits ist eine Anlassdatenspeicherung bei Daten möglich, die nach § 135 Abs. 2 StPO erlangt wurden, andererseits soll sie aber auch für Anordnungen

Vorratsdatenspeicherung

nach § 76a StPO angewendet werden können, wonach jeder konkrete Verdacht auf eine Straftat reicht, um eine Auskunft über Zugangs- und Stammdaten zu rechtfertigen. Eine Vorratsdatenspeicherung ist jedoch nur zur Bekämpfung schwerer Straftaten zulässig.[43] Zwar findet sich eine Definition des Begriffs der schweren Straftaten weder in der Judikatur des EuGH noch in der österreichischen Gesetzeslage, die Strafrahmen, die im konkreten Fall vorliegen müssen, sind jedoch nicht sehr hoch – im Fall des § 135 Abs. 2 StPO handelt es sich um ein Mindeststrafmaß von einem halben Jahr bzw. einem Jahr, im Fall des § 76a StPO ist überhaupt keine Schwelle gesetzt. Es ist daher anzunehmen, dass die Anforderung der schweren Straftat bei der vorliegenden Bestimmung nicht erfüllt ist und diese damit grundrechtswidrig ist, vom Verfassungsgerichtshof wurde sie aber noch nicht geprüft.[44]
Diese Befugnisse zur Anlassdatenspeicherung können potenziell zu einer Vorratsdatenspeicherung durch die Hintertüre[45] führen, da sie keine (z.B. örtlichen oder zeitlichen) Schranken zur Überwachung bieten. Die Anwendung der Anlassdatenspeicherung hält sich bislang in Grenzen – sie wurde seit ihrer Einführung bis zum 30.06.2019 drei Mal durchgeführt – die zugrundeliegenden Delikte (bzw. der Verdacht) bezogen sich dabei in einem Fall auf beharrliche Verfolgung, in einem auf Diebstahl und in einem weiteren auf schweren Diebstahl.[46]

7.6 Haftung und Herausgabepflichten von Host-Providern

Im E-Commerce-Gesetz (ECG), das auf der EU-Richtlinie über den elektronischen Geschäftsverkehr beruht, wird im Wesentlichen der elektronische (Online-)Geschäftsverkehr geregelt. Es regelt die Zulassung von Anbieter_innen, den Abschluss von Verträgen, Verantwortlichkeiten und nicht zuletzt auch Lösch- und Herausgabeverpflichtungen von Daten.[47]

7.6.1 Host-Provider-Privileg

Die Lösch- und Herausgabeverpflichtungen sind auch im Zuge einer Überwachungsgesamtrechnung interessant. Prinzipiell müssen nämlich Host-Provider, also Provider, die von Nutzer_innen eingegebene Informationen speichern und diese, im Gegensatz zu Access-Provider, nicht bloß „durchleiten"[48], für diese Inhalte haften. Darunter fallen auch „Medienunternehmen, [die] Kommentare und ‚Leserbriefe' von Nutzern zu bestimmten Nachrichten oder Artikeln online publizier[en]"[49]. § 16 ECG normiert aber als Ausnahme dazu das sogenannte Host-Provider-Privileg. Dadurch sind Host-Provider von der Haftung befreit, sofern sie über die rechtswidrigen Inhalte von Posts keine tatsächliche Kenntnis hatten, bzw. auch nicht aus den Umständen dies für sie offensichtlich sein musste, oder wenn sie unverzüglich nach der Kenntnisnahme den Inhalt löschen oder den Zugang dazu sperren.
Dieses Privileg geht relativ weit, zumal dadurch normiert wird, dass keine Prüfpflicht auf Seiten der Host-Provider bestehen darf. Dennoch können Provider Mechanismen einsetzen, um die Speicherung von rechtswidrigen Inhalten schon von vornherein zu verhindern.

§ 18 ECG, Art. 15 E-Commerce-RL

7.6.2 Herausgabepflichten von Host-Providern

§ 18 ECG regelt die Herausgabeverpflichtungen von Host-Providern. Damit wird geregelt, wie Provider mit den personenbezogenen Daten der Personen umgehen sollen, die hinter verdächtigen Inhalten stehen. Sie müssen jedenfalls deshalb nicht die gespeicherten Inhalte auf ihre Rechtskonformität hin überwachen, wie schon zu § 16 ECG ausgeführt. Das verbietet nämlich auch Art. 15 Abs. 1 der E-Commerce-Richtline, auf der das ECG aufbaut.

Es besteht aber sehr wohl die Pflicht, inländischen Gerichten und Verwaltungsbehörden alle Informationen zu übermitteln, durch die bestimmte Nutzer_innen identifiziert werden können, wenn dies notwendig ist, um strafbare Handlungen zu verhindern, respektive zu verfolgen und aufzuklären. Außerdem müssen die Daten sogar an Privatpersonen herausgegeben werden, wenn diese erstens ein „überwiegendes rechtliches Interesse" an der Identität des_der Nutzer_in im Zusammenhang mit einer rechtswidrigen Handlung haben und zweitens diese Privatpersonen auch glaubhaft machen können, dass diese Information notwendig ist, um ihr Recht gegen den_die andere_n User_in durchsetzen zu können. Die Privatpersonen müssen dafür also zunächst darstellen, dass ein „rechtswidriger Sachverhalt", also eine Rechtsverletzung, wie zum Beispiel eine (strafrechtlich relevante) Beleidigung, vorliegt, und sie müssen „glaubhaft machen", dass sie durch den Host-Provider an diese Daten kommen können.[50]
Daneben besteht die Möglichkeit für Diensteanbieter_innen, die ein Medium betreiben (also Medienunternehmer_innen oder Mediendienste im Sinne des Mediengesetzes sind), sich auf das Redaktionsgeheimnis zu berufen. Dazu gibt es eine detailreiche Rechtsprechung. Für Forenbeiträge wird das Redaktionsgeheimnis von den Gerichten aber nur in seltenen Fällen anerkannt. Die einzelnen Poster_innen können weder die Herausgabe ihrer eigenen Daten unter Berufung auf das Redaktionsgeheimnis verhindern, noch sind sie selbst in Bezug auch etwaige Quellen, die sie selbst für ihr Posting nutzen, berechtigt, sich darauf zu berufen. Sehr wohl aber können sich Medieninhaber_innen und -mitarbeiter_innen darauf berufen, wenn es um die persönlichen Daten von registrierten Online-Poster_innen geht. Berufen diese sich aber nicht darauf, hat der_die Poster_in kein Recht darauf, dies einzufordern.[51]
Allerdings gibt es noch eine weitere Einschränkung: Wo es keinen Zusammenhang mit der journalistischen Tätigkeit gibt, gilt auch das Redaktionsgeheimnis nicht. Es muss also wenigstens irgendeine Art von Kontrolle oder Kenntnisnahme eine_r Medienmitarbeiter_in geben, damit das Redaktionsgeheimnis wirkt.[52] Dies muss aber auch tatsächlich ein_e Mitarbeiter_in sein und kann nicht bloß durch ein Computerprogramm passieren, damit das Kriterium erfüllt ist.[53]
Diese Fragen stellen sich aber gar nicht erst, wenn der_die Medienunternehmer_in gar keine Daten der User gespeichert hat. Er_sie ist nach aktueller Rechtslage auch nicht dazu verpflichtet diese zu ermitteln und macht sich somit auch nicht strafbar.[54] Selbst wenn noch mehr Daten gespeichert wurden, dürfen dennoch nur Name und Adresse herausverlangt werden, auf weitergehende Informationen hat der_die Auskunftswerber_in keinerlei Anspruch.[55]
Tatsächlich sind aber auch im Bereich des § 18 ECG hier relativ weitreichende Möglichkeiten vorhanden, für Gerichte und Verwaltungsbehörden, personenbezogene Daten von Usern zu erhalten. Selbst Dritte können die Daten erhalten, wenn sie nur einen Verdacht glaubhaft machen und ebenso, dass sie die Daten für die Rechtsverfolgung benötigen. Auch das Redaktionsgeheimnis ist, wie dargestellt, nur in Ausnahmefällen ein Schutz vor der Herausgabepflicht.

Redaktionsgeheimnis § 31 MedienG

7.7 IMSI-Catcher

Durch einen IMSI-Catcher wird eine Funkzelle fingiert, in die sich die umliegenden Mobiltelefone einwählen. So kann festgestellt werden, welche Geräte – die anhand ihrer SIM-Kartennummer (IMSI) – identifiziert werden, sich im Umkreis befinden. Eine solche Standortbestimmung ist sowohl nach dem SPG als auch nach der StPO zulässig. Da alle Personen im Umkreis vom Einsatz dieser Maßnahme betroffen sind, auch wenn sie mit dem Grund für ihren Einsatz nichts zu tun haben, hat sie eine hohe Streubreite. Durch diese Maßnahme können aber mitunter auch Funkverbindungen unterbrochen werden, was ebenfalls unbeteiligte Dritte betrifft, die sich zufällig in der Nähe des IMSI-Catchers aufhalten. Die mobilen Endgeräte dieser Personen werden also daran gehindert, sich ins Netz einzubuchen, was einen Eingriff in eine Vielzahl an

IMSI-Catcher

Grundrechten zur Folge haben kann. Ein eindrückliches Beispiel für einen Eingriff in das Recht auf Leben wäre ein Fall, in der in einer lebensbedrohlichen Situation ein Notruf nicht mehr möglich ist, weil ein IMSI-Catcher den Mobilfunkverkehr verhindert.

Standortbestimmung nach dem SPG

§ 53 Abs. 3b SPG

Nach dem SPG kann ein IMSI-Catcher eingesetzt werden, wenn eine gegenwärtige Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen besteht und wenn sein Einsatz der Hilfestellung bzw. der Gefahrenabwehr dient. Ein Einsatzfall kann z.B. die Suche nach vermissten oder von Lawinen verschütteten Personen sein – zumindest wurden diese Szenarien bei der Einführung der Norm mit der SPG Novelle 2007 rechtspolitisch prominent argumentiert.

Standortbestimmung nach der StPO

§§ 135 Abs. 2a, 134 Z 2a StPO

Die Befugnis der Standortbestimmung wurde in der StPO erst mit dem Überwachungspaket eingeführt und ist seit 01.06.2018 in Kraft. 2018 wurde sie 72 Mal angewendet, woraus 2 Anklagen und 3 Verurteilungen resultierten.[56] 2019 wurde sie schon im ersten Halbjahr 92 Mal eingesetzt. Davon kam es zu vier Anklagen und keiner Verurteilung.[57] Bei der Einführung berichtete der damals amtierende Justizminister Moser, dass diese Befugnis schon vor der ausdrücklichen gesetzlichen Regelung eingesetzt wurde.[58] Mittels Standortbestimmung dürfen nur Standortdaten und Gerätenummern ermittelt werden, nicht aber Inhaltsdaten. Diese explizite gesetzliche Regelung ist deswegen bedeutsam, weil IMSI-Catcher aus technischer Sicht auch Inhaltsdaten erfassen können,[59] also mehr können als sie dürfen. Um die Verhältnismäßigkeit zu wahren, muss abgewogen werden, über welchen Zeitraum die Überwachungsmaßnahme eingesetzt wird und wie Unbeteiligte davon betroffen sein werden.[60] Es ist keine gerichtliche Bewilligung notwendig, die Maßnahme kann auf Anordnung der Staatsanwaltschaft erfolgen.

§ 137 Abs. 1 StPO

Diese Befugnis kann in folgenden Fällen eingesetzt werden:

- Es besteht ein dringender Verdacht, dass eine Person eine andere entführt hat oder sich „sonst ihrer bemächtigt hat“

  UND

- die Auskunft beschränkt sich auf Daten einer Nachricht, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung von dem_der Beschuldigten übermittelt, empfangen oder gesendet wird;

ODER

- Erwartungsgemäß kann dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einem Jahr Freiheitsstrafe bedroht ist, gefördert werden

  UND

- auf Grund bestimmter Tatsachen ist anzunehmen, dass dadurch die Daten des_der Beschuldigten ermittelt werden können;

ODER

- Auf Grund bestimmter Tatsachen ist anzunehmen, dass dadurch der Aufenthalt eine_r flüchtigen oder abwesenden Beschuldigten, der_die einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.

Endnoten

1 Vgl. *Reindl-Krauskopf/Tipold* in *Fuchs/Ratz* (Hrsg.), WK-StPO (2016) § 134, Rz 43f.
2 Ausgenommen die Tatbestände nach den §§ 278, 278a und 278b StGB, vgl. die Legaldefinition in § 16 SPG. Diese Tatbestände fallen in den Bereich des PStSG.
3 Siehe dazu *Reindl-Krauskopf/Tipold* in *Fuchs/Ratz* (Hrsg.), WK-StPO (2016) § 134, Rz 37; OGH in 15 Os 172/10y, 2011.
4 Vgl. *Tschohl* in *Jaksch-Ratajczak/Stadler*, Aktuelle Rechtsfragen der Internetnutzung, Band 2, Die Anonymität im Internet – Umsetzung der Vorratsdaten-RL im österreichischen Telekom-, Strafprozess- und Sicherheitspolizeirecht, 341; Vgl. auch *Edthaler/Schmid*, Auskunft über IP-Adressen im Strafverfahren, MR 2008, 220; *Schanda*, Auskunftspflicht über Inhaber dynamischer IP-Adressen contra Verpflichtung zur Löschung von Verkehrsdaten, MR 2007, 213; Vgl. auch *Hasberger*, Die providerinterne Auswertung von Verkehrsdaten und Datenschutz, MR 2010, 23.
5 Vgl. dazu die Erläuterungen zur Regierungsvorlage 1074 d. B. XXIV. GP, zu § 90 Abs. 7 TKG sowie zu § 92 Abs. 3 Z 16 TKG. (http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/fname_206854.pdf)
6 Mit weiteren Nachweisen *Tschohl*, in *Jaksch-Ratajczak/Stadler*, Aktuelle Rechtsfragen der Internetnutzung, Band 2, Die Anonymität im Internet – Umsetzung der Vorratsdaten-RL im österreichischen Telekom-, Strafprozess- und Sicherheitspolizeirecht, 341 (355f).
7 Erläuterungen zur Regierungsvorlage, 1074 d. B. XXIV. GP, 12f.
8 *Kassai/Raschauer*, 11. Abschnitt. Aufsichtsrechte, in *Riesz/Schilchegger* (Hrsg.), Telekommunikationsgesetz. Kommentar (2016), § 90 Rz 55.
9 Erläuterungen zur Regierungsvorlage 1074 d. B. XXIV. GP, 12f.
10 Siehe auch *Reindl-Krauskopf; Tipold/Zerbes* in *Fuchs/Ratz* (Hrsg.), WK StPO (2016) § 134, Rz 21.
11 Vgl. Ebd. § 135, Rz 24.
12 Ebd. Rz 29.
13 Vgl. Ebd. Rz 33.
14 Ebd. Rz 36.
15 OGH RS 0107304.
16 Zum Begriff des Herstellens einer Verbindung bestehen divergierende Ansichten, siehe hierzu: *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz* (Hrsg.), WK-StPO (2016) § 135, Rz 40; OGH in 12 Os 152/00.
17 Vgl. *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz*, WK-StPO (2016) § 135, Rz 43.
18 Vgl. Ebd. Rz 46.
19 Vgl. Ebd. Rz 51.
20 Vgl. Ebd. Rz 52.
21 Vgl. *Adensamer/Steinhauser*, Nie mehr allein… Überwachungsbericht 2017, 10; Bundesministerium für Inneres, Anfragebeantwortung AB/136, XXVI. GP vom 16.03.2018 zur Anfrage J/131, XXVI. GP vom 17.01.2018; *Bundesministerium für Inneres*, Anfragebeantwortung AB/2609, XXVI. GP vom 15.03.2019 zur Anfrage J/2625, XXVI. GP vom 16.01.2019; *Bundesministerium für Inneres*, Anfragebeantwortung AB/3918, XXVI. GP vom 04.09.2019 zur Anfrage J/3899, XXVI. GP vom 09.07.2019.
22 Vgl. *Bundesministerium für Inneres*, Anfragebeantwortung AB/3918, XXVI. GP vom 04.09.2019 zur Anfrage J/3899, XXVI. GP vom 09.07.2019, https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_03918/index.shtml (18.12.2018).
23 Vgl. dazu auch *Adensamer/Steinhauser*, Nie mehr allein… Überwachungsbericht 2017 (2018), 10.
24 Siehe *ISPA*, Beauskunftung-Übersicht, https://www.ispa.at/wissenspool/positionspapiere/beauskunftung.html (18.12.2019).
25 Vgl. *Heißl*, PStSG (2016) § 1, Rz 34.
26 Vgl. *Reindl-Krauskopf; Tipold/Zerbes* in *Fuchs/Ratz* (Hrsg.), WK-StPO (2016) § 135, Rz 61.
27 Vgl. ebd.
28 Vgl. Ebd. Rz 56.
29 *Bundesministerium für Verfassung, Deregulierung, Reformen und Justiz*, Wahrnehmungsbericht, 11. November 2019, https://www.justiz.gv.at/file/2c94848b6d50e800016e6a285abf00ed.de.0/wahrnehmungsbericht_hbm%20jabloner.pdf, 33.
30 *Heißl*, Überwachungen und Ermittlungen im Internet. Sicherheitspolizei, Militärische Nachrichtendienste, Kriminalpolizei (2017) 10ff.

31 Vgl. *Bundesministerium für Inneres*, Anfragebeantwortung AB/3918, XXVI. GP vom 04.09.2019 zur Anfrage J/3899, XXVI. GP vom 09.07.2019, Beilage zu Frage 1, (https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_03918/index.shtml (20.12.2019).
32 Vgl. Ebd. Beilage zu den Fragen 2–6.
33 Vgl. *Bundesministerium für Inneres*, Anfragebeantwortung AB/2609, XXVI. GP vom 15.03.2019 zur Anfrage J/2625, XXVI. GP vom 16.01.2019, Anlage zu Frage 1 und Anlage zu den Fragen 2–6, https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_02609/index.shtml (20.12.2019).
34 Vgl. *Bundesministerium für Inneres*, Anfragebeantwortung AB/136, XXVI. GP vom 16.03.2018 zur Anfrage J/131, XXVI. GP vom 17.01.2018, Anlage zu Fragen 1, 10, 23, 32 und Anlage zu Fragen 2–6, 11–15, 24–28, 33–37, https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_00136/index.shtml (20.12.2019)
35 Vgl. *Heißl*, PStSG (2016) § 11, Rz 89.
36 Vgl. Ebd. Rz 90.
37 Vgl. Ebd. Rz 98.
38 Vgl. Ebd. Rz 116.
39 Vgl. Ebd. Rz 140.
40 Siehe etwa: *Wirtschaftskammer Österreich,* Stellungnahme 14 zu ME/110 XXV. GP, 2f. (https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_03650/imfname_410972.pdf)
41 Vgl. Erläuterungen zum Ministerialentwurf ME/325 XXV. GP Erläuterungen, 7f., https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00325/index.shtml (21.12.2019).
42 Vgl. *epicenter.works*, Stellungnahme zum Strafprozessrechtsänderungsgesetz 2018 zu 17 d. B. XXVI. GP, 18.
43 Vgl. EuGH 8.4.2014, C-293/12, Digital Rights Ireland, Rz 60, http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=202022 (20.12.2019); EuGH 21.12.2016, C-203/15 Tele2 Sverige, Rz 102.
44 Vgl. *epicenter.works*, Stellungnahme zum Strafprozessrechtsänderungsgesetz 2018 zu 17 d. B. XXVI. GP, 19.
45 Vgl. ebd. 2ff.
46 Zu 2019: *Bundesministerium für Inneres,* Anfragebeantwortung AB/3918, XXVI. GP vom 04.09.2019 zur Anfrage J/3899, XXVI. GP vom 09.07.2019;
zu 2018: *Bundesministerium für Inneres*, Anfragebeantwortung AB/2609, XXVI. GP vom 15.03.2019 zur Anfrage J/2625, XXVI. GP vom 16.01.2019.
47 Vgl. § 1ff ECG BGBl I Nr. 152/2001 idF BGBl I Nr. 34/2015.
48 Vgl. Beilagen zur Regierungsvorlage 817 d. B. XXI. GP, 35.
49 Ebd.
50 Erläuterungen zur Regierungsvorlage 817 d. B. XXI. GP, 39. (https://www.parlament.gv.at/PAKT/VHG/XXI/I/I_00817/index.shtml, 21.12.2019)
51 Vgl. *Windhager/Gahleitner,* Redaktionsgeheimnis 2.0 – Sind Userdaten von § 31 MedienG geschützt. Medien und Recht 3/2013, 107–110.
52 OGH 23.01.2014 6 Ob 133/13x.
53 OGH 15.12.2014 6Ob188/14m.
54 OGH 10.04.2014 6 Ob 58/14v.
55 OGH 14.09.2001 6 Ob 104/11d.
56 Vgl. *Bundesministerium für Inneres,* Anfragebeantwortung AB/2609, XXVI. GP vom 15.03.2019 zur Anfrage J/2625, XXVI. GP vom 16.01.2019.
57 Vgl. *Bundesministerium für Inneres*, Anfragebeantwortung AB/3918, XXVI. GP vom 04.09.2019 zur Anfrage J/3899, XXVI. GP vom 09.07.2019.
58 Vgl. *Moser*, Vortrag an den Ministerrat vom 21.02.2018. (https://www.bundeskanzleramt.gv.at/dam/jcr:35b2c907-c7d5-44e0-a61d-68d28d330765/8_16_mrv.pdf)
59 Vgl. *epicenter.works*, Stellungnahme zur Regierungsvorlage 17 d. B. XXVI. GP, 6. (https://epicenter.works/sites/default/files/epicenter.works_-_strafprozessaenderungsg_2018_17_xxvi_gp-web_0.pdf)
60 OGH, 12 Os93/14i.

8 Umstrittene Befugnisse

In den vorherigen drei Kapitel haben wir drei Überwachungsbefugnisse mit besonderer Bedeutung genauer vorgestellt. Während auch diese in Teilbereichen überschießend und unverhältnismäßig sind – sei in der gesetzlichen Regelung oder im Einsatz – geht es nun um besonders umstrittene Befugnisse. Teils sind diese vom Verfassungsgerichtshof (VfGH) aufgehoben worden, wie der Bundestrojaner und die Kfz-Überwachung und Zugriff auf Section Control, teils sind sie in Kraft, wie die Rasterfahndung und die Fluggastdatenverarbeitung, wobei gegen letzte schon Beschwerden laufen (Stand 01.01.2020).

8.1 Bundestrojaner

Bundestrojaner

Für den Bundestrojaner sind unterschiedlichste Bezeichnungen im Umlauf, vom juristischen Begriff „Überwachung verschlüsselter Nachrichten“, über „Quellen-Telekommunikationsüberwachung“ (Quellen-TKÜ), „Staatstrojaner“, „staatliche Schadsoftware“ und „staatliche Spionagesoftware“ bis zu „Government Hacking“. Alle diese Bezeichnungen nehmen Bezug auf die Funktionsweise dieser Ermittlungsmethode. Relevant wurde diese Art der Überwachung, weil weltweit Kommunikation mittels Ende-zu-Ende-Verschlüsselung zunahm. Große Messengerdienste (wie WhatsApp, Telegram, Signal), welche mittlerweile häufig standardmäßig eine Ende-zu-Ende-Verschlüsselung anbieten, lösen zunehmend herkömmliche SMS ab. Die aktuelle Art der Verschlüsselung gilt bis jetzt als weitgehend undurchdringbar.[1] Sicherheitsbehörden könnten mit der herkömmlichen Nachrichtenüberwachung zwar eine verschlüsselte Nachricht auslesen, diese aber nicht entschlüsseln. Um den Inhalt der Nachricht zu erfahren, muss vor oder nach der Ver- bzw. Entschlüsselung angesetzt werden. Zu diesem Zweck wird heimlich, üblicherweise unter Ausnutzung von IT-Sicherheitslücken, ein Programm auf ein Computersystem (bspw. Smartphone, Laptop oder Smart-Home-Gerät) gespielt, welches die Informationen an die Sicherheitsbehörden weiterleitet. Praktisch wird oft ein *Keylogger* eingesetzt, ebenso wie eine Anwendung, die in regelmäßigen Abständen Screenshots anfertigt und ausleitet.[2]

Ende-zu-Ende Verschlüsselung

Keylogger

Geschichte der Befugnis

WannaCry

Weltweit haben Staaten ein zunehmendes Interesse daran, eine derartige Maßnahme einzusetzen, da Nachrichten vermehrt verschlüsselt verschickt werden. Daher haben in den letzten Jahren zahlreiche Staaten diese Befugnis eingeführt. Auch US-Behörden nutzen diese Art der Informationsgewinnung. Bis 2017 nutzte die NSA dafür die Sicherheitslücke *EternalBlue* im Windowssystem. Obwohl diese Sicherheitslücke den staatlichen Behörden also bekannt war, wurde sie Microsoft nicht mitgeteilt und somit bewusst offengehalten.[3] Ebendiese Lücke wurde schließlich im Jahr 2017 für Cyberangriffe ausgenutzt. Tausende Computerprogramme wurden mit Ransomware (Schadprogramm, das Computersysteme sperren oder Dateien verschlüsseln kann) wie *WannaCry*[4] und *Petya*[5] infiziert. Dateien auf den betroffenen Computersystemen wurden verschlüsselt und nur gegen Zahlung von Lösegeld wieder freigegeben. Betroffene waren unter anderem Universitäten, eine spanische Telefongesellschaft, das russische Innenministerium, globale Unternehmen und Spitäler. Wie weitreichend die konkreten Auswirkungen sind, ist schwer einzuschätzen.

In England wurden beispielsweise 139 als dringend eingestufte medizinische Termine verschoben.[6]

Trotz dieser verheerenden Geschehnisse wird diese Befugnis in vielen Ländern legalisiert, beispielsweise in Deutschland (§ 100b deutsche StPO[7]). Es wurde 2016[8] und 2017[9] versucht, den Bundestrojaner in Österreich auf eine gesetzliche Grundlage zu stellen, die Regierung scheiterte damit jedoch zwei Mal politisch. Schließlich wurde die Bundestrojaner-Regelung in Umsetzung der EU-Antiterror-Richtlinie[10] im April 2018 eingeführt, obwohl diese Maßnahme nicht explizit in der Richtlinie vorgesehen ist. Auf Antrag jeweils eines Drittels der Abgeordneten des Nationalrats sowie des Bundesrats wurden die Bestimmungen schließlich im Dezember 2019 vom VfGH wieder aufgehoben. Als Begründung führte der VfGH an, dass die Befugnis nur zur Bekämpfung schwerer Straftaten zulässig sein darf, was nicht gegeben war, dass auch nicht verdächtige Personen betroffen waren (Streubreite), dass der Rechtsschutz nicht ausreichend ausgestaltet war und, dass geheime Hausdurchsuchungen zur Installation grundrechtswidrig sind. Aufgrund der hohen Eingriffsintensität und da die „vertrauliche Nutzung von Computersystemen und digitalen Nachrichtendiensten […] ein wesentlicher Bestandteil des Rechts auf Achtung des Privatlebens“[11] sind, sah der VfGH das Recht auf Achtung der Privatsphäre verletzt.

§ 516a Abs 9 StPO

Artikel 8 EMRK

➲ 9.2 Privatleben

Bemerkenswert ist, dass für den VfGH eine gerichtliche Bewilligung und Kontrolle durch den Rechtsschutzbeauftragten nicht ausreichte, um ein angemessenes Schutzniveau zu gewährleisten.[12] Es muss sichergestellt sein, dass die Durchführung der Maßnahme auch während ihres Einsatzes kontrolliert wird, und auch in Hinsicht auf technische und personelle Ressourcen eine effektive Kontrolle tatsächlich möglich ist.

Da die österreichische Verfassung das Legalitätsprinzip vorsieht – die Exekutive also nur auf Grundlage von Gesetzen agieren dürfte – erscheint es erstaunlich, dass die Maßnahme aber bereits zuvor eingesetzt wurde. Bei Ermittlungen gegen politische Aktivist_innen (bekannt als „Tierschützerprozess“) wurde die „Durchführung einer Internetüberwachung (Keylogging, Screenshotting, usw.)“[13] beantragt, um verschlüsselte E-Mails mitlesen zu können. Die Beschuldigten, alle wegen Verdacht auf Beteiligung an einer kriminellen Organisation angeklagt, wurden 2014 rechtskräftig freigesprochen. Ob die Maßnahme tatsächlich eingesetzt wurde, ist nicht bekannt.

Tierschützerprozess

§ 278a StGB alte Fassung

Der andere Fall betraf Mohamed M., der wegen Mitgliedschaft in einer terroristischen Vereinigung verurteilt wurde. Gegen ihn wurde eine Quellen-TKÜ jedenfalls eingesetzt:

> „Ab dem 29. Juli [2007] wird zudem mit einem großen Lausch- und Spähangriff gegen den Verdächtigen vorgegangen. Zu diesem Zweck dringt die Sondereinheit für Observation (SEO) in die Wohnung der Familie M. ein. […] Zunächst wird lediglich an einem der ganzen Familie zugänglichen Computer eine so genannte Angriffssoftware installiert, am 1. September dringt die SEO erneut in die Wohnung ein, um auch den Laptop von Mohamed M. zu manipulieren. Die installierte Angriffssoftware besteht aus zwei Programmen. Das eine übermittelt online und im Minutentakt einen Screenshot an die SEO. Aufgrund der durchgehenden Internetverbindung des Laptops ist diese Übermittlung lückenlos, die ErmittlerInnen erhalten so etwa auch die Möglichkeit, Einblicke in Textdokumente zu nehmen, die M. gerade bearbeitet. Beim zweiten Programm handelt es sich um eine Key-Log-Datenerfassung: Jeder Tastaturanschlag wird online der SEO übermittelt. Die angeführten Maßnahmen werden vom Untersuchungsrichter regelmäßig bewilligt, in Fällen, in denen es der Zustimmung eines Rechtsschutzbeauftragten bedarf, wird diese erteilt.“[14]

Dieses Szenario veranschaulicht gut, wie diese Maßnahme typischerweise funktioniert und wie intensiv in das Privatleben von verschiedensten Personen eingedrungen wird, in diesem Fall der ganzen Familie. Das Gericht entschied

schließlich, dass die Maßnahmen rechtmäßig waren, da es sich um eine optische Überwachung gehandelt hätte. Die Argumentation lautete, dass man auch eine Kamera hätte installieren können, die Bildschirm und Tastatur abfilmt.[15] Allerdings wurde kurz darauf im Zuge der großen Strafprozessreform 2008 die Rechtslage geändert, sodass Ermittlungsbefugnisse nach der StPO ausdrücklich geregelt sein müssen und nicht einfach analog angewendet werden dürfen. Dass – wie vielfach kritisiert – die Eingriffsintensität einer optischen Überwachung und die eines Bundestrojaners jedoch in keinster Weise miteinander vergleichbar sind, hat der VfGH endlich bestätigt.

§ 5 Abs. 1 StPO

Ausgewählte problematische Aspekte

Einige Gefahren dieser Befugnis liegen in ihrem Wesen selbst begründet und lassen sich daher nicht durch begleitende Kontrollbestimmungen oder durch hohe Zulassungsvoraussetzungen beseitigen. Diese Überwachungsbefugnis stellt einen besonders intensiven Eingriff in die Privatsphäre betroffener Personen dar. Es kann das gesamte Nutzungsverhalten einer Person, inklusive intimer Details, ausgelesen und über Jahre gespeichert werden.

Die Beweismittel, die lukriert werden, sind ungeeignet: Ein Computersystem, in dem ein solches Programm erfolgreich installiert werden konnte, ist grundsätzlich infiltrierbar. Ansonsten wäre es nicht möglich gewesen, das Programm zu installieren. Die Analyse einer „Staatstrojaner"-Software, die in Deutschland zum Einsatz kam, zeigte auch, dass die verwendete Programmarchitektur sogar weitere Angriffsszenarien für Dritte eröffnete.[16] Das bedeutet, dass es sowohl den Sicherheitsbehörden möglich ist, auf das System zuzugreifen und es zu manipulieren, als auch anderen Akteur_innen. Das wirft die Frage auf, welchen Wert die erlangten Beweismittel haben. Immerhin müsste die Unschuldsvermutung in den meisten Fällen dazu führen, dass die Beweise nicht der beschuldigten Person zugerechnet werden können, da nicht ausgeschlossen werden kann, dass die Beweise von dritter Seite platziert wurden oder auch eine andere Person physisch das Computersystem nutzte.[17] Damit ein Bundestrojaner auf einem Gerät installiert werden kann, muss dieses Gerät bzw. die darauf laufende Software Sicherheitslücken aufweisen. Der mittelbare oder unmittelbare Einkauf von Wissen über solche Sicherheitslücken am Schwarzmarkt bzw. „Grauen Markt" und dessen Finanzierung durch österreichische Steuergelder ist keinesfalls zu rechtfertigen und stattdessen abzulehnen.

Grauer Markt

Grundsätzlich könnten alle Arten von Computersystemen gehackt werden. Computersysteme sind bspw. Notebooks und Smartphones, aber mittlerweile auch PKWs, Kinderspielzeuge, Windeln (Tweet-Pee), Mülleimer[18], Glühbirnen, Alexa oder Kühlschränke. Computersysteme haben sehr unterschiedliche Aufgaben, werden sehr unterschiedlich verwendet und haben sehr unterschiedliche Bedeutungen für unser Leben. Zu manchen Geräten besteht eine engere emotionale Beziehung, weil soziale Interaktion über sie stattfindet und sie häufig nahe am Körper getragen werden. Andere Geräte erfüllen wichtige Aufgaben im Alltag oder ersetzen menschliche Fähigkeiten. All diese Geräte dürfen gehackt werden, wenn das Konzept Bundestrojaner in die Rechtsordnung Einzug hält. Dabei ist eine Beeinträchtigung dieser Computersysteme nie ausgeschlossen, was bei manchen Systemen sehr dramatische Auswirkungen haben kann: Wenn beispielsweise beim Versuch ein Fahrzeug zu hacken etwas schief geht, kann die Verkehrssicherheit – und damit Menschenleben – gefährdet werden. Passieren Fehler beim Hacken eines intelligenten Notrufsystems für alte oder beeinträchtigte Personen, kann dies ebenso deren Leben gefährden.

Internet of Things

Der Cyberangriff *WannaCry* zeigt deutlich, dass Staaten, wenn sie diese Art von Software einsetzen möchten, ein Interesse an der Aufrechterhaltung von IT-Sicherheitslücken haben und somit IT-Sicherheit erheblich schwächen. Computersysteme nehmen, gerade mit den Entwicklungen hin zu Smart Home, aber auch auf andere Weisen, einen immer wichtigeren Platz im menschlichen Leben ein. Dass Sicherheitslücken in diesen Systemen aufrechterhalten werden, kann unabsehbare Folgen für alle Menschen haben – nicht nur für jene, die direkt von dieser Überwachungsmaßnahme betroffen sind.

Sicherheitslücken

8.2 Fluggastdaten

PNR steht für Passenger Name Records, auf Deutsch Fluggastdaten. Dabei handelt es sich um Datensätze zu einer Person, die einen Flug unternimmt. Nach der EU-PNR-Richtlinie von 2016 muss jeder Mensch, der in die oder aus der EU fliegt, in einer Datenbank erfasst werden. In Österreich werden zusätzlich sogar Daten über Flüge innerhalb der EU erfasst. Neben den Daten zum Flug kann auch der Aufenthalt im Gastland (z.B. Hotel und Adresse) oder auch das Ausleihen eines Mietwagens festgehalten werden. Auch wie lange man in einem Land bleibt und wie man die Reise bezahlt hat (z.B. Kreditkartendaten) wird gespeichert. Alle diese Daten müssen von den Fluglinien zweimal an eine staatliche Stelle weitergeleitet werden: einmal vor dem Flug und einmal nach der Ankunft. Nach sechs Monaten werden die Daten de-personalisiert, das bedeutet aber nur, dass der Klarname gelöscht wird. Potentiell können sie aber auch dann immer noch auf eine bestimmte Person zurückgeführt werden, sie sind also nicht anonymisiert. Erst nach fünf Jahren werden sie gänzlich gelöscht.

RL (EU) 2016/681

§ 2 Abs. 5 PNR-G iVm PNR-Verordnung BGBl II 2018/208 idF 2019/237

§ 3 PNR-G

§ 6 Abs. 1 PNR-G

Diese Daten werden automatisiert und nach bestimmten „Kriterien" vom System algorithmisch gefiltert. Dies soll dazu dienen, einen Verdacht, der davor nicht bestanden hat, erst zu erzeugen. Auch ein Abgleich mit Fahndungsdaten und gezielte Abfragen sind möglich. Zugriff auf die Daten haben Sicherheitsbehörden, Zoll- und sogar militärische Behörden. Die Informationen können innerhalb der EU mit anderen Mitgliedsstaaten ausgetauscht werden.

§ 4 Abs. 1 PNR-G, Erwägungsgrund 7 PNR-Richtlinie

Die Datenverarbeitung obliegt der nationalen Fluggastdatenzentralstelle (Passenger Information Unit – PIU), bei der zum Stichtag am 03.06.2019 21 Mitarbeiterinnen und Mitarbeiter beschäftigt waren. Für das Jahr 2019 werden dafür Personalkosten in Höhe von 1.840.570 Euro erwartet, 2020 sollen es laut Innenministerium 1,87 Millionen Euro sein.[19] Es ist nicht ausgeschlossen, dass die Zahl der Beschäftigten noch weiter steigt, sobald alle Fluglinien in das System eingebunden sind. Im Jahr 2018 reisten 31,7 Millionen Menschen auf österreichischen Flughäfen.[20]

Diskriminierende Merkmale dürfen zwar nicht Teil der Kriterien sein, nach denen gesucht wird, Algorithmen verschleiern aber oftmals die Verwendung solcher sensiblen Merkmale, indem sie stattdessen auf Platzhaltern aufbauen, wie z.B., dass die Essensauswahl im Flugzeug als Platzhalter für die Religion gilt. Wenn die verwendeten Algorithmen nicht offengelegt werden, ist es außerdem unmöglich, sie zu überprüfen. Wenn Entscheidungen (z.B. über das Setzen von Überwachungsmaßnahmen) von Algorithmen getroffen werden, ist diese Intransparenz ein schwerwiegendes demokratiepolitisches und rechtsstaatliches Problem.

➲ *3. Überwachungstechnologien Algorithmen und Big Data*

Bei Datensätzen von enormer Größe, wie es bei den Fluggastdaten der Fall ist, kommt es auch bei hoher Treffsicherheit zu einer großen Zahl an falschen Treffern („false positives"). Daran führt mathematisch kein Weg vorbei, weil man in einem sehr großen Datenset nach etwas sucht, das sehr selten ist. Alle Treffer, die algorithmisch entstehen, müssen durch eine Person individuell überprüft werden. Dies soll z.B. durch einen Abgleich mit Daten aus anderen Datenbanken geschehen. Damit wird eine weitere Ermittlungshandlung gesetzt, die ausdrücklich auch Personen betrifft, gegen die kein begründeter Verdacht vorliegt, denn genau die sollen durch den Vorgang aussortiert werden. Man fängt also von hinten an: Alle werden überwacht, es gibt sehr viele Treffer und von diesen müssen noch mehr händisch aussortiert werden. Bereits bis zum 30. September 2019 wurden 23.877.277 Datensätze 11.900.000 betroffenen Personen verarbeitet,[21] und dies seit der Anbindung der ersten Fluglinie am 1. Februar 2019 bei noch nicht voll ausgebautem Betrieb.[22] Im selben Zeitraum gab es 190.541 Treffer, die jeweils von einer Person überprüft wurden. Nur 280 stellten sich nach der Überprüfung als valide heraus. Es sind also nur 0,15 % der Treffer korrekt. Die Effizienz dieser Ermittlungsmaßnahme ist also äußerst gering, was ihre Verhältnismäßigkeit in Zweifel stellt.

➲ *3.1 Größe der Datensets und Prävalenzfehler*

Die Speicherung von Fluggastdaten ist eine weitere Form der Vorratsdatenspeicherung, deren Grundrechtswidrigkeit bereits dreimal vom Europäischen Gerichtshof festgestellt wurde – zuletzt 2017, als entschieden wurde,

dass der Austausch von Fluggastdaten mit Kanada das Recht auf Achtung der Privatsphäre und das Grundrecht auf Datenschutz verletzt.[23] Die Verarbeitung und Speicherung erfolgen anlasslos und verdachtsunabhängig. Aus diesen Gründen sind Verfahren gegen die Fluggastdatenverarbeitung in Österreich[24], Deutschland[25] und Belgien anhängig.

8.3 Kfz-Überwachung und Zugriff auf Section Control

📖 *Sicherheitspaket 2018*

Das Überwachungspaket von 2018 beinhaltete mit der Kfz-Überwachung und dem Zugriff auf Daten aus der Section Control zwei Überwachungsmaßnahmen, die schon bei ihrer Einführung stark umstritten waren und im Dezember 2019 vom VfGH wegen ihrer Grundrechtswidrigkeit schließlich wieder aufgehoben wurden.

➲ *Datenschutz 9.2.3, 9.2.4*

Die Kfz-Überwachung sah vor, dass die Polizei verdeckt zu Zwecken der Fahndung Bildaufnahmen von Kfz machen konnte, die der Identifizierung der Kennzeichen, der Type, Marke und Farbe des Fahrzeuges sowie der Lenker_innen dienen[26] sollten. Da dies verdeckt erfolgte, konnten die Betroffenen außerdem nicht davon wissen und hatten keine Möglichkeit, die Rechtmäßigkeit des Einsatzes zu überprüfen. Die Daten durften bis zu zwei Wochen gespeichert werden – ohne konkreten Anlass, sondern für mögliche spätere Fahndungen[27].

Es war also eine Vorratsdatenspeicherung vorgesehen, wie sie der EuGH schon öfters für grundrechtswidrig erklärt hatte. Insbesondere die Erfordernis, dass eine Vorratsdatenspeicherung nur dazu dienen kann, schwere Verbrechen zu verfolgen, war hier nicht gegeben. So sah es schließlich auch der VfGH: „Es werden damit Daten fast ausschließlich von Personen erfasst, die keinerlei Anlass – in dem Sinne, dass sie ein Verhalten gesetzt hätten, das ein staatliches Einschreiten erfordern würde – für die Datenerfassung gegeben haben. Durch eine solche verdeckte, automatische Datenerfassung von Fahrzeugen und Fahrzeuglenkern kann in großen Teilen der Bevölkerung das „Gefühl der Überwachung“ entstehen. Dieses Gefühl der Überwachung kann wiederum Rückwirkungen auf die freie Ausübung anderer Grundrechte – etwa der Versammlungs- oder Meinungsäußerungsfreiheit – haben.“[28] Somit hat hier der VfGH erstmals ausdrücklich das Problem des chilling effect anerkannt.

➲ *9.4 Versammlungsfreiheit*
➲ *Chilling effect 9.3*

Die Section Control (oder auch Abschnittskontrolle[29]) dient der Geschwindigkeitsmessung: es werden mit bestimmten Abständen Aufnahmen von Kfz gemacht und aus dem Vergleich der Kennzeichen abgeleitet, ob jemand zu schnell gefahren ist. Nur wenn dies der Fall ist, werden die Daten verschlüsselt an die Behörde weitergeleitet, ansonsten werden keine Daten gespeichert. Die Messstrecken werden per Verordnung festgelegt. Heute (Stand 18.12.2019) gibt es davon in Österreich 30.[30] Im Zuge des Überwachungspakets bekam die Polizei Zugriff auf die so ermittelten Daten zu Zwecken der „Strafrechtspflege“ ohne Eingrenzung auf die Verfolgung bestimmter schwerer Delikte. Vom Innenministerium wurden drei Punkte mit besonderer Fahndungsrelevanz identifiziert, wo diese neue Befugnis eingesetzt werden sollte: auf der A2 am Wechsel, im Ehrentalerbergtunnel und auf der A7 im Tunnel Bindermichl.[31] Pilotversuche waren aber aufgrund der technischen Gegebenheiten der bestehenden Systeme ebenso wenig möglich wie eine konkrete Einschätzung über die zu erwartenden Kosten.[32] Die ASFINAG, die diese Anlage betreibt, schrieb in der Gesetzesbegutachtung, ein Zugriff auf ihre Videosysteme und eine Speicherverpflichtung, die über das hinausgehe, was im Moment technisch möglich ist, könnte Kosten im zweistelligen Millionenbereich bedeuten.[33]

§ 98f Abs. 3 StVO

Schon 2007 hatte der VfGH über die Verwendung der Daten aus der Section Control entschieden.[34] In dieser Entscheidung betonte er unter anderem die strenge Zweckbindung im Datenschutzrecht, nach der Daten nur für den Zweck verwendet werden dürfen, zu dem sie erhoben wurden, nicht aber z.B. Daten, die zur Feststellung der Geschwindigkeit erhoben wurden, zur Verfolgung von Straftaten. Auf diese Entscheidung nahm der VfGH auch 2019 wieder Bezug und hob diese Überwachungsbefugnis auf, weil sie eine Verletzung des Grundrechts auf Achtung der Privatsphäre darstellte. Begründet wurde die Entscheidung mit der Betroffenheit einer Vielzahl an Menschen, die kein verdächtiges Verhalten gesetzt hatten und einer fehlenden Einschränkung auf die Verfolgung nur schwerer Straftaten.[35] Die Verwendung von Daten aus der Section Control für polizeiliche Zwecke ist beispielhaft für die grundrechtswidrige Ausweitung der Überwachungsbefugnisse in Form von anlassloser Massenüberwachung, die in den letzten Jahren häufig politisch vorangetrieben wurde.

Art. 8 EMRK

8.4 Rasterfahndung

Die Rasterfahndung ist ein automationsunterstützter Abgleich personenbezogener Daten. So können Datenbanken nach kennzeichnenden oder ausschließenden Merkmalen Verdächtiger durchsucht werden oder auch verschiedene Datenbanken auf solche Merkmale verglichen werden und Schnittmengen gebildet werden. Gerade in Zeiten von Big Data kann dieser Befugnis große Bedeutung zukommen. Im Bereich der Sicherheitspolizei und des Verfassungsschutzes ist die Rasterfahndung unzulässig. Schon in den Erläuterungen zur Einführung heißt es, die Rasterfahndung solle nur zur Aufklärung eines bereits begangenen Verbrechens eingesetzt werden, nicht allerdings präventiv.[36]

§ 141 StPO

📖 *Rasterfahndung*
➲ *3.Überwachungstechnologien*

Die „kleine Rasterfahndung“ erlaubt den Datenabgleich von Daten, die die Gerichte, Staatsanwaltschaften und Sicherheitsbehörden schon verarbeiten, wenn die Aufklärung eines Verbrechens[37] ansonsten wesentlich erschwert wäre. Bei einer „großen Rasterfahndung“ ist auch der Abgleich mit Daten von Personen möglich, die von bestimmten Unternehmen bestimmte Waren oder Dienstleistungen bezogen haben, oder die Mitglieder von Vereinigungen, Gesellschaften, Vereinen o.ä. sind. Dies ermöglicht laut Heißl also die Suche auf Plattformen, die eine Registrierung verlangen, wie Facebook oder Parship, nicht aber das Verwenden einer Suchmaschine.[38]

§ 141 Abs. 2 StPO (klein) und § 141 Abs. 3 StPO (groß)

Besonders sensible Kategorien dürfen in die Rasterfahndung nicht einbezogen werden. Ausnahmen sind u.a. die Staatsangehörigkeit, und andere rechtmäßig erhobene Daten wie DNA im Rahmen einer kleinen Rasterfahndung. Eine Rasterfahndung muss vom Gericht bewilligt und von der Staatsanwaltschaft angeordnet werden. Die Merkmale, nach denen gesucht wird, die Datenbanken und die zur Datenübermittlung Verpflichteten müssen schon in der Bewilligung genau bestimmt sein.

§ 141 Abs. 4 StPO

§ 142 Abs. 1 StPO

Die Rasterfahndung wurde 1997 gegen die Proteste der Grünen, des Liberalen Forums und der FPÖ eingeführt.[39] Bei der Einführung waren die Rasterfahndung und andere zugleich eingeführte Bestimmungen bis 31.12.2001 befristet (sogenannte „sunset clause“),[40] um die „Notwendigkeit ihrer Bewährung unter den Gesichtspunkten der Effizienz und Verhältnismäßigkeit“ hervorzuheben.[41] Obwohl sie bis 2014 kein einziges Mal eingesetzt wurde,[42] wurde die Befugnis beibehalten. Über den Einsatz der Rasterfahndung wird jährlich im Bericht über den Einsatz besonderer Ermittlungsmaßnahmen des Justizministeriums berichtet. In den Berichten von 2014 und 2015 wird über einen Fall berichtet[43], in dem 50 Personen ausgeforscht wurden, allerdings keine Ermittlungsergebnisse erzielt wurden.[44] 2017 und 2018 wurde laut den Berichten des Justizministeriums keine Rasterfahndung durchgeführt. In Anbetracht dessen steht die Effizienz und Notwendigkeit dieser Maßnahme stark in Zweifel.

➲ *2.2 Der große Lauschangriff 1997*

Bericht des Justizministeriums
➲ *4.6 Bericht über die Quellenlage*

8.5 Beschlagnahme von Briefen

Die Beschlagnahme von Briefen ist „das Öffnen und Zurückbehalten von Telegrammen, Briefen oder anderen Sendungen, die der Beschuldigte abschickt oder die an ihn gerichtet werden“. Die Befugnis befähigt also die Strafverfolgungsbehörden, Briefe, aber auch Postkarten oder Pakete, im Wesentlichen also sämtliche Gegenstände, die sich auf dem Postweg befinden, zu beschlagnahmen. Nach dieser Bestimmung können Sendungen jedoch nicht beschlag-

§§ 135 Abs. 1 iVm 134 Z 1 StPO
§ 134 Z 1 StPO BGBl 2004/19 idF BGBl I 2018/27

nahmt werden, wenn sie sich noch bei dem_der Absender_in, einer anderen Person oder Empfänger_in befinden.[45] Relevant ist, dass die beschuldigte Person als Adressatin bezeichnet ist. Die Vermutung, dass eine beschuldigte Person einen Brief erhalten soll, obwohl ein_e andere_r Empfänger_in darauf steht, reicht nicht aus.[46]

§ 134 Z 1 iVm § 135 Abs. 1 StPO

Der Zeitraum, in dem eine Sendung beschlagnahmt werden kann, reicht von dem Zeitpunkt, in dem ein Brief in einen Postkasten eingeworfen oder in einer Postfiliale (oder bei einem privaten Boten- oder Expressdienst) aufgegeben wird, bis zu dem Zeitpunkt, in dem der Brief in einen Hausbriefkasten eingeworfen, in einem Postfach abgelegt oder dem_der Empfänger_in übergeben wird.[47] Die Transportunternehmen sind verpflichtet, Briefe abzufangen, die an Beschuldigte gerichtet sind, eine bundesweite Nachforschungspflicht kann diesen Beförderungsanstalten aber bei von Beschuldigten aufgegebenen Briefen laut der Lehre aber nicht aufgebürdet werden.[48] Bei Personen, die sich in Untersuchungshaft befinden, ist der Zugriff auf Sendungen im Rahmen besonderer Regeln zulässig. Gefährliche Sendungen (Briefbomben o.ä.) darf auch die Sicherheitspolizei – ohne weitere Voraussetzungen wie jene der StPO – sicherstellen. Auch Zollorgane sind darüber hinaus berechtigt, bestimmte Waren in Beschlag zu nehmen.[49]

§§ 188f StPO
§ 42 Abs 1 Z 1 SPG,
§ 26 ZollR-DG

§ 135 Abs. 1 StPO

Die Beschlagnahme von Briefen und Sendungen ist nur zulässig, wenn diese Maßnahme zur Aufklärung einer vorsätzlich begangenen Straftat erforderlich ist, die außerdem mit mehr als einjähriger Freiheitsstrafe bedroht ist. Die Beschlagnahme von Briefen (oder sonstigen Sendungen) muss von der Staatsanwaltschaft angeordnet und schon zuvor vom Gericht bewilligt werden.[50] Die Beschlagnahme darf nur für einen solchen künftigen Zeitraum angeordnet werden, der zur Erreichung ihres Zwecks voraussichtlich erforderlich ist. Auch eine neuerliche Anordnung ist jedoch zulässig, soweit „aufgrund bestimmter Tatsachen anzunehmen ist, dass die weitere Durchführung der Ermittlungsmaßnahme Erfolg haben werde.“ Wenn die Voraussetzungen aber wegfallen, ist die Ermittlungsmaßnahme zu beenden. Die Staatsanwaltschaft darf ohne gerichtliche Bewilligung bis zu drei Tage lang die Zurückhaltung der Sendung anordnen, wenn bis dann aber keine gerichtliche Bewilligung vorliegt, darf die Sendung nicht weiter zurückgehalten werden.

§ 137 StPO

§ 137 Abs. 3 StPO

§ 138 Abs. 2 StPO

In der Lehre haben sich in Anbetracht des Grundrechtes auf Achtung der Privatsphäre einige weitere materielle Voraussetzungen herausgebildet, die für die Beschlagnahme von Sendungen vorliegen müssen: Die Sendung muss für ein konkretes Strafverfahren gebraucht werden, in dem bereits ein Verdacht besteht und darf nicht zur Gewinnung von Verdachtsgründen eingesetzt werden. Die Anlasstat muss eine schwerwiegende sein. Mit weniger einschneidenden Maßnahmen wäre die Erfolgsaussicht wesentlich geringer. Diese Punkte fließen wiederum in eine Gesamtbeurteilung ein, sie sind nicht alle verpflichtend, wenn aber eine fehlt, gibt es erhöhten Begründungsbedarf.[51] Auch Art. 10 Staatsgrundgesetz (StGG) von 1867 schützt das Briefgeheimnis, erlaubt aber grundsätzlich die Beschlagnahme von Briefen auf der Grundlage von Gesetzen nach richterlicher Bewilligung.

Art. 8 EMRK

➲ *Grundrechte, 9.2.1*

Geschichte und Kritik

Die Befugnis zur Beschlagnahme von Briefen wurde 2018 im Zuge des Überwachungspakets wesentlich geändert. Es wurde die Voraussetzung gestrichen, dass sich Beschuldigte wegen einer vorsätzlichen, mit mehr als einjähriger Freiheitsstrafe bedrohten Tat in Haft befinden oder eine Vorführung oder Festnahme deswegen angeordnet wurde.[52] Erst seit dieser Novelle können also auch Briefe von Personen, die sich nicht bereits in Haft befinden (oder gegenüber denen eine Festnahme angeordnet ist), überhaupt beschlagnahmt werden. Es handelte sich um eine massive Ausweitung dieser Ermittlungsbefugnis.

Sicherheitspaket 2018

Laut den Erläuterungen der Regierung sollte der Entfall dieser Voraussetzungen bei der Beschlagnahme „insbesondere eine effektive Bekämpfung und Verfolgung des zunehmenden Versandes von Briefen mit im sog. Darknet angebotenen Suchtmitteln ermöglichen.“[53] Eine Einschränkung des Rechtsschutzes sei damit deshalb nicht verbunden, weil die Befugnis weiterhin nur auf Anordnung der Staatsanwaltschaft und mit gerichtlicher Bewilligung zulässig sei.[54]

Außerdem wurde in derselben Novelle die Voraussetzung entfernt, dass Betroffene sofort über die Beschlagnahme informiert werden müssen. Die Aufschiebung dieser Zustellung der Benachrichtigung wurde eingeführt, da sonst laut Materialien die damalige Regierung die Beschlagnahme von Briefen (an und von Personen, die nicht inhaftiert sind) dem Zweck zuwiderlaufen würde, da die Betroffenen dann über die Ermittlungen informiert wären.[55]
In der parlamentarischen Begutachtung stoß die Ausweitung auf Kritik, u.a. auch von der Vereinigung der österreichischen Richterinnen und Richter[56], der rechtswissenschaftlichen Fakultät der Universität Wien[57] und des Österreichischen Rechtsanwaltskammertages[58] aufgrund grundrechtlicher Bedenken. In einer Gesamtbetrachtung ist diese Befugnis, die im Geheimen angewandt wird, in eines der ältesten Grundrechte eingreift und zur Bekämpfung von Drogendelikten dienen soll unverhältnismäßig und damit wohl verfassungswidrig. Diese Befugnis wurde im ersten Jahr seit ihrer Ausweitung 14 Mal angewendet.[59]

Endnoten

1 Vgl. *Paar/Pelzl*, Kryptografie verständlich, ein Lehrbuch für Studierende und Anwender (2016) 3.
2 So etwa im Fall vom Mohamed M.(Vgl. *Pentz/Prack/Schmidinger/Wittek*, „Das ist kein Gottesstaat!“ Terrorismus und Rechtsstaat am Beispiel des Prozesses gegen Mohamed M. und Mona S. (2008) 89f.)
3 Vgl. *Scherschel*, EternalBlue: Hunderttausende Rechner über alte NSA-Schwachstelle infizierbar in: heise.de 19.09.2018, https://www.heise.de/security/meldung/EternalBlue-Hunderttausende-Rechner-ueber-alte-NSA-Schwachstelle-infizierbar-4167918.html (15.04.2020).
4 Vgl. *Briegleb*, WannaCry: Was wir bisher über die Ransomware-Attacke wissen, in: heise.de 13.05.2017, https://www.heise.de/newsticker/meldjetzt ung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html (15.04.2020).
5 Vgl. *Scherschel*, Alles, was wir bisher über den Petya/NotPetya-Ausbruch wissen, in: heise.de 28.06.2017, https://www.heise.de/security/meldung/Alles-was-wir-bisher-ueber-den-Petya-NotPetya-Ausbruch-wissen-3757607.html (15.04.2020).
6 Vgl. *Smart*, Lessons learned review of the WannaCry Ransomware Cyber Attack (2018) 10; 14. (https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wanna-cry-ransomware-cyber-attack-cio-review.pdf)

7 Gesetzesbeschluss des deutschen Bundestags 2017. (https://dipbt.bundestag.de/dip21/brd/2017/0527-17.pdf)
8 Ministerialentwurf 192/ME, XXV.GP, https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00192/index.shtml (19.12.2019).
9 Ministerialentwurf 325/ME, XXV. GP, https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00325/index.shtml (19.12.2019).
10 Richtlinie (EU) 2017/541 des europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates.
11 Verfassungsgerichtshof, Kfz-Kennzeichenerfassung und „Bundestrojaner" verfassungswidrig, 11.12.2019, https://www.vfgh.gv.at/medien/Kfz-Kennzeichenerfassung_und___Bundestrojaner___verfass.de.php (19.12.2019).
12 VfGH 11.12.2019, G 72-74/2019-48, G 181-182/2019-18, Rz 195.
13 Zitat aus dem Akt nachzulesen in *Sulzbacher,* Wenn der Staat hackt, wird nicht vom „Bundestrojaner" geredet, in: derstandard.at 07.08.2017, https://derstandard.at/2000062083703/Wenn-der-Staat-hackt-wird-nicht-vom-Bundestrojaner-geredet (15.04.2020).
14 *Pentz/Prack/Schmidinger/Wittek*, „Das ist kein Gottesstaat!" Terrorismus und Rechtsstaat am Beispiel des Prozesses gegen Mohamed M. und Mona S. (2008) 89f.
15 Ebd. 91.
16 *Chaos Computer Club,* Analyse einer Regierungs-Malware (2011) 5. (https://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf)
17 Vgl. *Adensamer/Hanel*, Das Überwachungspaket im Überblick. Kritik an neuen Ermittlungsbefugnissen, juridikum 3/2018, 295.
18 Vgl. *Fischer/Müller/Pilcher/van Rinsum,* Internet World Business, Leben in der Welt 4.0 17/2014, 8.
19 Vgl. *Bundesministerium für Inneres*, Anfragebeantwortung „Fluggastdatenanalyse – Kosten und Beschaffung" vom 03.07.2019, https://fragdenstaat.at/anfrage/fluggastdatenanalyse-kosten-und-beschaffung/#nachricht-4374 (17.12.2019).
20 Vgl. *Bundesministerium für Inneres,* Anfragebeantwortung 3516/AB XXVI. GP vom 09.07.2019 zur Anfrage 3506/J XXVI. GP vom 09.05.2019, 3. (https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_03516/imfname_760990.pdf)
21 *Bundesministerium für Inneres,* Anfragebeantwortung „Fluggastdatenanalyse – Datenschutzrechtliche Aspekte" vom 08.10.2019, https://fragdenstaat.at/anfrage/fluggastdatenanalyse-datenschutzrechtliche-aspekte/ (17.12.2019).
22 Im Juli 2019 waren 10 von 91 Fluglinien an das System angebunden. Vgl. *Bundesministerium für Inneres,* Anfragebeantwortung 3516/AB XXVI. GP vom 09.07.2019 zur Anfrage 3506/J XXVI. GP vom 09.05.2019, 6.
23 *Europäischer Gerichtshof,* Gutachten 1/15 vom 26.07.2017, http://curia.europa.eu/juris/document/document.jsf?text=&docid=193216&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=9304217 (17.12.2019).
24 Vgl. https://epicenter.works/thema/pnr (17.12.2019).
25 Vgl. https://nopnr.eu/ (17.12.2019).
26 Vgl. Erläuterungen zu § 54 Abs. 4b SPG, 15 d. B., XXVI. GP, 2. (https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00015/imfname_681955.pdf)
27 Vgl. Ebd.
28 Verfassungsgerichtshof, G 72-74/2019, G 181-182/2019, vom 11.12.2019, 4. (https://www.vfgh.gv.at/downloads/VfGH_Verkuendung_11.12.2019_G_72_2019.pdf)
29 Siehe § 53 Abs. 2 SPG und *Heißl,* Überwachungen und Ermittlungen im Internet (2017) 90.
30 Abfrage auf ris.bka.gv.at: A4 Fischamend-Bruck West I, Amras, Bosrucktunnel, Ehrentalerbergtunnel, Flughafen-Fischamend, Gleinalmtunnel, Gräberntunnel, Graz Ost, Grimmenstein, Haag – Ried, Hochstraße Inzersdorf, Hummelhof, A4, Kaisermühlentunnel, Lafnitz-Hartberg, Nordumfahrung Klagenfurt, Oswaldibergtunnel, Pichl, Plabutschtunnel, Pöchlarn, Bruck-Oberaich, Tunnel Donnersberg, Tunnel Kollmann, Tunnel Selzthal, Pretallerkogel, Voestbrücke 3b, Wechselabschnitt, Weibern-Haag, Wr. Neustadt – Grimmenstein und Ybbs.
31 Vgl. *Bundesministerium für Inneres,* Anfragebeantwortung 2841/AB, XXVI. GP vom 15.04.2019 zur Anfrage 2855/J, XXVI. GP vom 15.02.2019. (https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_02841/imfname_748095.pdf)
32 Vgl. Ebd.
33 Vgl. ASFINAG, Stellungnahme 8859 zu ME/326 XXV. GP, 10. (https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_30400/imfname_667745.pdf)
34 Vgl. *Verfassungsgerichtshof*, VfSlg 18146 vom 15.06.2007, https://www.ris.bka.gv.at/VfghEntscheidung.wxe?Abfrage=Vfgh&Dokumentnummer=JFT_09929385_06G00147_00&IncludeSelf=True (17.12.2019).
35 Vgl. *Verfassungsgerichtshof*, G 72-74/2019, G 181-182/2019, vom 11.12.2019, 8f. (https://www.vfgh.gv.at/downloads/VfGH_Verkuendung_11.12.2019_G_72_2019.pdf)
36 Vgl. Erläuterungen zur Regierungsvorlage, 49 d. B. XX. GP, 22. (https://www.parlament.gv.at/PAKT/VHG/XX/I/I_00049/fname_138938.pdf)
37 Also Vorsatzdelikte mit lebenslanger oder mit mehr als dreijähriger Freiheitsstrafe bedroht sind (§ 17 Abs. 1 StGB).
38 Vgl. *Heißl*, Überwachungen und Ermittlungen im Internet (2017) 93.
39 Vgl. Parlamentskorrespondenz Nr. 455 vom 02.07.1997: Justizausschuss: SP-VP-Mehrheit für neue Ermittlungsmethoden https://www.parlament.gv.at/PAKT/PR/JAHR_1997/PK0455/index.shtml (18.12.2019).
40 Vgl. BGBl I 105/1997.
41 Erläuterungen zur Regierungsvorlage, 49 d. B. XX. GP, 15f.
42 Vgl. Parlamentskorrespondenz Nr. 210 vom 30.03.2011, Rasterfahndung wurde noch nie eingesetzt. Kritik an Tierschützerprozess und Vorratsdatenspeicherung https://www.parlament.gv.at/PAKT/PR/JAHR_2011/PK0310/index.shtml (18.12.2019), *Bundesministerium für Justiz,* Anfragebeantwortung 3829/AB vom 4.5.2015 XXV. GP zur Anfrage 4034/J XXV. GP (https://www.parlament.gv.at/PAKT/VHG/XXV/AB/AB_03839/imfname_406589.pdf) und *Ministerium für Inneres,* Bericht über den Einsatz besonderer Ermittlungsmaßnahmen 2014, 16. (https://www.parlament.gv.at/PAKT/VHG/XXV/III/III_00256/imfname_528370.pdf)
Vgl. aber auch die Ungereimtheiten in den Zahlen von 2008 bis 2014 in *Adensamer/Steinhauser,* Ermittlungsmaßnahmen nach 2008, in Die Grünen (Hrsg.), Nie mehr allein… Überwachungsbericht 2017, https://www.gruene.at/ueberwachungsbericht (19.12.2019).
43 Vgl. *Bundesministerium für Justiz,* Gesamtbericht 2015. Einsatz besonderer Ermittlungsmaßnahmen (2016) 15. (https://www.parlament.gv.at/PAKT/VHG/XXV/III/III_00319/imfname_567496.pdf)
44 Vgl. *Bundesministerium für Justiz,* Gesamtbericht 2016. Einsatz besonderer Ermittlungsmaßnahmen (2017) 9. (https://www.parlament.gv.at/PAKT/VHG/XXVI/III/III_00063/imfname_674973.pdf)
45 Vgl. *Reindl-Krauskopf/Tipold/Zerbes,* WK-StPO § 134 StPO Rz 1.
46 Vgl. ebd. Rz 11.
47 Vgl. ebd. Rz 13f.
48 Vgl. ebd. Rz 9.
49 Vgl. ebd. Rz 5.
50 Vgl. ebd. Rz 9.
51 Vgl. ebd. Rz 10 mwN. Anm.: In dieser Aufzählung war auch noch der Punkt „Die Betroffenen werden verständigt. Ihnen stehen Rechtsmittel offen", enthalten, dieser ist aber mit dem Strafprozessrechtsänderungsgesetz 2018 wohl hinfällig.
52 § 137 StPO; Regierungsvorlage 17 d. B. XXVI. GP, 3, https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00017/index.shtml (20.12.2019).
53 Erläuterungen zur Regierungsvorlage 17 d. B. XXVI. GP, 3.
54 Vgl. ebd. 19.
55 Vgl. Ebd.
56 Vgl. *Vereinigung der österreichischen Richterinnen und Richter,* Stellungnahme 88 zu 17 d. B. XXVI. GP, 5. (https://www.parlament.gv.at/PAKT/VHG/XXVI/SN/SN_00088/imfname_687945.pdf)
57 Vgl. *Rechtswissenschaftliche Fakultät Universität Wien,* Stellungnahme 58 zu 17 d. B. XXVI. GP, 6. (https://www.parlament.gv.at/PAKT/VHG/XXVI/SN/SN_00058/imfname_687572.pdf)
58 Vgl. *Österreichischer Rechtsanwaltskammertag ÖRAK,* Stellungnahme 5 zu 17 d. B. XXVI. GP, 3. (https://www.parlament.gv.at/PAKT/VHG/XXVI/SN/SN_00005/imfname_684291.pdf)
59 Vgl. *Bundesministerium für Inneres,* Anfragebeantwortung 3918/AB, XXVI. GP vom 04.09.2019 zur Anfrage 3899/J, XXVI. GP vom 09.07.2019, https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_03918/index.shtml (21.12.2019). Siehe auch *Bundesministerium für Inneres,* Anfragebeantwortung 3918/AB, XXVI. GP vom 04.09.2019 zur Anfrage 3899/J, XXVI. GP vom 09.07.2019, https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_03918/index.shtml (21.12.2019).

RECHTE VON BETROFFENEN

Arguing that you don't care about
the right to privacy because you
have nothing to hide is no different
than saying you don't care about
free speech because you have
nothing to say

Edward Snowden

9 Grundrechte

9.1 Grundrechte und Überwachung

Grundrechte erfüllen eine Schutzpflicht

Im Rahmen der Evaluierungsprozesse von Überwachungsbefugnissen kommt den Grundrechten eine besonders hohe Bedeutung zu, denn sie bilden die Legitimationsgrundlage für das gesamte staatliche Handeln eines modernen, demokratischen Verfassungsstaates. Aus rechtstheoretischer Sicht schließen sich die Menschen mittels Gesellschaftsvertrag zu einer Gesellschaft zusammen, um dem Staat die Macht zu übertragen, die Bürger_innen vor Eingriffen in ihre Rechte zu bewahren.[1] Die Schutzpflicht besteht auf zwei Ebenen, nämlich zum einen zwischen den Bürger_innen und zum anderen im Verhältnis zum Staat selbst. Da die Grundrechte Schranken für staatliches Handeln darstellen, ist das Handeln nur legitim, wenn es innerhalb der durch die Grundrechte gesteckten Grenzen stattfindet.

Das folgende einleitende Kapitel gibt zunächst Einblick in die Rechtsnatur der Grundrechte und benennt die Grundrechtskataloge, die in Österreich gelten (9.1.2). Danach wird aufgezeigt, welche Voraussetzungen erfüllt sein müssen, damit ein staatlicher Eingriff in ein Grundrecht gerechtfertigt und damit zulässig ist (9.1.3). Anschließend werden jene Grundrechte näher behandelt, die durch staatliche Überwachungsmaßnahmen berührt sein können und daher im Rahmen des Gesetzgebungsprozesses und in der Vollziehung zu beachten sind (9.2–9.5).Um einen besseren Überblick über die Grundrechtsthematik zu erhalten, werden die einzelnen Grundrechte und die jeweiligen staatlichen Eingriffsmöglichkeiten in den relevanten Rechtsgrundlagen separat behandelt.

9.1.1 Rechtsnatur der Grundrechte

Grundrechte als objektive Maßstäbe

Im Stufenbau der Rechtsordnung – dem Verhältnis der Normen zueinander – sind die Grundrechte in der Verfassungsebene angesiedelt und stehen daher über den einfachen Gesetzen. Sie begrenzen den Staat in der gesamten Machtausübung, also sowohl in der Gesetzgebung als auch in der Rechtsprechung und in der Verwaltung. Das gesamte staatliche Handeln ist immer an den Grundrechten zu messen, weshalb es sich um objektive Grundrechtsnormen handelt. Die Grundrechte bilden aber nicht nur objektive Maßstäbe für staatliches Handeln, sondern sie sind auch vor den unabhängigen Gerichten durchsetzbar. Man spricht in diesem Zusammenhang deshalb von subjektiven Rechten. Der konkrete Rechtsanspruch hängt dabei vom Schutzbereich (bzw. Gewährleistungsbereich) des betroffenen Grundrechts ab. Grundsätzlich ist der Staat entweder zu einem Tun (z.B. Recht auf den_die gesetzliche_n Richter_in) oder zu einem Unterlassen (z.B. Willkürverbot, Zensurverbot) verpflichtet.
In inhaltlicher Hinsicht umfassen die einzelnen Grundrechte verschiedene Schutzbereiche, die grob in Freiheitsrechte, Gleichheitsrechte, Verfahrensgarantien, politische und soziale Grundrechte unterteilt werden können.[2] Im Zusammenhang mit den hier relevanten Überwachungsmaßnahmen sind insbesondere die Freiheitsrechte von Bedeutung, da diese den Bürger_innen gewisse Freiheiten vor staatlichen Eingriffen garantieren (sog. Abwehrfunktion). Daneben spielen aber auch Verfahrensgarantien eine Rolle.

Während Grundrechte als vertikale Rechte konzipiert sind, also grundsätzlich nur im Verhältnis zwischen Bürger_in und Staat gelten, bildet das Recht auf Datenschutz das einzige Grundrecht, welches auch in einem horizontalen Verhältnis, also zwischen den Bürger_innen, direkt Wirkung entfaltet (sog. unmittelbare Drittwirkung). Von einer mittelbaren Drittwirkung der Grundrechte spricht man, wenn Grundrechte im Privatrecht, also zwischen den Bürger_innen, durch einfaches Gesetzesrecht vermittelt werden.[3]

9.1.2 Grundrechtskataloge: StGG, EMRK und GRC

Staatsgrundgesetz
Europäische Konvention der Menschenrechte
Europäische Grundrechtecharta

Der österreichische Staat ist in seinem Handeln durch mehrere – im Verfassungsrang stehende – Rechtsgrundlagen beschränkt, die sich teilweise in ihrem Schutzumfang unterscheiden. Mit dem Staatsgrundgesetz über die allgemeinen Rechte der Bürger_innen (StGG) hat Österreich 1867 auf nationaler Ebene einen Grundrechtskatalog geschaffen, dessen Grundrechte insbesondere durch die Europäische Konvention der Menschenrechte (EMRK) ergänzt wurden. Dabei handelt es sich um einen völkerrechtlichen Vertrag des Europarats. Zudem werden die in der Europäischen Grundrechtscharta (GRC) verbürgten Grundrechte wie verfassungsgesetzlich gewährleistete Rechte der österreichischen Bundesverfassung angesehen. Die Mitgliedstaaten der EU sind aber nur bei der Durchführung von Unionsrecht an die GRC gebunden (Art. 51 Abs. 1 GRC), d.h. wenn eine Handlungs- oder Durchführungsverpflichtung aus dem Primär- oder Sekundärrecht vorliegt.[4] Neben der EMRK, dem StGG und der GRC gibt es noch eine Vielzahl weiterer Grundrechtsquellen[5], die jedoch für unseren Zweck nicht von besonderer Relevanz sind.

(Unions-)Bürger_innen- vs. Menschenrechte

Der Anwendungsbereich der drei Grundrechtskataloge unterscheidet sich insofern, als die in der EMRK verbürgten Rechte als Menschenrechte, also als Rechte Aller, konzipiert sind. Daraus folgt, dass sie nicht an eine konkrete Staatsbürger_innenschaft geknüpft sind und sich somit auch Fremde in Österreich darauf berufen können. Im Unterschied dazu sind viele der Grundrechte des StGG als Bürger_innenrechte ausgestaltet, das heißt, dass das StGG häufig an die österreichische Staatsbürger_innenschaft gekoppelt ist. Die GRC beinhaltet sowohl Menschen- als auch Bürger_innenrechte. Letztere knüpfen an die Unionsbürger_innenschaft an. Die Menschenrechte haben ihren Anknüpfungspunkt bei der Person und schützen daher Unionsbürger_innen, Nicht-EU-Bürger_innen und Personen ohne Staatsbürger_innenschaft gleichermaßen.

Zur Übersichtlichkeit sind in diesem Kapitel Verweise auf Fälle farblich gekennzeichnet. Es gibt folgende Kategorien von Verweisen und Hervorhebungen:
1. Bezug zur EMRK
3. Bezug zum StGG
2. Bezug zur GRC

Bestehen Unsicherheiten bei der Auslegung einzelner verfassungsrechtlicher Normen, ist in Österreich grundsätzlich der Verfassungsgerichtshof (VfGH) zuständig, Klarheit zu schaffen. Das gilt insbesondere im Rahmen des StGG, welches nur in Österreich in Kraft ist. Bestimmungen der EMRK können ebenfalls vom VfGH auslegt werden, da es sich dabei um österreichisches Verfassungsrecht handelt. Grundsätzlich folgt der VfGH aber der Rechtsanschauung des Gerichtshof für Menschenrechte (EGMR) in Straßburg. Der EGMR ist dem VfGH in Bezug auf die EMRK übergeordnet und kann daher von Betroffenen erst nach Ausschöpfung des innerstaatlichen Instanzenzugs angerufen werden.[6] Handelt es sich bei der betroffenen Norm um eine Bestimmung aus der GRC, muss der VfGH die Frage dem Europäischen Gerichtshof (EuGH) vorlegen, wenn der VfGH selbst nicht zweifelsfrei entscheiden kann (sog. Vorabentscheidungsverfahren nach Art. 267 AEUV).

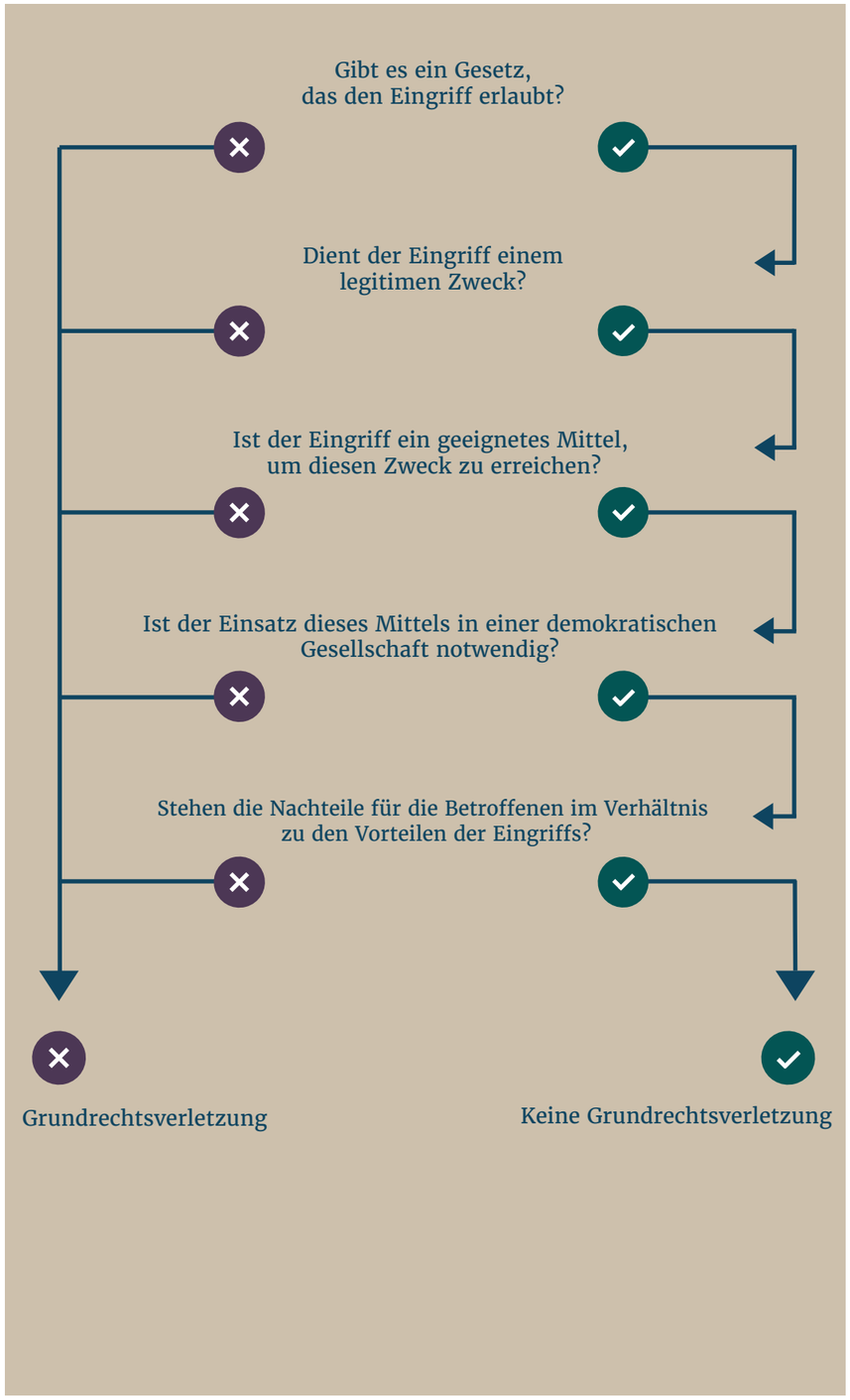


Abb. 12
Die Verhältnismäßigkeits-prüfung

9.1.3 Verhältnismäßigkeitsprüfung

Ein Eingriff in ein Grundrecht findet immer dann statt, wenn der Schutzbereich berührt ist. Wenn das der Fall ist, ist das staatliche Handeln aber nicht per se rechtswidrig: Betreten beispielsweise Polizeibeamt_innen ein Haus ohne Einwilligung der dort wohnenden Person, um es zu durchsuchen, sind eindeutig mehrere Grundrechte berührt: das Recht auf Achtung des Privatlebens, vielleicht auch des Familienlebens sowie das Recht auf Achtung der Wohnung und das Grundrecht auf Datenschutz. Hausdurchsuchungen sind unter bestimmten Voraussetzungen in unserer Rechtsordnung aber ein vorgesehenes Mittel zur Verbrechensbekämpfung. Grundrechtseingriffe sind daher nicht per se unzulässig. Vielmehr muss dass staatliche Handeln einer umfassenden Prüfung standhalten, dann sind auch Grundrechtseingriffe rechtmäßig.

Für diese Überprüfung wird ein stufenweise aufgebautes Schema angewendet. Ist jede der Fragen zu bejahen, stellt der gegenständliche Eingriff keine Verletzung des Grundrechts dar, ist also zulässig. Diese Prüfung variiert bei einzelnen Grundrechten leicht, es geht jedoch im Kern immer um die im Folgenden aufgelisteten Fragen.

Legitimer Zweck, angemessene Mittel

Als Vorfrage ist zunächst in jedem Fall zu prüfen, ob überhaupt der Schutzbereich eines Grundrechts berührt ist. Ist dies der Fall, kann mit der eigentlichen Prüfung begonnen werden, bei der es stark um die Frage der Verhältnismäßigkeit geht. Zunächst muss festgestellt werden, ob der Eingriff eine gesetzliche Grundlage hat. Das heißt auch, dass der Eingriff die gesetzlichen Voraussetzungen erfüllt und das Gesetz der Verfassung entspricht. Danach muss klargestellt werden, ob der Zweck, den das staatliche Handeln verfolgt, überhaupt legitim ist. Danach ist zu prüfen, ob die Maßnahme zur Erreichung dieses Ziels geeignet ist. Zudem muss das gewählte Mittel in einer demokratischen Gesellschaft erforderlich sein. Damit ist gemeint, dass es das gelindeste Mittel sein muss, falls also eine Vielzahl an Mitteln zur Auswahl steht, um den Zweck zu erreichen, muss es das sein, das am wenigsten in Grundrechte eingreift. Abschließend ist die Adäquanz zu prüfen, was einer Verhältnismäßigkeitsprüfung im engeren Sinn gleichkommt: Es ist eine Abwägung zwischen dem angestrebten Zweck und der Beeinträchtigung des Rechtsgutes durchzuführen und damit zu überprüfen, ob Ersteres wirklich höherwertig ist als Zweiteres.

9.2 Privatleben und Datenschutz

Grundrechte, die im Zusammenhang mit Überwachungsmaßnahmen besonders stark betroffen sind, sind das Recht auf Privatleben sowie das Recht auf Datenschutz. Dabei handelt es sich zwar um eigenständige Rechte, aufgrund des ähnlichen Anwendungsbereiches werden sie aber im folgenden Kapitel gemeinsam erläutert.

9.2.1 Recht auf Achtung des Privat- und Familienlebens.

Art. 8 EMRK

Art. 8 Europäische Menschenrechtskonvention

(1) Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihres Briefverkehrs.

(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und

Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

Art. 8 EMRK umfasst vier Rechte, nämlich den Schutz des Privatlebens, des Familienlebens, der Wohnung und der Korrespondenz. Obwohl die einzelnen Rechte unterschiedliche Schutzbereiche umfassen, sind sie nicht immer exakt voneinander abgrenzbar. Häufig subsumiert der EGMR einen Tatbestand unter einen der Schutzbereiche, ohne sich damit auseinanderzusetzen, ob der Tatbestand möglicherweise auch unter einen anderen Schutzbereich fallen könnte.[7] Den vier Bereichen ist gemein, dass sie alle grundsätzlich frei von staatlicher Einflussnahme sein sollen, weshalb dem Art. 8 EMRK im Zusammenhang mit staatlichen Überwachungsmaßnahmen sowie der Sammlung und Speicherung von Daten eine besonders hohe Bedeutung zukommt.
Im Folgenden wird skizziert, wann Art. 8 EMRK im Zusammenhang mit polizeilichen Überwachungsmaßnahmen relevant ist. Anschließend wird erläutert, unter welchen Bedingungen ein solcher Eingriff gerechtfertigt sein kann.

Privatleben

Der Begriff des Privatlebens wird vom EGMR weit ausgelegt, wodurch Schutzlücken vermieden werden sollen. Eine abschließende Definition des Begriffs ist nicht möglich. Grundsätzlich umfasst das Privatleben im Sinne des Art. 8 EMRK aber jedenfalls alle Dimensionen, die der individuellen Persönlichkeitssphäre zurechenbar sind, wodurch die Identität, Entwicklung und Verwirklichung der einzelnen Person gewährleistet werden soll.[8] Dieser Bereich soll grundsätzlich frei von staatlicher Beobachtung, Überwachung und Ausforschung sein.[9]

Eingriff

personenbezogene Daten

Personenbezogene Daten, „also alle Daten über eine bestimmte oder bestimmbare Person“[10], sind vom Privatleben umfasst und daher von Art. 8 EMRK geschützt. Es handelt sich dabei um solche Daten, die eine Identifikation der betroffenen Person ermöglichen. Ob dynamische IP-Adressen personenbezogene Daten sind, ist vom EGMR noch nicht beurteilt worden. Ausschlaggebend ist, ob die Identifizierung der betroffenen Person ohne weiteres möglich ist.[11]

Videoüberwachung

Grundsätzlich werden aber nur jene Daten geschützt, die nicht als allgemein verfügbare Informationen der öffentlichen Sphäre zuzurechnen sind.[12] Allerdings hat der EGMR bereits mehrmals festgestellt, dass das gezielte Sammeln und Speichern von öffentlichen Informationen über eine Person sehr wohl einen Eingriff in Art. 8 EMRK darstellt. Auch die Videoüberwachung im öffentlichen Raum zeichnet grundsätzlich nur öffentlich zugängliche Informationen auf, da das gefilmte Verhalten auch von jeder anderen anwesenden Person wahrnehmbar ist. Daher stellt die Videoüberwachung nur dann einen Eingriff in Art. 8 EMRK dar, wenn das gefilmte Material systematisch oder dauerhaft gespeichert wird. Ähnliches gilt bei der GPS-Überwachung, wenn dadurch ein Bewegungsprofil des Datensubjekts erstellt wird. Informationen, die im Internet öffentlich zugänglich sind, können von Sicherheitsbehörden grundsätzlich rechtmäßig erworben werden, wobei auch hier das Legalitätsprinzip (Art. 18 B-VG) beachtet werden muss. Auch hier liegt ein Eingriff vor, wenn diese Informationen systematisch gesammelt werden und die betroffene Person identifizierbar wird.

Rotaru Rz 43

P.G. und J.H. Rz 57

Uzun Rz 44

Peck Rz 59
Rotaru Rz 43 ff.;

Systematische Datensammlung

Das systematische Sammeln von Daten, die in einer Datenbank gespeichert werden, ist daher immer ein Eingriff in das Recht auf Privatsphäre. Irrelevant ist, ob die Daten öffentlich zugänglich sind oder nicht. Diese Auslegung von Art. 8 EMRK soll verhindern, dass Daten angehäuft werden, die in ihrer Gesamtheit eine Profilbildung und damit eine Identitätsidentifikation der betroffenen Person ermöglichen.[13] Unerheblich ist dabei, ob die Daten an Dritte weitergegeben wurden oder die Speicherung der Daten zu Nachteilen (z.B. Verwendung in einem Verfahren) geführt hat.

Copland Rz 43

Briefverkehr

Neben dem Privatleben erklärt Art. 8 EMRK auch ausdrücklich den Briefverkehr als schutzwürdigen Lebensbereich. Aufgrund der technologischen Entwicklungen der letzten Jahre, wodurch der Briefverkehr zunehmend durch andere Kommunikationsmöglichkeiten abgelöst wurde, hat der EGMR bereits mehrmals festgestellt, dass die Tatbestände Privatleben und Briefverkehr auch Telefongespräche umfassen. Auch die Kommunikation via Fax, E-Mail, Telefonieren über das Internet sowie die Individualkommunikation über message services (z.B. WhatsApp, Skype, Facebook Messenger etc.) sind vom Schutzbereich des Privatlebens und des Briefverkehrs mitumfasst. Da für die Schutzwürdigkeit der Kommunikation primär entscheidend ist, dass es sich nicht um öffentlich zugängliche Korrespondenz handelt, fällt berufliche bzw. geschäftliche Kommunikation ebenso unter Art. 8 EMRK wie private Kommunikation.

Klass Rz 41
Message services als Schutzbereich
Copland Rz 42;
Liberty Rz 52

Ekimdzhiev Rz 60

Verbindungsdaten

Kommunikationsverkehrsdaten (auch: Verbindungsdaten) geben Aufschluss darüber, wer mit wem, wann, wo und wie lange kommuniziert hat.[14] Diese Daten – sowohl bei Telefongesprächen als auch im E-Mailverkehr – sind jedenfalls vom Tatbestand der Korrespondenz umfasst. Ob sie als personenbezogene Daten auch vom Recht auf Privatleben umfasst sind, hängt davon ab, ob dadurch die Identifikation einer Person möglich ist.[15] Im Urteil zur Massenüberwachung in Großbritannien hat der EGMR aber festgestellt, dass Verkehrsdaten grundsätzlich ähnlich schützenswert sind wie der Kommunikationsinhalt selbst.

Vgl. Copland Rz 44

Big Brother Watch Rz 356

Das Recht auf Achtung der Wohnung ist auf einen räumlichen Bereich begrenzt und daher um vieles enger als das Recht auf Achtung des Privatlebens, das auch in öffentlichen Räumen Wirkung entfaltet. Dadurch wird die ungestörte Nutzung einer Wohnung, eines Büros oder auch einer Gefangenenzelle gewährleistet. Eine Hausdurchsuchung oder das Anbringen von optischen Überwachungsmitteln und Abhörgeräten stellen beispielsweise einen Eingriff in Art.8 EMRK dar. Aber auch das bloße Betreten einer Wohnung greift bereits in Art. 8 EMRK ein.

Vgl. VfSlg 11.266.

Rechtfertigung

Gemäß Art 8. Abs. 2 EMRK ist ein Eingriff gerechtfertigt – und somit keine rechtswidrige Verletzung – wenn der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist. Die legitimen Ziele, die einen Eingriff rechtfertigen, werden von Art. 8 Abs. 2 EMRK taxativ (d.h. vollständig und abschließend, im Gegensatz zu demonstrativ=beispielhaft) aufgezählt, somit gelten alle nicht aufgezählten als keine legitimen Ziele. Folglich handelt es sich dabei um einen sogenannten materiellen Gesetzesvorbehalt. Anders als beim formellen Gesetzesvorbehalt braucht es also mehr als bloß ein nicht näher spezifiziertes öffentliches Interesse.[16]

Die Voraussetzungen für einen gerechtfertigten Eingriff in Art. 8 EMRK:

1. Voraussetzung: „gesetzlich vorgesehen“

Der EGMR hat mehrmals festgestellt, dass die Voraussetzung in Art. 8 Abs. 2 EMRK, wonach ein Eingriff „gesetzlich vorgesehen“ (eng. „in accordance with the law“) sein muss, mehr als die bloße Existenz eines Gesetzes erfordert. Vielmehr muss das Gesetz, das den Eingriff legitimiert, eine gewisse Qualität aufweisen. Dabei sind an Gesetze, die eine geheime Überwachungsmaßnahme erlauben, besonders hohe Anforderungen an die nationalen Schutzmaßnahmen gestellt. Dies begründet der EGMR mit der mangelnden Kenntnis der Betroffenen, da eine nachträgliche Benachrichtigung über eine geheime Überwachung nicht für die Fälle gesetzlich verankert sein muss, bei denen die Benachrichtigung dazu führen könnte, dass Arbeitsweisen der Geheimdienste und verdeckte Ermittler_innen aufgedeckt würden. Im Fall Malone hält der EGMR fest: „Die Gefahr der Willkür tritt dort, wo die Exekutive im Geheimen handelt, mit einzigartiger Klarheit zutage.“ In diesem Sinne hat der

Klass Rz 58

Malone Rz 67

Klass Rz 34

EGMR mehrmals festgestellt, dass die bloße Existenz einer gesetzlichen Grundlage für eine geheime Überwachung bereits einen Eingriff in Art. 8 EMRK darstellt. Ob die Anforderungen an die Gesetzesqualität erfüllt sind, ist für jeden Fall einzeln zu beurteilen. Grundsätzlich **muss jedes Überwachungsgesetz aber alle folgenden Merkmale erfüllen:**

Big Brother Watch Rz 303

- **Vereinbarkeit mit der Rechtsstaatlichkeit**, d.h. es gilt die „Vorherrschaft der Gesetze", wie es in der Präambel der EMRK festgeschrieben ist. Daher würde es dem Rechtsstaat widersprechen, wenn die Exekutive ein unbegrenztes Ermessen hätte. Konkret fordert der EGMR, dass bspw. bei Abhörmaßnahmen – bei welchen die Eingriffsintensität tendenziell sehr hoch ist – eine unabhängige Genehmigung sowie eine richterliche oder sonst unabhängige Kontrolleinrichtung gesetzlich vorgesehen wird. Ein gewisser Ermessensspielraum wird den Behörden aber eingeräumt.[17]

Ekimdzhiev Rz 71; Malone Rz 66ff

Szabó Rz 65

- **Zugänglichkeit des Gesetzes**, d.h. das Gesetz muss ordentlich kundgemacht worden sein und es muss erkennbar sein, welche rechtlichen Vorschriften anwendbar sind.

- **Vorhersehbarkeit**, d.h. das Gesetz muss insoweit bestimmt sein, dass für die Bürger_innen erkennbar ist, unter welchen Umständen und Bedingungen eine Überwachung gesetzlich erlaubt ist.[18] Es muss also möglich sein, die Folgen eines Verhaltens mit einem entsprechenden Grad an Gewissheit vorherzusehen.

Grundsätzlich steigen die qualitativen Anforderungen an das Gesetz mit der Eingriffsintensität, weshalb bei geheimen Überwachungsmaßnahmen besonders hohe Anforderungen gestellt werden.[19] Das bedeutet aber nicht, dass Eingriffe derart konkret vorhersehbar sein müssen, dass der_die Einzelne genau weiß, ob und wann bspw. eine Telekommunikationsüberwachung stattfindet, sodass er_sie sein_ihr Verhalten danach richten kann. Wichtig ist, dass die Umstände und Bedingungen, unter denen eine Überwachung erfolgen kann, klar und detailliert formuliert sind.

Weber Rz 93

Weber Rz 95

Im Fall Weber und Saravia hat der EGMR daher **sechs Voraussetzungen der Vorhersehbarkeit** entwickelt, die zwingend festgelegt sein müssen, wenn ein Gesetz geheime Überwachungsmaßnahmen erlaubt:

- die Art der Straftaten, die eine Überwachungsanordnung rechtfertigen können,

Zakharov Rz 245

- die Personengruppen, deren Telefongespräche abgehört werden können (z.B. nur Verdächtige oder auch deren Kontakt- und Begleitpersonen),

- die Begrenzung der Dauer der Abhörmaßnahme,

Catt Rz 112

- das Verfahren für die Auswertung, Verwendung und Speicherung der erlangten Daten (dabei gelten für sensible personenbezogene Daten wie die politische Meinung erhöhte Anforderungen an die prozessrechtlichen Sicherungsmaßnahmen),

- die bei der Übermittlung der Daten an andere Parteien zu beachtenden Vorsichtsmaßnahmen und

- die Umstände, unter denen die Aufzeichnungen gelöscht und vernichtet werden müssen oder dürfen.

Nur wenn ein betreffendes Gesetz diese sechs Merkmale aufweist, ist es ausreichend präzise formuliert, damit vorhersehbar und stellt damit eine „gesetzliche Grundlage" im Sinne des Art. 8 Abs. 2 EMRK dar.

Fallbeispiel: Big Brother Watch gegen Vereinigtes Königreich (13.09.2018, 58170/13)

Nachdem Edward Snowden 2013 die Massenüberwachung durch die britischen Geheimdienste aufdeckte, klagten mehrere NGOs vor dem EGMR, da sie eine Verletzung ihrer Privatsphäre nach Art. 8 EMRK vermuteten. Der EGMR prüfte den Fall anhand der Voraussetzungen nach Weber und Saravia, da es sich um eine geheime Telekommunikationsüberwachung handelte. Dabei stelle der EGMR fest, dass die gesetzliche Grundlage (Regulation of Investigatory Powers Act 2000) nicht die notwendigen Voraussetzungen der Vorhersehbarkeit erfüllte, da das Gesetz u.a. keine unabhängige Kontrolle des gesamten Auswahlverfahrens, also der eingesetzten Suchfilter und Selektoren, vorsah (Rz. 387). Der Eingriff war daher nicht „gesetzlich vorgesehen" iSd Art. 8 Abs. 2 EMRK, weshalb der EGMR entschied, dass die Massenüberwachung durch die britischen Geheimdienste einen ungerechtfertigten Eingriff in die Privatsphäre nach Art. 8 EMRK darstellt.

Für Überwachungsmaßnahmen von **geringerer Eingriffsintensität** gelten weniger strenge Voraussetzungen, nämlich **allgemeinere Voraussetzungen der Vorhersehbarkeit:**

Uzun Rz 63

- die Art, der Umfang und die Dauer der möglichen Maßnahmen;

- die Gründe, aus denen sie angeordnet werden dürfen;

- die für die Genehmigung, Durchführung und Überwachung solcher Maßnahmen zuständigen Behörden und

- die Art des nach innerstaatlichen Recht vorgesehenen Rechtsbehelfs.

Diese allgemeineren Voraussetzungen der Vorhersehbarkeit verlangt der EGMR bspw. bei der GPS-Überwachung, da diese weniger stark in die Privatsphäre eingreife als visuelle oder akustische Überwachungsmaßnahmen. Der EGMR argumentiert, dass eine GPS-Überwachung die Bewegungen an öffentlichen Plätzen beträfe und primär dazu diene die Aufenthaltsorte von Täter_innen zu ermitteln.

Uzun Rz 66-68

2. Voraussetzung: „in einer demokratischen Gesellschaft notwendig"

Neben den qualitativen Voraussetzungen an die gesetzliche Grundlage verlangt Art. 8 Abs. 2 EMRK, dass der Eingriff notwendig sein muss, um zumindest eines der explizit genannten legitimen Ziele zu erreichen. Es handelt sich dabei um die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, der Schutz der Gesundheit und der Moral oder der Schutz der Rechte und Freiheiten anderer. Die Frage der legitimen Ziele ist selten strittig.[20]

Grundsätzlich gilt, dass ein Eingriff notwendig ist, wenn ein „dringendes soziales Bedürfnis" („pressing social need") besteht, das legitime Ziel zu erreichen, und die dafür vorgesehenen Mittel verhältnismäßig sind. Notwendigkeit bedeutet, dass der Eingriff nicht bloß nützlich oder zweckmäßig sein darf.[21] Ob eine Maßnahme notwendig ist, weil ein dringendes soziales Bedürfnis besteht, liegt grundsätzlich im Beurteilungsspielraum

S. und Marper Rz 101

S. und Marper Rz 102

der Gerichte und Behörden des betreffenden Staates („margin of appreciation"). Die Mitgliedsstaaten haben daher „bei der Wahl der Mittel zum Erreichen des legitimen Ziels des Schutzes der nationalen Sicherheit einen großen Ermessensspielraum". Jedoch ist „[b]ei wesentlichen Aspekten der Existenz oder Identität einer Person […] der Ermessensspielraum begrenzt"[22].

Weber Rz 106

Verhältnismäßigkeit

Wichtiger Schritt der Notwendigkeitsprüfung ist die Beurteilung der Verhältnismäßigkeit, d.h. die ergriffene Maßnahme muss im Hinblick auf das legitime Ziel verhältnismäßig sein.[23] Im Rahmen einer Interessenabwägung wird das Interesse der Öffentlichkeit („pressing social need") an der Verfolgung des legitimen Ziels mit dem Interesse der betroffenen Person abgewogen.[24] Beispielsweise ist es verhältnismäßig, bei Vorliegen eines bloßen Anfangsverdachts einer Straftat von erheblicher Bedeutung eine Observation anzuordnen. Eine Abhörmaßnahme des gesprochenen Wortes ist dagegen eingriffsintensiver und daher nicht verhältnismäßig zum bloßen Anfangsverdacht.

Uzun Rz 26

Unabhängige gerichtliche Kontrolle

Konkret muss ein Gleichgewicht zwischen den widerstreitenden Interessen hergestellt werden. Dazu gehören insbesondere verfahrensrechtliche Schutzmaßnahmen, sodass der Eingriff auf ein vernünftiges Maß beschränkt ist. Der EGMR hält fest, dass „zu prüfen [ist], ob die Verfahren zur Kontrolle von Anordnung und Durchführung von Beschränkungsmaßnahmen geeignet sind, den sich aus den angefochtenen Vorschriften ergebenden Eingriff in den Grenzen dessen zu halten, was in einer demokratischen Gesellschaft notwendig ist." Wichtigste Kontrollinstanz exekutiven Handelns bildet grundsätzlich die unabhängige gerichtliche Kontrolle. Allerdings hält der EGMR in Szabó und Vissy gegen Ungarn fest, „dass es wegen des Charakters der heutigen terroristischen Bedrohungen Notfallsituationen geben kann, in denen die zwingende Anwendung einer richterlichen Genehmigung nicht durchführbar ist, wegen des mangelnden Spezialwissens kontraproduktiv wäre oder schlicht eine Verschwendung wertvoller Zeit darstellen würde." Es sei aber wünschenswert „einen Richter mit der Aufgabe der nachprüfenden Kontrolle zu betrauen."

Klass Rz 54

Szabó, Vissy

Szabó Rz 80

Klass Rz 56

Jedoch wurde oben bereits darauf hingewiesen, dass es Fälle geben kann, in denen Betroffene im Nachhinein nicht über die Überwachungsmaßnahme in Kenntnis gesetzt werden müssen, weshalb der EGMR grundsätzlich hohe Anforderungen an die staatlichen Sicherungsmaßnahmen stellt. Dadurch soll die Gefahr willkürlichen Handelns auf ein Minimum beschränkt werden. Es ist aber durchaus mit der EMRK vereinbar, eine nichtrichterliche Behörde mit der Genehmigung von Telefonüberwachung zu betrauen, vorausgesetzt diese Behörde ist von der Exekutive ausreichend unabhängig.

Szabó Rz 77

9.2.2 Schutz des Privatlebens. Art. 9, Art. 10 und Art. 10a StGG

Art. 9 StGG: Das Hausrecht ist unverletzlich.

Art. 10 StGG: Das Briefgeheimnis darf nicht verletzt und die Beschlagnahme von Briefen, außer dem Falle einer gesetzlichen Verhaftung oder Haussuchung, nur in Kriegsfällen oder auf Grund eines richterlichen Befehls in Gemäßheit bestehender Gesetze vorgenommen werden.

Art. 10a StGG: Das Fernmeldegeheimnis darf nicht verletzt werden. Ausnahmen von der Bestimmung des vorstehenden Absatzes sind nur auf Grund eines richterlichen Befehles in Gemäßheit bestehender Gesetze zulässig.

Hausrecht, Hausdurchsuchung

Anders als die EMRK oder die GRC kennt das österreichische StGG kein allgemeines Recht auf Achtung des Privatlebens. Die relevanten Artikel im Zusammenhang mit Überwachungsmaßnahmen sind Art. 9, Art. 10 und Art. 10a StGG.

Die Unverletzlichkeit des Hausrechts (Art. 9 StGG iVm HausrechtsG) schützt nach der ständigen Rechtsprechung des VfGH ausschließlich vor willkürlichen Hausdurchsuchungen und ist damit wesentlich enger gefasst als das Recht auf Achtung der Wohnung nach Art. 8 EMRK. Hausdurchsuchungen sind daher grundsätzlich nur rechtmäßig, wenn ein richterlicher Befehl vorliegt (§ 1 HausrechtsG). Eine Hausdurchsuchung auf Anordnung der Sicherheitsbehörden – und somit ohne richterlichen Befehl – ist zulässig, wenn Gefahr im Verzug vorliegt, d.h. wenn eine Bewilligung nicht zeitgerecht eingeholt werden kann, ohne den Zweck der Amtshandlung zu gefährden (§ 2 1. Satz HausrechtsG). Eine Hausdurchsuchung kann auch dann durch die Sicherheitsorgane aus eigener Macht vorgenommen werden, wenn gegen jemanden ein Vorführungs- oder Haftbefehl erlassen, oder wenn jemand auf frischer Tat ertappt, durch öffentliche Nachteile oder öffentlichen Ruf einer strafbaren Handlung verdächtig bezeichnet oder im Besitz von Gegenständen betreten wird, welche auf die Beteiligung an einer solchen hinweisen (§ 2 2. Satz HausrechtsG). Aber selbst unter diesen Umständen muss versucht werden, einen richterlichen Befehl beim zuständigen Gericht fernmündlich einzuholen. Erst wenn dieser Versuch fehlschlägt, darf die Sicherheitspolizei selbst prüfen, ob die geplante Hausdurchsuchung die gesetzlichen Bedingungen erfüllt.

Vgl. VfSlg 12.056

Vgl. VfSlg 12.513

Da Art. 8 EMRK Hausdurchsuchungen auch ohne Richtervorbehalt ermöglicht, bietet Art. 9 StGG grundsätzlich die günstigere Regelung. Allerdings ist der Schutzbereich von Art. 8 EMRK weiter, da nicht nur eine Durchsuchung sondern beispielsweise bereits das bloße Betreten einer Wohnung einen Eingriff in Art. 8 EMRK begründen.[25]

Der Schutz des Briefgeheimnisses umfasst die Vertraulichkeit von Briefen, d.h. von „verschlossenen Schriftstücken". Art. 10 StGG hat damit einen sehr begrenzen Anwendungsbereich, da die Kommunikation über das Telefon oder das Internet nicht in den Schutzbereich des Briefgeheimnisses fällt. Außerdem umfasst das Briefgeheimnis nur Inhaltsdaten und bspw. nicht die Informationen auf dem Kuvert.[26] Art. 8 EMRK bietet hier weitreichenderen Schutz, da nicht nur Schriftstücke, sondern auch mündliche Korrespondenz geschützt ist. Darüber hinaus greift Art. 8 EMRK bereits im Vorfeld, da nicht nur das Öffnen von Briefen sondern auch jede andere Behinderung der Korrespondenz einen Eingriff darstellt (z.B. Zurückhalten von Schriftstücken für Häftlinge).

VfSlg 938

Herczegfalvy Rz 88

Art. 10 StGG legt fest, dass das Briefgeheimnis nur gebrochen werden darf, wenn eine gesetzliche Hausdurchsuchung oder Verhaftung, ein Kriegsfall oder ein richterlicher Befehl vorliegt. Art. 8 Abs. 2 EMRK verlangt zusätzlich, dass ein bestimmtes öffentliches Interesse vorliegt, das im Sinne des Verhältnismäßigkeitsprinzips überwiegt.

➲ 9.1.3 Verhältnismäßigkeit

Das Fernmeldegeheimnis (Art. 10a StGG) schützt die Vertraulichkeit und daher den Inhalt von schriftlicher und mündlicher Kommunikation über Telekommunikationsnetze (z.B. über Telefon, Internet). Wie auch das Briefgeheimnis erstreckt sich der Schutzbereich des Fernmeldegeheimnisses nur auf Inhaltsdaten, nicht aber auf andere Daten wie bspw. Stammdaten, Telefonnummern oder auch Metadaten (z.B. statische und dynamische IP-Adressen, Zeitpunkt und Dauer der Kommunikation) etc. Diese Lücke wird aber sowohl durch die DSGVO als auch die EMRK geschlossen.

Vgl. VfSlg 19.657.

🕮 Metadaten

Das Fernmeldegeheimnis darf im Zuge von Überwachungsmaßnahmen nur verletzt werden, wenn ein richterlicher Befehl vorliegt. Damit sind den Eingriffsmöglichkeiten in das Fernmeldegeheimnis engere Grenzen gesetzt als jenen in das Briefgeheimnis, da in Art. 10 StGG im Falle einer gesetzlichen Hausdurchsuchung oder Verhaftung sowie im Kriegsfall auch ohne richterliche Genehmigung eingegriffen werden darf.

Da Art. 9 StGG iVm HausrechtsG, Art. 10 und Art. 10a StGG die staatlichen Eingriffsmöglichkeiten explizit nennen, handelt es sich dabei um sog. qualifizierte Gesetzesvorbehalte. Daher muss das eingreifende Gesetz den Bedingungen

bzw. Anforderungen, die das Grundrecht auf Verfassungsebene selbst nennt, entsprechen (z.B. Richtervorbehalt bei Hausdurchsuchungen).
Abschließend kann festgehalten werden, dass die Regelungen im StGG, die den Schutz des Privatlebens betreffen, für bestimmte Eingriffe (z.B. Hausdurchsuchungen) ganz konkrete Voraussetzungen (z.B. einen richterlicher Befehl) vorsehen, die die EMRK in dieser Bestimmtheit nicht fordert. Dagegen ist der Anwendungsbereich von Art. 8 EMRK viel weiter und umfasst daher auch Überwachungsmaßnahmen, die von Art. 9, 10 und 10a StGG nicht erfasst sind (z.B. Ermittlung von Metadaten)[27]. Darüber hinaus verlangt die Prüfung nach der EMRK immer auch die Wahrung der Verhältnismäßigkeit.

9.2.3 Recht auf Datenschutz. Art. 1 § 1 DSG

> Art. 1 § 1 Datenschutzgesetz
>
> (1) Jede Person hat, insbesondere auch im Hinblick auf die Achtung ihres Privat- und Familienlebens, Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf die betreffende Person einem Geheimhaltungsanspruch nicht zugänglich sind.

Das österreichische Datenschutzgesetz (DSG) ergänzt die europäische DSGVO, die in den Mitgliedsstaaten der EU unmittelbar anwendbar ist. Zwar steht das DSG selbst nicht im Verfassungsrang, allerdings hat der Gesetzgeber das Recht auf Datenschutz (Art. 1 § 1 DSG) zur Verfassungsbestimmung erhoben, weshalb es – genauso wie die Bestimmungen im StGG, der EMRK und der GRC – im Rahmen der vorliegenden Grundrechtsanalyse zu erläutern ist.

Eingriff

Das Recht auf Schutz personenbezogener Daten im DSG erstreckt sich nur auf solche Daten, an denen ein schutzwürdiges Interesse besteht. Irrelevant ist, ob die Daten manuell oder automationsunterstützt verarbeitet werden. Allgemein verfügbare Daten sowie Daten ohne Personenbezug, die nicht auf die_den Betroffene_n rückführbar sind (z.B. anonymisierte Daten), fallen nicht in den Schutzbereich des DSG.

Personenbezogene Daten

Der ausdrücklich genannte Anspruch auf Achtung des Privat- und Familienlebens in Art. 1 § 1 Abs. 1 DSG orientiert sich an Art. 8 EMRK, welcher in Österreich im Verfassungsrang steht. Das Grundrecht auf Datenschutz ist aber konkreter als Art. 8 EMRK, da es explizit einen Anspruch auf Geheimhaltung normiert. Art. 1 § 1 DSG kann deshalb „als Erfüllung der aus Art. 8 EMRK resultierenden Schutzpflicht gedeutet werden".[28]

Recht auf Auskunft

Neben dem Recht auf Geheimhaltung beinhaltet Art. 1 § 1 Abs. 3 DSG das verfassungsrechtlich geschützte Recht auf Auskunft, um zu erfahren, welche konkreten personenbezogenen Daten verarbeitet wurden, woher diese stammen, wozu sie verwendet wurden und an wen sie gegebenenfalls übermittelt wurden.

Recht auf Löschung

Darüber hinaus können Betroffene die Berichtigung unrichtiger Daten sowie die Löschung von Daten, die unzulässigerweise verarbeitet wurden, verlangen. Eine unrechtmäßige Verarbeitung liegt vor, wenn die Daten entgegen den Bestimmungen der DSGVO oder dem DSG verarbeitet werden. Werden personenbezogene Daten manuell (d.h. nicht automationsunterstützt) verarbeitet, garantiert das nationale DSG dem_r Betroffenen nur dann ein Recht auf Löschung, wenn es sich dabei um sog. Dateien handelt (Art. 1 § 1 Abs. 3 DSG). Von Dateien spricht man, wenn Daten in besonders strukturierter Weise verarbeitet werden (Art. 4 Z. 6 DSGVO). Ein nicht strukturierter Papierakt ist daher nicht vom Grundrecht auf Löschung nach dem DSG umfasst.

Rechtfertigung

Ein Eingriff in die Rechte auf Geheimhaltung, Auskunft, Richtigstellung und Löschung ist nur erlaubt, wenn **eine der folgenden drei Voraussetzungen** nach Art. 1 § 1 Abs. 2 DSG vorliegt:

Zustimmung zur Datenverarbeitung

- Der Eingriff erfolgt mit **Zustimmung des_der Betroffenen.**

- Der Eingriff liegt im **lebenswichtigen Interesse des_der Betroffenen.** Ein Eingriff unter dieser Voraussetzung ist nur erlaubt, wenn der_die Betroffene zur eigenen Interessenwahrnehmung nicht fähig ist und eine Zustimmung nicht eingeholt werden kann, aber anzunehmen ist, dass der_die Betroffene in die Datenverarbeitung einwilligen würde.[29] Als Beispiel für einen legalen Eingriff dieser Art nennt der Verfassungsdienst des Bundeskanzler_innenamts notfallmedizinisch indizierte Eingriffe.[30]

- Der Eingriff erfolgt aufgrund **überwiegender berechtigter Interessen anderer.** In diesem Fall liegt die Notwendigkeit zur Datenverarbeitung nicht bei dem_der Betroffenen, sondern bei einer dritten Person. Das Interesse des_r Dritten an der Datenverarbeitung muss das Interesse des_der Betroffenen überwiegen.

Die genannten Eingriffsmöglichkeiten gelten sowohl bei einem Eingriff durch eine natürliche bzw. juristische Person als auch bei einem behördlichen Vorgehen. Bei behördlichen Eingriffen verlangt das DSG, dass der Eingriff auf einer gesetzlichen Grundlage beruht (sog. Gesetzesvorbehalt). Das Gesetz muss den Anforderungen von Art. 8 Abs. 2 EMRK entsprechen und daher präzise und vorhersehbar formuliert und aus den abschließend aufgezählten Gründen notwendig, d.h. verhältnismäßig sein. Das Prinzip der Verhältnismäßigkeit wird von Art. 1 § 1 Abs. 2 DSG explizit genannt, da Eingriffe „jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden [dürfen]".

9.2.4 Recht auf Schutz personenbezogener Daten und Recht auf Achtung des Privat- und Familienlebens. Art. 7 und Art. 8 GRC

> Art. 7 Europäische Grundrechtecharta
>
> Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.
>
> Art. 8 Abs. 1 Europäische Grundrechtecharta
>
> Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Der Schutz des Privat- und Familienlebens ist nicht nur in der EMRK, sondern auch in der Grundrechtscharta der Europäischen Union (GRC) verankert. Anders als die EMRK kennt die GRC ein ausdrückliches Recht auf den Schutz personenbezogener Daten (Art. 8 GRC). Das Verhältnis zwischen Art. 7 (Recht auf Achtung des Privatlebens) und Art. 8 GRC (Recht auf Schutz personenbezogener Daten) ist äußerst umstritten. Im Folgenden werden beide Grundrechte in Zusammenschau erläutert.
Die GRC hält in Art. 52 Abs. 3 GRC ausdrücklich fest, dass jene Rechte der GRC, die sich auch in der EMRK wiederfinden, die gleiche Bedeutung und Tragweite

haben, wie in der EMRK vorgesehen ist. Das Recht auf Achtung des Privat- und Familienlebens zählt zu diesen Rechten, da es sowohl in der GRC als auch in der EMRK verankert ist. Folglich beachtet der EuGH die Judikatur des EGMR als Auslegungshilfe, obwohl die EU selbst der EMRK (noch) nicht beigetreten ist. Das Recht auf Schutz personenbezogener Daten gibt es in der GRC, aber nicht ausdrücklich in der EMRK.

Eingriff

Der Schutzumfang des Rechts auf Achtung des Privatlebens nach Art. 7 GRC orientiert sich an Art. 8 EMRK, weshalb diesbezüglich auf die Ausführungen in Kapitel 9.2.1 verwiesen werden kann.

An dieser Stelle stellt sich daher prinzipiell die Frage, inwiefern sich der Anwendungsbereich von Art. 7 GRC – der Art. 8 EMRK entspricht – zu Art. 8 GRC unterscheidet. Der EuGH zog beide Grundrechte erstmals im Fall Schecke zusammen und bezeichnete sie als das „Recht auf Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten" und erfasst damit all jene Informationen, die eine bestimmte oder bestimmbare natürliche Person betreffen.

Schecke Rz 52

Das Kombinationsgrundrecht schützt „bereits im Vorfeld möglicher Verletzungen vor Gefährdungen des Privatlebens und damit der inneren Entfaltungsfreiheit, die von der Datenverarbeitung durch staatliche Stellen ausgehen".[31]

Datenschutzgrundrecht als Teilaspekt des Rechts auf Privatleben

Das Verhältnis beider Grundrechte ist als konzentrische Kreise vorstellbar, wobei das Recht auf Privatleben den größeren Kreis bildet und das Recht auf Datenschutz zur Gänze umfasst. Während das Datenschutzgrundrecht nur die unrechtmäßige Verarbeitung personenbezogener Daten erfasst, geht das Recht auf Achtung des Privatlebens über Datenverarbeitungsvorgänge hinaus. Folglich stellt jeder Eingriff in das Recht auf Schutz personenbezogener Daten zugleich auch einen Eingriff in das Recht auf Schutz des Privatlebens dar. Das Datenschutzgrundrecht bildet insofern einen Teilaspekt des Rechts auf Achtung des Privatlebens.[32]

Digital Rights Ireland Rz 33; Schrems Rz 87

Grundsätzlich stellen also alle Verarbeitungsvorgänge von personenbezogenen Daten einen Eingriff in Art. 7 und Art. 8 GRC dar.[33] Nach ständiger Rechtsprechung des EuGH ist es für das Vorliegen eines Eingriffs in Art. 7 GRC unerheblich, „ob die betreffenden Informationen über das Privatleben sensiblen Charakter haben oder ob die Betroffenen durch den Eingriff Nachteile erlitten haben könnten […]." Eine Datenverarbeitung im Sinne der Datenschutz-Grundverordnung der EU (DSGVO) liegt dann vor, wenn Daten erhoben, erfasst, organisiert, geordnet, gespeichert, angepasst oder verändert, ausgelesen, abgefragt, verwendet, durch Übermittlung offengelegt, verbreitet, abgeglichen, verknüpft, eingeschränkt, gelöscht oder vernichtet werden. Irrelevant ist, ob die Daten automationsunterstützt oder manuell verarbeitet werden. Darüber hinaus ist auch das nicht-strukturierte Sammeln von Daten ein Eingriff in das Grundrecht auf Datenschutz, womit dieses weiter reicht als die DSGVO, die nur das strukturierte Sammeln von Daten erfasst.

Datenverarbeitung im Sinne der DSGVO

Art. 4 Abs. 2 DSGVO

Art. 4 Abs. 6 DSGVO

Ein Eingriff liegt beispielsweise dann vor, wenn öffentlich zugängliche Kommunikationsdienste sowie öffentliche Kommunikationsnetze gesetzlich verpflichtet werden, personenbezogene Daten von Kund_innen auf Vorrat zu speichern (sog. Vorratsdatenspeicherung). Der behördliche Zugriff auf diese gespeicherten Daten über das Privatleben einer Person ist als zusätzlicher Eingriff zu werten und erfordert daher auch eine eigene Rechtfertigung. Darüber hinaus stellt auch das Speichern von personenbezogenen Daten durch die Behörde selbst einen Eingriff dar. Die Speicherung von Verkehrs- und Standortdaten auf Vorrat ist daher nur unter bestimmten Voraussetzungen möglich, die unten näher erörtert werden.

Digital Rights Ireland Rz 34

Digital Rights Ireland Rz 35

Vorratsdatenspeicherung

Tele2/Watson Rz 77

Tele2/Watson Rz 125

Eine weitere Form des Eingriffs in Art. 7 und Art. 8 GRC bildet die Weitergabe bzw. Übermittlung von personenbezogenen Daten an ein Nicht-EU-Land (Drittland). Der Eingriff liegt unabhängig davon vor, ob diese Daten später tatsächlich verwendet werden. Werden Daten über das Privatleben einer Person an Drittländer übermittelt, muss das Empfängerland ein gewisses Schutzniveau erfüllen, d.h. das Drittland muss das „Schutzniveau der Grundfreiheiten

Weitergabe von Daten an Drittländer

EuGH Gutachten 1/15, Rz 124 u. Rz 214

und Grundrechte gewährleisten, das dem in der Union garantierten Niveau der Sache nach gleichwertig ist". In diesem Zusammenhang ist das Urteil Schrems erwähnenswert, in dem der EuGH die *Safe-Harbor-Regelung* und die daraus erwachsende Vermutung, dass in den USA ein angemessenes Datenschutzniveau gelte, für ungültig erklärte, weil die USA keine ausreichenden Garantien für den Schutz personenbezogener Daten bieten.

Schrems Rz 34 und 82

Zusammenfassend lässt sich festhalten, dass das Datenschutzgrundrecht zum einen enger ist als das Recht auf Schutz des Privatlebens, weil es nur die Datenverarbeitung erfasst und damit einen engeren Schutzbereich hat. Gleichzeitig aber bietet das Datenschutzgrundrecht insofern einen besseren Schutz, als es in Art. 8 Abs. 2 GRC Begleitgrundrechte (Auskunfts- und Berichtigungsrecht) gibt, die das Recht auf Privatleben in Art. 7 GRC nicht enthält. Darüber hinaus sieht Art. 8 Abs. 3 GRC explizit eine unabhängige Überwachungsstelle für die Einhaltung von Art. 8 GRC vor.

Rechtfertigung

Die gesetzlichen Schranken für einen Eingriff in das Recht auf Schutz des Privatlebens sowie in das Datenschutzrecht ergeben sich – neben den Schranken des Art. 8 EMRK – aus Art. 52 Abs. 1 GRC. Demnach ist ein Eingriff nach europäischem Recht nur zulässig, wenn

- der Eingriff auf einer **gesetzlichen Grundlage** beruht,
- der **Wesensgehalt** des Grundrechts geachtet wird; d.h. der Kernbestandteil des Rechts muss erhalten bleiben, sodass die Ausübung des Rechts nicht verhindert wird[34] (bspw. würde es den Wesensgehalt von Art. 7 GRC verletzen, wenn Behörden generell auf den Inhalt elektronischer Kommunikation zugreifen dürften),

Schrems Rz 94

- der Eingriff den von der Union anerkannten dem **Gemeinwohl dienenden Zielsetzungen** oder Erfordernissen des Schutzes der Rechte und Freiheiten anderer entspricht und
- der Eingriff **verhältnismäßig** und **erforderlich** ist.

Darüber hinaus zieht die Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58, auch e-Privacy Verordnung genannt), die dem Schutz der Grundrechte nach Art. 7 und Art. 8 GRC dient, engere Grenzen als die GRC selbst. Art. 15 Abs. 1 der RL zählt nämlich abschließend auf, aus welchen spezifischen Zwecken das Recht auf Privatleben bzw. auf Datenschutz gesetzlich eingeschränkt werden darf. Bei diesen legitimen Zielen handelt es sich um die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder den unzulässigen Gebrauch von elektronischen Kommunikationssystemen.

Ausgehend vom Urteil Digital Rights Ireland über die Vorratsdatenspeicherung entwickelte der EuGH eine fundierte Rechtsprechung sowie strenge gesetzliche, zu erfüllende Mindeststandards für Gesetze, die Datenverarbeitung regeln und daher in das Recht auf Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten eingreifen. Den Schutzstandard entwickelte der EuGH insbesondere in den Urteilen Tele2 Sverige und Watson, Schrems sowie im Gutachten zum PNR-Abkommen weiter. Zu diesen Mindestanforderungen gehören in ständiger Rechtsprechung die folgenden Voraussetzungen:

Schrems Rz 91; EuGH Gutachten 1/15 Rz 39; Tele2/Watson Rz 109, 117; Digital Rights Ireland Rz 54

1. Das eingreifende Gesetz muss „klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen und Mindestanforderungen aufstellen […], so dass [Betroffene] über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor

Missbrauchsrisiken sowie vor jedem unberechtigtem Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen“. Werden personenbezogene Daten automatisch verarbeitet, ist es umso wichtiger, Garantien gegen eventuellen Missbrauch vorzusehen. Das gilt insbesondere, wenn sensible personenbezogene Daten betroffen sind.

Notwendigkeit

Der Eingriff, der durch das Gesetz legitimiert werden soll, muss auf das absolut Notwendige beschränkt sein, d.h. die betroffene Maßnahme muss in Bezug auf die legitimen Ziele angemessen und erforderlich sein. Da dies nicht der Fall war, kippte der EuGH die Regelung zur Vorratsdatenspeicherung; diese erstreckte sich „generell auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des [verfolgten] Ziels […] vorzusehen“. Dementsprechend verlangt der EuGH ein objektives Kriterium, das zwischen den zu speichernden Daten sowie dem verfolgten Ziel einen Zusammenhang herstellt, woraus folgt, dass der von der Speichermaßnahme betroffene Personenkreis (z.B. geografisch) begrenzt sein muss.

EuGH Gutachten 1/15 Rz 41; Tele2/Watson Rz 105; Digital Rights Ireland Rz 52

Digital Rights Ireland Rz 57

Objektives Kriterium

Tele2/Watson Rz 110

Weiters hat der EuGH festgestellt, dass die Speicherung von Verkehrs- und Standortdaten auf Vorrat grundsätzlich nur zulässig ist, wenn damit der Zweck der Bekämpfung schwerer Straftaten bzw. eine Beteiligung daran verfolgt wird. Darüber hinaus verlangt der EuGH ein zusätzliches objektives Kriterium, wenn den Behörden der Zugriff auf die auf Vorrat gespeicherten Daten ermöglicht werden soll. So wie bei der Datenspeicherung muss auch beim Datenzugriff dieses objektive Kriterium auf strikt begrenzte Zwecke beschränkt sein und des weiteren dazu geeignet sein, den Eingriff durch den behördlichen Zugriff sowie durch die spätere Nutzung dieser Daten zu rechtfertigen. Das Vorliegen eines objektiven Kriteriums, das die Eingriffe rechtfertigen kann, ist für die Datenspeicherung und für den Datenzugriff durch nationale Behörden separat zu beurteilen. Im Sinne des Verhältnismäßigkeitsprinzips ist der Zugang nationaler Behörden auf die auf Vorrat gespeicherten Daten grundsätzlich nur dadurch zu rechtfertigen, dass damit schwere Straftaten bekämpft werden sollen. Im Urteil Ministerio Fiscal hat der EuGH aber festgestellt, dass ein behördlicher Zugriff auf die gespeicherten Daten auch bei Straftaten, die nicht als schwer einzustufen sind, gerechtfertigt sein kann, wenn der Eingriff selbst nicht als schwer einzustufen ist. Ein nicht schwerer Eingriff liegt beispielsweise dann vor, wenn lediglich auf solche Daten zugegriffen wird, aus denen sich „keine genauen Schlüsse auf das Privatleben der [betroffenen] Personen ziehen [lassen]“.

Datenspeicherung und Datenzugriff: separate Beurteilung

Schrems Rz 93

Tele2/Watson Rz 115

Ministerio Fiscal Rz 60

2. Werden personenbezogene Daten verarbeitet, verlangt der EuGH, dass jeder Zugang nationaler Behörden auf diese gespeicherten Daten einem unabhängigen Aufsichtsmechanismus unterliegen muss. Konkret fordert der EuGH eine „vorherige Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung den Zugang zu den Daten und deren Nutzung auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken soll“.

Unabhängiger Aufsichtsmechanismus

Digital Rights Ireland Rz 62; EuGH Gutachten 1/15 Rz 41

Selbiges gilt, wenn personenbezogene Daten an ein Nicht-EU-Land (Drittland) weitergegeben werden sollen, wie das beispielsweise im PNR-Abkommen mit Kanada vorgesehen war (siehe Fallbeispiel weiter unten). Wollen daher die Behörden des Drittlandes auf die von den Flugunternehmen gespeicherten Daten zugreifen, ist dieser behördliche Zugriff zuvor einer Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle zu unterziehen.

Nur wenn ein Gesetz, das die Verarbeitung personenbezogener Daten vorsieht, die genannten Kriterien erfüllt, ist es mit der GRC vereinbar. Die Wichtigkeit des vom EuGH verlangten objektiven Kriteriums, das einen Zusammenhang zwischen den zu verarbeitenden personenbezogenen Daten und dem verfolgten legitimen Ziel herstellen soll, wird anhand folgenden Beispiels gezeigt. Nur wenn dieses objektive Kriterium gegeben ist, beschränkt sich der Eingriff in die Grundrechte nach Art. 7 und Art. 8 GRC auf das absolut Notwendige und ist damit rechtfertigbar.

EuGH Gutachten 1/15 Rz 202

Fallbeispiel: Geplantes Abkommen zwischen Kanada und der Europäischen Union hinsichtlich der Übermittlung von Fluggastdatensätzen aus der Union nach Kanada (PNR-Abkommen)

Das geplante Abkommen über die Fluggastdatenspeicherung mit Kanada sah vor, dass die PNR-Daten sämtlicher Fluggäste selbst nach deren Ausreise aus Kanada dauerhaft gespeichert werden dürften. Nämlich selbst dann, wenn sich während der Aufenthaltsdauer in Kanada keine objektiven Anhaltspunkte ergeben haben, dass von der betroffenen Person eine Gefahr im Zusammenhang mit der Bekämpfung von Terrorismus und grenzüberschreitender schwerer Kriminalität ausgeht (vgl. Rz. 205).
Der EuGH argumentierte, dass ohne derartige Anhaltspunkte kein objektives Kriterium bestünde, das einen Zusammenhang zwischen den zu verarbeitenden Daten und dem verfolgten legitimen Ziel herstelle. Die geplante Regelung ging daher über das absolut Notwendige hinaus und wurde vom EuGH gekippt.

9.3 Freiheit der Meinungsäußerung

Das Recht auf Meinungsfreiheit bildet einen der „Grundpfeiler einer demokratischen Gesellschaft“, da es gewährleistet, dass sich Menschen frei von staatlicher Einflussnahme eine Meinung bilden und diese auch frei äußern können. Dadurch sollen demokratische Werte wie Toleranz, Pluralismus und Weltoffenheit gewahrt bleiben.[35]

Handyside Rz 38

Eine weitreichende Überwachung von Verhalten und Kommunikation begünstigt ein Klima, in dem Menschen sich in ihrer Meinungsäußerungsfreiheit sowie im Konsum von – selbst legaler – Information zur Meinungsbildung selbst beschränken. Diese Selbstbeschränkung wird auch als chilling effect – eine potentiell abschreckende Wirkung für Bürger_innen – bezeichnet.[36] Diese Gefahr besteht insbesondere dann, wenn der von der Überwachungsmaßnahme betroffene Personenkreis nur vage definiert ist und nur schwache Kontroll- und Rechtsschutzmechanismen vorhanden sind. Im Rahmen der vorliegenden Grundrechtsanalyse ist es daher notwendig, nicht nur die Auswirkungen von Überwachungsgesetzen auf das Grundrecht auf Achtung des Privatlebens sowie auf das Grundrecht auf Datenschutz zu analysieren, sondern auch damit zusammenhängende Eingriffe in das Recht auf Meinungsfreiheit zu untersuchen.
Die Freiheit der Meinungsäußerung wird in der EMRK, im StGG und in der GRC geschützt, die jeweiligen Artikel werden im vorliegenden Kapitel ausgeführt.

9.3.1 Art 10 EMRK

> Art. 10 EMRK
>
> (1) Jede Person hat Anspruch auf freie Meinungsäußerung. Dieses Recht schließt die Freiheit der Meinung und die Freiheit zum Empfang und zur Mitteilung von Nachrichten oder Ideen ohne Eingriffe öffentlicher Behörden und ohne Rücksicht auf Landesgrenzen ein. Dieser Artikel schließt nicht aus, dass ein Staat ein Rundfunk-, Lichtspiel- oder Fernsehunternehmen einem Genehmigungsverfahren unterwirft.

Eingriff

Meinungs- und Pressefreiheit

Das in der EMRK verbürgte Recht auf Meinungsfreiheit umfasst sowohl das Recht Informationen zu empfangen als auch weiterzugeben und erfasst grundsätzlich Werturteile sowie Tatsachenaussagen. Lediglich Informationen, „die sich gegen die der Konvention zugrunde liegenden Werte richten, wie insb. rassistische Hassreden oder politischer Extremismus“[37] fallen nicht in den Schutzbereich von Art. 10 EMRK. Anders als das Recht auf Achtung des Privatlebens – das die Vertraulichkeit von Informationen schützt – schützt das Recht auf Meinungsfreiheit den Inhalt selbst.[38] Für die Anwendbarkeit von Art. 10 EMRK ist deshalb irrelevant, ob es sich um geheime oder öffentlich zugängliche Informationen handelt.[39]

Vgl. VfSlg 11.297

Art. 10 EMRK schützt aber nicht nur den Empfang und die Weitergabe von Nachrichten, sondern auch das Beschaffen und Ermitteln von öffentlich zugänglichen Informationen zum Zweck der Verbreitung. Es liegt daher ein Eingriff in Art. 10 EMRK vor, wenn ein Staatsorgan die Informationsbeschaffung behindert (z.B. durch die Zerstörung von Informationsmaterial wie Filmen).

Telegraaf Rz 127

Auch die Pressefreiheit fällt unter Art. 10 EMRK. Der EGMR bezeichnet die Funktion von unabhängigen Massenmedien als *public watchdog* und betont damit ihre öffentliche Kontrollfunktion. Medien müssen von staatlicher Einflussnahme unabhängig sein, um einen demokratischen pluralistischen Meinungsaustausch zu gewährleisten. Insbesondere müssen journalistische Quellen geschützt und vertraulich behandelt werden. Das Redaktionsgeheimnis genießt folglich einen hohen Stellenwert. Widrigenfalls könnten potentielle Informant_innen abgeschreckt werden und in Folge der Presse keine Informationen mehr weitergeben, die von öffentlichem Interesse sind *(chilling effect)*.

Individuelle vs. strategische Überwachung

Weber Rz 145

In Zusammenhang mit staatlichen Überwachungsmaßnahmen bedeutet das, dass ein Eingriff in Art. 10 EMRK beispielsweise dann vorliegt, wenn aufgrund der Überwachung des Fernmeldeverkehrs „journalistische Quellen entweder offen gelegt oder [Fernmeldebeziehungen] davon abgehalten würden, anzurufen oder über das Telefon Informationen zu übermitteln“. Für das Vorliegen eines Eingriffs ist grundsätzlich unerheblich, ob es sich dabei um eine individuelle Überwachung (d.h. eine Überwachung bestimmter Personen) oder eine strategische Überwachung (d.h. eine Überwachung des gesamten Fernmeldeverkehrs, um Informationen zu sammeln und so ernste Gefahren für den Staat zu erkennen und abzuwenden) handelt. Da die strategische Überwachung aber nicht gezielt darauf ausgerichtet ist, journalistische Quellen aufzudecken, ist der Eingriff in Art. 10 EMRK nicht als besonders schwer zu werten. Eine ähnliche Unterscheidung trifft der EGMR übrigens auch dann, wenn der Wohnort oder der Arbeitsplatz von Journalist_innen polizeilich durchsucht wird: Der Eingriff in Art. 10 EMRK wiegt schwerer, wenn die Durchsuchung mit dem Zweck vollzogen wird, journalistische Quellen aufzudecken. Erfolgt die Durchsuchung aus Gründen, die nicht mit der journalistischen Tätigkeit in Zusammenhang stehen, ist der Eingriff in Art. 10 EMRK nicht als schwer einzustufen.

Journalistische Quellen

Weber Rz 151

Roemen Rz 52

Nicht nur Massenmedien erfüllen eine *public watchdog*-Rolle. Im Fall Big Brother Watch hat der EGMR mehreren NGOs, die sich für Bürger_innenrechte und Datenschutz einsetzen, eine ähnlich wichtige Rolle wie der Presse zugesprochen. Die besonderen Schutzvorkehrungen für Journalist_innen zum Schutz der Pressefreiheit sowie zum Schutz von Informant_innen im Rahmen des Art. 10 EMRK waren im konkreten Fall daher auch für die betroffenen NGOs anwendbar.

Big Brother Watch Rz 469

Auch das bloße Speichern von Daten über politische Meinungen, Zugehörigkeiten und Aktivitäten durch die Geheimpolizei in Schweden wurde vom EGMR als Eingriff in das Recht auf Freiheit der Meinungsäußerung und das Recht auf Versammlungsfreiheit gewertet.

Rechtfertigung

Ähnlich wie Art. 8 EMRK unterliegt auch Art. 10 EMRK einem materiellen Gesetzesvorbehalt, d.h. ein Eingriff in das Recht auf Meinungsfreiheit ist nur gerechtfertigt, wenn er gesetzlich vorgesehen ist und aufgrund einer der in Art. 10 Abs. 2 EMRK taxativ aufgezählten Gründe ergeht. Bei den legitimen Zielen handelt es sich um die nationale Sicherheit, die territoriale Unversehrtheit oder die öffentliche Sicherheit, die Aufrechterhaltung der Ordnung und die Verbrechensverhütung, den Schutz der Gesundheit und der Moral, den Schutz des guten Rufes und der Rechte anderer.

Darüber hinaus muss der Eingriff in das Recht auf Meinungsfreiheit in einer demokratischen Gesellschaft notwendig sein. In Anbetracht des hohen Stellenwertes der Pressefreiheit für die demokratische Gesellschaft verlangt der EGMR, dass der Eingriff „durch ein vorrangiges, das öffentliche Interesse betreffende Erfordernis gerechtfertigt ist“. Der Prüfung der Verhältnismäßigkeit kommt daher eine besonders hohe Relevanz zu. Je schwerwiegender der Eingriff in Art. 10 EMRK ist, desto stärker müssen die gesetzlichen Schutzvorkehrungen sein.

Weber Rz 149; Big Brother Watch Rz 488

Da der Eingriff in Art. 10 EMRK bei individuellen Überwachungsmaßnahmen schwerer ist als bei strategischen Überwachungsmaßnahmen, stellt der EGMR dementsprechend höhere Anforderungen an die Regelungen zum Schutz der Pressefreiheit sowie zum Schutz von Informant_innen. Konkret fordert der EGMR bei individuellen Abhörmaßnahmen von Journalist_innen, dass diese zuvor von einer unabhängigen Stelle genehmigt werden.

> Fallbeispiel: Weber und Saravia gegen Deutschland
>
> Im Fall Weber und Saravia setzte sich der EGMR mit der Frage auseinander, ob die strategische Überwachung des Fernmeldeverkehrs in das Recht auf Pressefreiheit (Art. 10 EMRK) eine_r Journalist_in ungerechtfertigt eingreife. Der EGMR räumte zwar ein, dass das eingreifende nationale Gesetz keine besonderen Schutzvorkehrungen im Hinblick auf die Pressefreiheit sowie den Informant_innenschutz beinhaltete. Aufgrund der strategischen Überwachung sei der Eingriff aber nicht als schwer einzustufen, da die Sicherheitsbehörden nur bei einer Überprüfung des abgehörten Materials davon Kenntnis erlangen, dass überhaupt Gespräche von Journalist_innen abgehört wurden (vgl. Rz 151).
>
> Es handelt sich daher um einen gerechtfertigten Eingriff in Art. 10 EMRK – und damit in die Pressefreiheit –, weil der Eingriff „zum Erreichen der legitimen Ziele erforderlich war“ und „die Offenlegung journalistischer Quellen auf ein unvermeidbares Mindestmaß“ beschränkt wurde. Folglich wertete der EGMR den Eingriff als verhältnismäßig und somit als gerechtfertigt (vgl. Rz 152).

Exkurs: Whistleblower_innen

Whistleblower_in

Im Zusammenhang mit der Verfolgung von Whistleblower_innen hat der EGMR eine fundierte Rechtsprechung entwickelt. Drohen einem_einer Whistleblower_in – in diesem Fall in der Position einer öffentlich bediensteten Person, die geheime wichtige Informationen von hohem allgemeinen Interesse veröffentlicht – Sanktionen, liegt grundsätzlich ein Eingriff in das Recht auf Meinungsfreiheit vor, da sowohl der Empfang als auch die Weitergabe grundrechtlich geschützt sind (siehe oben). Die folgenden Punkte sind für die Beurteilung, ob ein Eingriff in Art. 10 EMRK gerechtfertigt ist, maßgeblich:

Meinungsfreiheit

Guja Rz 70–78

- Die betroffene Person hatte keine andere Möglichkeit auf den Missstand hinzuweisen (Rz 73),
- die veröffentlichte Information ist von öffentlichem Interesse (Rz 74),
- die veröffentlichte Information ist authentisch (Rz 75),
- das öffentliche Interesse an der Information muss größer sein als der allfällige Schaden, der der betroffenen Institution aufgrund der Veröffentlichung zugefügt wurde (Rz 76),
- der_die Whistleblower_in muss gutgläubig und in der Annahme gehandelt haben, dass die Information echt ist, die Veröffentlichung von allgemeinem Interesse ist, und es keine anderen – diskreteren – Mittel gab, den Missstand zu beseitigen (Rz 77) und
- der staatliche Eingriff muss verhältnismäßig sein (Rz 78).

Nur wenn eine Zusammenschau der dargelegten Punkte ergibt, dass das Interesse des Staates an der Geheimhaltung der veröffentlichten Informationen größer wiegt als das öffentliche Interesse an der Veröffentlichung, ist der Eingriff in Art. 10 EMRK gerechtfertigt und die Veröffentlichung der geheimen Informationen darf somit sanktioniert werden.

9.3.2 Art. 13 StGG

> Art. 13 StGG
>
> Jede Person hat das Recht, durch Wort, Schrift, Druck oder durch bildliche Darstellung ihre Meinung innerhalb der gesetzlichen Schranken frei zu äußern.
> Die Presse darf weder unter Zensur gestellt, noch durch das Concessions-System beschränkt werden. Administrative Postverbote finden auf inländische Druckschriften keine Anwendung.

Da der Schutzbereich des Art. 10 EMRK weit über den Schutzbereich des Art. 13 StGG hinausgeht, hat Art. 13 StGG seine eigenständige Relevanz in Österreich praktisch verloren.[40] Lediglich das absolute Verbot der Zensur – konkret der Vorzensur – geht über Art. 10 EMRK hinaus, weil es unter keinem Gesetzesvorbehalt steht und damit unbeschränkbar ist. Eine Nachzensur (z.B. Strafen) ist im Rahmen der Grenzen von Art. 10 Abs. 2 EMRK zulässig.

Vgl. VfSlg 1829, 1830, 2987, 3910, 6615.

9.3.3 Art. 11 GRC

> Art. 11 GRC
>
> (1) Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben.
>
> (2) Die Freiheit der Medien und ihre Pluralität werden geachtet.

Das Recht auf Meinungs- und Informationsfreiheit in der GRC entspricht dem Schutzbereich des Art. 10 EMRK, weshalb auf die dortigen Ausführungen verwiesen wird. Die beiden Grundrechte unterscheiden sich nur dadurch, dass die GRC die Verpflichtung zur Achtung der Freiheit und Vielfalt der Medien explizit nennt, während die EMRK diese Pflicht nur implizit zum Ausdruck bringt.[41]

Versammlungsfreiheit stützt die Meinungsfreiheit

9.4 Versammlungsfreiheit

Das Recht auf Versammlungsfreiheit dient dem Schutz der Meinungsfreiheit. Diese hätte eine sehr beschränkte Reichweite, dürfte man sich zur Manifestation von Ideen und Überzeugungen nicht kollektiv versammeln. Folglich gehört auch die Versammlungsfreiheit zu den Grundpfeilern einer demokratischen Gesellschaft.[42]
Ähnlich wie beim Recht auf Meinunsgfreiheit hat eine polizeiliche Überwachung von Versammlungen potentiell einen sog. *chilling effect*, woraufhin Menschen aufgrund der einschüchternden Wirkung von Überwachung freiwillig auf die Ausübung ihrer Grundrechte verzichten bzw. sich in ihrer Ausübung beschränken, ohne dass der Staat den_die Einzelne_n aktiv daran hindert. Im Folgenden werden die in der EMRK, dem StGG und der GRC vom Versammlungsrecht gesteckten Grenzen für staatliche Überwachung näher beleuchtet.

9.4.1 Art. 11 EMRK

> Art. 11 EMRK
>
> (1) Alle Menschen haben das Recht, sich friedlich zu versammeln und sich frei mit anderen zusammenzuschließen, einschließlich des Rechts, zum Schutze ihrer Interessen Gewerkschaften zu bilden und diesen beizutreten.

Eine Versammlung iSd. Art. 11 EMRK liegt dann vor, wenn sich mehrere Personen organisiert mit dem gemeinsamen Ziel zusammenfinden, an einem kommunikativen Prozess teilzunehmen. Geschützt sind nur jene Veranstalter_innen und Teilnehmer_innen, die sich friedlich verhalten.[43]

Eingriff

Von einem Eingriff in die Versammlungsfreiheit ist jedenfalls dann die Rede, wenn durch unmittelbare behördliche Maßnahmen auf das Versammlungsrecht eingewirkt wird (z.B. durch Untersagung, Auflösung oder Beschränkungen bzgl. Zeit und/oder Ort). Weil der EGMR seinen Beurteilungen zu Art. 11 EMRK einen weiten Eingriffsbegriff zugrunde legt, können aber auch mittelbare Maßnahmen einen Eingriff begründen.[44] In einem solchen Fall findet die Versammlung zwar auf die vorgesehene Art und Weise statt und das Versammlungsrecht kann grundsätzlich ausgeübt werden, der Staat wirkt aber durch abschreckende („chilling“) oder beeinträchtigende („affecting“) Maßnahmen auf den Willen der Demonstrierenden ein.

Gewerkschaft der Polizei in der Slowakei Rz 60

Disk Rz 22

Zu diesen mittelbaren Maßnahmen zählt die polizeiliche Überwachung von Versammlungen durch erkennbare und nicht erkennbare Polizeipräsenz sowie durch die Verwendung von Bild- und/oder Tonaufnahmegeräten. Seit dem Frühjahr 2019 hat die Polizei im Regeldienst Body Worn Cameras im Einsatz, die gemäß § 13a Abs. 3 SPG dem Dokumentationszweck dienen sollen. Als Teil der

Polizeiliche Überwachung von Versammlungen

Body Worn Cameras

Wirkt lenkend und abschreckend statt nur zum Dokumentationszweck

Gefahrenabwehr haben diese polizeilichen Überwachungsbefugnisse aber nicht nur einen Dokumentationszweck sondern auch eine Lenkungsfunktion, weil sie auf die Unterlassung von Straftaten gerichtet sind; offene Kameras wirken repressiv und als staatliche „Machtverstärker“[45]. In vielen Ländern, darunter Großbritannien und Ungarn, werden zur Überwachung von Versammlungen nicht nur offline sondern bereits auch digitale Überwachungstechnologien (z.B. Gesichtserkennung) eingesetzt.[46]

Die abschreckende Wirkung von polizeilicher Überwachung ist letztlich auch dazu geeignet, über die direkte Abwehr von Gefahren hinauszugehen: Ihr *chilling effect* kann zur Folge haben, dass sich Einzelne in ihrer Ausübung des Versammlungsrechts selbst beschränken. Das betrifft zum einen Versammlungsteilnehmer_innen, aber insbesondere auch potentielle Demonstrationsveranstalter_innen, die unter noch größerer Beobachtung stehen und daher davor zurück schrecken könnten, führende Aufgaben zu übernehmen. Durch die polizeiliche Überwachung wird daher insgesamt das Mobilisieren sozialer Bewegungen erschwert. Nicht zuletzt auch deshalb, weil die intensive und offenkundige Überwachung von Versammlungen dazu geeignet ist, diese in ein kriminelles oder extremistisches Licht zu rücken und Versammlungen dadurch zu delegitimieren.[47]

Catt

Obwohl der EGMR den mittelbaren Grundrechtseingriff durch abschreckende und beeinträchtigende Maßnahmen bereits anerkannt hat, hat er es bis dato verabsäumt, einen Eingriff in die Versammlungsfreiheit aufgrund von polizeilichen Überwachungsmaßnahmen festzustellen. So wurde beispielsweise im Fall Catt die Sammlung von Daten über einen regelmäßigen Demonstrationsteilnehmer lediglich im Rahmen des Rechts auf Privatsphäre (Art. 8 EMRK) beurteilt, nicht aber der damit einhergehende mittelbare Eingriff in das Versammlungsrecht thematisiert. Die Überwachung von Versammlungen einzig aufgrund von Art. 8 EMRK zu beurteilen ist für Betroffene problematisch, weil Art. 8 EMRK nur jene Daten schützt, die nicht allgemein verfügbar sind. Ein Eingriff in Art. 8 EMRK liegt bei öffentlichen Daten nur dann vor, wenn diese systematisch gesammelt werden.

VG Berlin 5.7.2010, VG 1 K 905.09 Rz 16f

Entsprechend eines weiten Eingriffsverständnisses hat das Verwaltungsgericht Berlin die Videoüberwachung einer friedlichen Versammlung aufgrund seiner Abschreckungswirkung als Eingriff gewertet. Diese sei dazu geeignet, dass Menschen von einer Teilnahme absehen oder sich zu bestimmten Verhaltensweisen zwingen, wodurch letztlich auf den demokratischen Meinungsbildungsprozess eingewirkt werde. Für die Qualifikation als Eingriff ist dabei irrelevant, ob die polizeilichen Aufnahmen gespeichert werden, da ein etwaiger Speichervorgang für die einzelnen Teilnehmer_innen nicht erkennbar ist und somit dieselbe Wirkung wie im Falle des Nicht-Speicherns entfalten wird.

Rechtfertigung

Liegt ein Eingriff in das Versammlungsrecht nach Art. 11 EMRK vor, müssen die Grenzen des materiellen Gesetzesvorbehalts nach Art. 11 Abs. 2 EMRK eingehalten werden, damit der Eingriff zulässig ist. Es braucht daher eine gesetzliche Grundlage, die zugänglich und vorhersehbar ist. Darüber hinaus muss der Eingriff einem legitimen Zweck dienen, wobei ausschließlich die nationale oder öffentliche Sicherheit, die Aufrechterhaltung der Ordnung oder Verhütung von Straftaten, der Schutz der Gesundheit oder der Moral, oder der Schutz der Rechte und Freiheiten Anderer in Frage kommen. Als dritte und letzte Voraussetzung muss die eingreifende Maßnahme in einem angemessenen Verhältnis zum verfolgten legitimen Ziel sein. Aufgrund der besonderen Bedeutung des Rechts auf Versammlungsfreiheit für eine demokratische Gesellschaft hat eine Rechtfertigungsprüfung eines Eingriffs in Art. 11 EMRK mit besonders hoher Sorgfalt zu geschehen.

➲ *9.2.1 Recht auf Achtung des Privat- und Familienlebens. Art. 8 EMRK*

In Österreich ist es einfachgesetzlich (d.h. durch Gesetze geregelt, nicht aber in der Verfassung verankert) erlaubt, Übersichtsaufnahmen von Versammlungen mit Mastkameras anzufertigen, sofern ein gefährlicher Angriff gegen Leben, Gesundheit oder Eigentum von Menschen droht (§ 54 Abs. 5 SPG). Die Gefährdungsprognose wird ex ante erstellt, und wenn konkrete Anhaltspunkte für Gefahren bestehen, ist ein polizeiliches Filmen der Versammlung möglich, sofern die Aufzeichnung zuvor angekündigt wurde. Das Einschalten der Körperkameras, die – anders als Mastkameras – eine konkrete Person filmen, ist nur dann erlaubt, wenn die Polizist_innen Befehls- und Zwangsgewalt (z.B. Wegweisung) ausüben und die Aufzeichnung angekündigt wird. Das schlichte Fotografieren und Videoaufzeichnen durch Beamt_innen stellt übrigens keine Ausübung von Befehls- und Zwangsgewalt dar, sondern bildet ein sog. schlicht hoheitliches Handeln. Die durch die Körperkameras ermittelten personenbezogenen Daten dürfen nur zur Verfolgung von strafbaren Handlungen ausgewertet werden (§ 13a Abs. 3 SPG). Neben diesen beiden offenen Überwachungsbefugnissen hat die Polizei gem. § 54 Abs. 4 SPG die Möglichkeit, personenbezogene Daten mit Bild- und Tonaufzeichnungsgeräten geheim zu ermitteln, wenn sonst die Aufgabe, also die Abwehr gefährlicher Angriffe, gefährdet oder erheblich erschwert wäre.[48] Dieselbe Voraussetzung kennt das Gesetz für den Fall, dass sich Polizist_innen in Zivil unter die Demonstrierenden mischen und personenbezogene Daten durch Beobachten (Observation) ermitteln (§ 54 Abs. 2 SPG).

Die polizeilichen Überwachungsbefugnisse halten zwar einzeln gesehen einer Rechtfertigungsprüfung stand, die Summe der Maßnahmen ändert aber auch deren Qualität und Eingriffsintensität. Die österreichische Polizei hat bereits Befugnisse und Instrumente, die dazu geeignet sind, Bürger_innen von der Ausübung des Grundrechts auf Versammlungsfreiheit abzuhalten. Das Primat der Sicherheit und die stetige Ausweitung von Polizeibefugnissen bewirken, dass das Versammlungsrecht zunehmend hinter Interessen einer vermeintlichen Erhöhung der Sicherheit (sog. Versicherheitlichung) zurücktreten muss. Im Sinne einer Grundrechtspolitik, die Grundrechte als Abwehrrechte gegen den Staat versteht, wäre es dagegen angebracht, Überwachungsbefugnisse bei Versammlungen nicht weiter auszudehnen. Darüber hinaus wäre es besonders wünschenswert, dass der EGMR die intensive Überwachung von Versammlungen als das anerkennt, was sie ist; nämlich eine abschreckende Maßnahme, die mittelbar dazu geeignet ist, von einer vollständigen Ausübung der Versammlungsfreiheit abzusehen.

9.4.2 Art. 12 StGG

> Art. 12 StGG
>
> Die österreichischen Staatsbürger_innen haben das Recht, sich zu versammeln und Vereine zu bilden. Die Ausübung dieser Rechte wird durch besondere Gesetze geregelt.

Im Wesentlichen garantiert das österreichische StGG dieselben Versammlungs- und Vereinsrechte wie die EMRK, weshalb auf die obigen Ausführungen verwiesen werden kann. Wie auch der EGMR hat der österreichische VfGH bis dato Überwachungsmaßnahmen von Versammlungen nicht im Rahmen der Versammlungsfreiheit, sondern lediglich im Rahmen des Rechts auf Privatsphäre geprüft.[49]

9.4.3 Art. 12 GRC

> Art. 12 GRC
>
> (1) Jede Person hat das Recht, sich insbesondere im politischen, gewerkschaftlichen und zivilgesellschaftlichen Bereich auf allen Ebenen frei und friedlich mit anderen zu versammeln und frei mit anderen zusammenzuschließen, was das Recht jeder Person umfasst, zum Schutz ihrer Interessen Gewerkschaften zu gründen und Gewerkschaften beizutreten.

Die Versammlungsfreiheit in der GRC wurde in inhaltlicher Entsprechung zu Art. 11 EMRK formuliert[50], sodass auch hierzu auf die obigen Ausführungen verwiesen werden kann.

9.5 Recht auf ein faires Verfahren. Art. 6 EMRK

Art. 6 EMRK

(1) Jede Person hat Anspruch darauf, dass ihre Sache in billiger Weise öffentlich und innerhalb einer angemessenen Frist gehört wird, und zwar von einem unabhängigen und unparteiischen, auf Gesetz beruhenden Gericht, das über zivilrechtliche Ansprüche und Verpflichtungen oder über die Stichhaltigkeit der gegen sie erhobenen strafrechtlichen Anklage zu entscheiden hat. Das Urteil muss öffentlich verkündet werden, jedoch kann die Presse und die Öffentlichkeit während der gesamten Verhandlung oder eines Teiles derselben im Interesse der Sittlichkeit, der öffentlichen Ordnung oder der nationalen Sicherheit in einem demokratischen Staat ausgeschlossen werden, oder wenn die Interessen von Jugendlichen oder der Schutz des Privatlebens der Prozessparteien es verlangen, oder, und zwar unter besonderen Umständen, wenn die öffentliche Verhandlung die Interessen der Rechtspflege beeinträchtigen würde, in diesem Fall jedoch nur in dem nach Auffassung des Gerichts erforderlichen Umfang.

(2) Bis zum gesetzlichen Nachweis seiner Schuld wird vermutet, dass der_die wegen einer strafbaren Handlung Angeklagte unschuldig ist.

Unschuldsvermutung

(3) Jede angeklagte Person hat mindestens (englischer Text) insbesondere (französischer Text) die folgenden Rechte:

a) in möglichst kurzer Frist in einer für sie verständlichen Sprache in allen Einzelheiten über die Art und den Grund der gegen sie erhobenen Beschuldigung in Kenntnis gesetzt zu werden;

b) über ausreichende Zeit und Gelegenheit zur Vorbereitung ihrer Verteidigung zu verfügen;

c) sich selbst zu verteidigen oder den Beistand eines Verteidigers ihrer Wahl zu erhalten und, falls sie nicht über die Mittel zur Bezahlung eine_r Verteidiger_in verfügt, unentgeltlich den Beistand eine_r Pflichtverteidiger_in zu erhalten, wenn dies im Interesse der Rechtspflege erforderlich ist;

d) Fragen an die Belastungszeug_innen zu stellen oder stellen zu lassen und die Ladung und Vernehmung der Entlastungszeug_innen unter denselben Bedingungen wie die der Belastungszeug_innen zu erwirken;

Recht auf Dolmetscher_in bei fremder Verhandlungssprache

e) die unentgeltliche Beiziehung eine_r Dolmetscher_in zu verlangen, wenn der_die Angeklagte die Verhandlungssprache des Gerichts nicht versteht oder sich nicht darin ausdrücken kann.

Mit Art. 6 EMRK wurden wesentliche Verfahrensgarantien in das österreichische Verfassungsrecht aufgenommen, die jedem Menschen ein faires Zivil- bzw. Strafverfahren garantieren sollen. Damit ein Verfahren fair ist, muss insbesondere das Gebot der Rechtsstaatlichkeit gewahrt sein, und Gerichte dürfen nicht willkürlich agieren. Außerdem müssen den Betroffenen angemessene

Mitwirkungsrechte zukommen und gerichtliche Entscheidungen sind in einer angemessenen Frist zu erledigen. Weiteres Kernelement eines fairen Verfahrens ist die Waffen- und Chancengleichheit aller Beteiligten.[51] Art. 6 Abs. 2 und 3 EMRK enthalten bestimmte Rechte, die jedenfalls in einem Strafverfahren zu gelten haben und damit jede_r Angeklagten zukommen. Im Zusammenhang mit Überwachungsmaßnahmen – insbesondere verdeckten Ermittlungen – besteht die Gefahr, dass Verfahrensgarantien ausgehöhlt und verletzt werden. Im Folgenden werden die im Zusammenhang mit Überwachungsmaßnahmen relevanten Bestimmungen hervorgehoben und analysiert.

Eingriff

Zentraler Grundsatz eines fairen Verfahrens ist der sog. Nemo-tenetur-Grundsatz, also das Recht, als Angeklagte_r zu schweigen und sich nicht selbst strafrechtlich belasten zu müssen. Zwar wird die Selbstbelastungsfreiheit nicht ausdrücklich von Art. 6 EMRK genannt, sie ergibt sich aber aus dem Grundsatz auf ein faires Verfahren und steht auch im Zusammenhang mit der in Art. 6 Abs. 2 EMRK verfassungsgesetzlich garantierten Unschuldsvermutung.[52] Sah der EGMR zunächst das Recht auf Selbstbelastungsfreiheit nur dann verletzt, wenn direkter und willensbeugender Zwang von den Behörden ausgeübt wurde[53], erweiterte der EGMR mit dem Fall Allan sein Verständnis vom Schweigerecht und setzte verdeckten Ermittlungsbefugnissen engere Grenzen. In Allan setzte sich der EGMR mit der Frage auseinander, ob es fair im Sinne des Art. 6 EMRK sei, wenn ein Spitzel in der Zelle einer verdächtigen Person, die bis dahin in ordentlichen Vernehmungen zum Vorwurf des Mordverdachts geschwiegen hatte, untergebracht wird, um deren Vertrauen und in Folge ein Geständnis zu erlangen. Um diese Frage zu beantworten, entwickelte der EGMR zwei Kriterien, bei deren Vorliegen die (aktive) verdeckte Ermittlung rechtswidrig war:

1. Staatliche_r Agent_in: Ist die relevante Unterhaltung zwischen Informant_in und beschuldigter Person im Auftrag der Behörde zustande gekommen, ist der_die Informant_in als staatliche_r Agent_in zu werten. Irrelevant ist, ob es sich dabei um eine_n behördliche_n Mitarbeiter_in oder eine Privatperson (z.B. Vertraute_r des_der Verdächtigen) handelt. Ausschlaggebend ist einzig der Umstand, ob die selbstbelastenden Aussagen in einem Gespräch getätigt wurden, das von der Behörde gesteuert wurde.

Allan Rz 51

2. Funktionale Einvernahme: Eine vernehmungsgleiche Befragung liegt vor, wenn der_die staatliche Informant_in die Drucksituation des_der Beschuldigten nutzt, in der diese_r besonders beeinflussbar ist, und das Geständnis durch hartnäckige Fragen herbeiführt. Das Vorliegen einer besonderen Drucksituation hat der EGMR bis dato aber nur in Haftsituation angenommen. In Fällen, in denen staatliche Informant_innen das Geständnis herbeigeführt haben, die verdächtige Person aber auf freiem Fuß war, hat der EGMR keine Drucksituation erkannt und das Geständnis daher als freiwillige Willensentscheidung gewertet.

Drucksituation, Entscheidungsfreiheit

Allan Rz 52

Heglas, Bykov

Liegen diese beiden Voraussetzungen vor, geht der EGMR nicht von einem freiwilligen Geständnis aus, sondern von einer Verletzung des Fairnessgebots nach Art. 6 EMRK, weil eine funktionale Einvernahme ohne Einhaltung der Belehrungspflichten über Beschuldigtenrechte stattgefunden hat. Zwar wird in einem solchen Fall der Wille und die Entscheidungsfreiheit der verdächtigen Person nicht direkt gebrochen, die Polizei handelt aber listig und damit rechtswidrig, um den Willen des_der Verdächtigen zu umgehen.[54] Weil der EGMR die Selbstbelastungsfreiheit mit den oben zitieren Fällen Heglas und Bykov auf Drucksituationen beschränkt hat, ist die einfachgesetzliche Grundlage in Österreich für Betroffene günstiger, weil § 5 Abs. 3 StPO das Verlocken zu einem Geständnis

Heimliche Überwachung

durch heimlich bestellte Personen insgesamt für rechtswidrig erklärt, ohne dass es auf das Vorliegen einer Drucksituation ankommt.
Liegt dagegen gar keine Befragung des_der Verdächtigen vor, sondern handelt es sich um eine passive verdeckte Ermittlung (z.B. Überwachung von Telefon, E-Mail, Räumlichkeiten etc.), ohne dass ein_e staatliche_r Informant_in Druck auf die verdächtige Person ausübt, wird Art. 6 EMRK gar nicht berührt. Hier tätigt die verdächtige Person die selbstbelastende Aussage freiwillig, wird dabei aber heimlich aufgezeichnet. Weil es sich dabei aber um einen Eingriff in die Privatsphäre handelt, prüft der EGMR, ob die Überwachungsmaßnahme den Erfordernissen des Art. 8 Abs. 2 EMRK genügt. Eine passive Überwachungsmaßnahme verletzt aber dann das Fairnessgebot, wenn es sich bei der abgehörten Kommunikation um ein Gespräch zwischen einer beschuldigten Person in Haft und deren Rechtsvertreter_in handelt. Dadurch wird das Recht nach Art. 6 Abs. 3 lit. b EMRK verletzt, über eine Gelegenheit zur Vorbereitung einer Verteidigung zu verfügen.

Khan Rz 36

Zagaria; VwGH 27.01.2009, 2008/06/0157.

Prozessuale Auswirkungen

Ein Verfahren, das mit einer Verletzung von Art. 6 EMRK behaftet ist, kann insgesamt fair sein, wenn die Fairnesseinbußen entsprechend ausgeglichen wurden (z.B. bei Überwiegen der korrekt erhobenen Beweise, ausreichend Möglichkeit den rechtswidrig erlangten Beweis vor Gericht zu bekämpfen etc.). Ob eine Verletzung von Art. 6 EMRK wie im Fall Allan ausgeglichen werden kann, hat der EGMR bis dato nicht klar beantwortet.[55] Aber auch für den Fall, dass ein Verfahren dem Fairnessgebot genügt, ist die Beweiserhebung mittels verdeckter Ermittler_innen insofern problematisch, dass die Identitäten der Informant_innen von der Polizei geheimgehalten werden können. Dadurch droht eine potentielle Verletzung des Unmittelbarkeitsgrundsatzes (§ 13 StPO) sowie des Rechts, Fragen an Belastungszeug_innen zu stellen bzw. stellen zu lassen (Art. 6 Abs. 3 lit. d EMRK).[56]

Kostovski Rz 43

Bei besonders schweren Verstößen gegen Art. 6 EMRK, wenn zB. Beweise durch Folter oder foltergleiche Handlungen und damit unter einer Verletzung von Art. 3 EMRK zustande gekommen sind, ist das Verfahren durch diese Fairnessverletzung mit einer sog. absoluten Unheilbarkeit von dieser behaftet, die nicht mehr kompensierbar ist. So eine absolute Fairnessverletzung ist auch durch eine sog. Tatprovokation begründet; wenn durch einen Spitzel zur Begehung einer Straftat verleitet wurde.

Teixeira de Castro Rz 39; Ramanauskas Rz 55

Die im Kapitel erwähnten Fälle, in alphabetischer Reihenfolge

abrufbar unter https://hudoc.echr.coe.int

EGMR

Big Brother Watch/Vereinigtes Königreich, 13.09.2018, 58170/13
Bykov/Russland, 21.01.2009, 4378/02
Catt/Vereinigtes Königreich, 24.01.2019, 43514/15
Copland/Vereinigtes Königreich, 03.07.2007, 62617/00
Disk ua/Türkei, 27.11.2012, 38676/08
Ekimdzhiev/Bulgarien, 28.06.2007, 62540/00
Gewerkschaft der Polizei in der Slowakei ua/Slowakei, 25.09.2012, 11828/08
Guja/Moldawien, 12.02.2008, 14277/04
Handyside/Vereinigtes Königreich, 07.12.1976, 5493/72
Harutyunyan/Armenien, 28.06.2007, 36549/03
Heglas/Tschechien, 01.03.2007, 5935/02
Herczegfalvy/Österreich, 24.09.1992, 48/1991/300/371
Khan/Vereinigtes Königreich, 02.05.2000, 35394/97
Klass ua/Deutschland, 06.09.1978, 5029/71
Kostovski/Niederlande, 20.11.1989, 11454/85
Liberty ua/Vereinigtes Königreich, 01.07.2008, 58243/00
Malone/Vereinigtes Königreich, 02.08.1984, 8691/79
P.G. und J.H./Vereinigtes Königreich, 25.09.2001, 44787/98
Peck/Vereinigtes Königreich, 28.01.2003, 44647/98
Ramanauskas/Litauen, 05.02.2008, 74420/01
Roemen ua/Luxemburg, 25.02.2003, 51772/99
Rotaru/Rumänien, 04.05.2000, 28341/95
Segerstedt-Wiberg/Schweden, 06.06.2006, 62332/00
S. und Marper/Vereinigtes Königreich, 04.12.2008, 30562/04 30566/04
Szabó ua/Ungarn, 12.01.2016, 37138/14
Teixeira de Castro/Portugal, 09.06.1998, 25829/94
Telegraaf Media Nederland Landelijke Media B.V. ua/ Niederlande, 22.11.2012, 39315/06
Uzun/Deutschland, 02.09.2010, 35623/05
Weber ua/Deutschland, 29.06.2006, 54934/00
Zagaria/Italien, 27.11.2007, 58295/00
Zakharov/Russland, 04.12.2015, 47143/06

EuGH

Digital Rights Ireland, C293/12 und C594/12, ECLI:EU:C:2014:238
Gutachten 1/15, ECLI:EU:C:2017:592
Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788
Schecke ua, C-92/09 und C-93/09, ECLI:EU:C:2010:662
Schrems, C-362/14, ECLI:EU:C:2015:650
Tele2 Sverige und Watson, C-203/15 und C-698/15, ECLI:EU:C:2016:970

Endnoten

1 Vgl. *Nowak*, Menschenwürde und Menschenrechte, in *Löcker* (Hrsg.), Wiener Vorlesungen im Rathaus, Bd. 190 (2018) 11.
2 Vgl. *Lehner*, Das Grundrecht auf Datenschutz, in *Heißl* (Hrsg.), Handbuch Menschenrechte (2009) 212.
3 Vgl. *Mayer/Kucsko-Stadlmayer/Stöger*, Grundriss des österreichischen Bundesverfassungsrechts[11] (2015) Rz. 1334.
4 Vgl. *Tamblé*, Der Anwendungsbereich der EU-Grundrechtecharta (GRC) gem. Art. 51|1 GRC – Grundlagen und aktuelle Entwicklungen, in *Tietje* (Hrsg.), Beiträge zum Europa- und Völkerrecht, Heft 9 (2014) 29.
5 Vgl. *Mayer et al.*, Bundesverfassungsrecht[11] Rz. 1345.
6 Vgl. *Mayer et al.*, Bundesverfassungsrecht[11] Rz. 1569.
7 Vgl. EGMR 16.10.2007, 74336/01, Wieser ua/Österreich Rz. 45.
8 Vgl. *Meyer-Ladewig/Nettesheim*, EMRK[4] (2017) Art. 8 Rz. 7.
9 Vgl. *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, in *Bogdandy et al.* (Hrsg), Beiträge zum ausländischen öffentlichen Recht und Völkerrecht, Bd 259 (2016) 26.
10 *Paefgen*, Persönlichkeitsrechte im Internet 197.
11 Ebd. Rz. 67.
12 Vgl. *Mayer et al.*, Bundesverfassungsrecht[11] Rz. 1421.
13 Vgl. *Paefgen*, Persönlichkeitsrechte im Internet 89.
14 Ebd. Rz. 21.
15 Ebd. Rz. 70.
16 Vgl. *Mayer et al.*, Bundesverfassungsrecht [11] Rz. 1340.
17 Vgl. *Meyer-Ladewig et al.*, EMRK[4] Art. 8 Rz. 107.
18 Ebd. Rz. 105.
19 Vgl. *Paefgen*, Persönlichkeitsrechte im Internet 151.
20 Vgl. *Meyer-Ladewig et al.*, EMRK[4] Art. 8 Rz. 109.
21 Ebd. Rz. 110.
22 *Meyer-Ladewig et al.*, EMRK[4] Art. 8 Rz. 112.
23 Ebd. Rz. 113.
24 Vgl. *Paefgen*, Persönlichkeitsrechte im Internet 157.
25 Vgl. *Mayer et al.*, Bundesverfassungsrecht[11] Rz. 1431.
26 Ebd. Rz. 1437.
27 Ebd. Rz. 1438.
28 Ebd. Rz. 1439.
29 Vgl. VfSlg 19.691.
30 Vgl. Bundeskanzleramt-Verfassungsdienst 14.05.2008, 810.016/0001-V/3/2007.
31 *Marsch*, Das europäische Datenschutzgrundrecht: Grundlagen – Dimensionen – Verflechtungen, in Jus Publicum. Beiträge zum öffentlichen Recht (2018) 206.
32 Vgl. *Michl*, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh – zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht, in Datenschutz und Datensicherheit (2017) 353.
33 Vgl. Artikel-29-Datenschutzgruppe, Arbeitsunterlage 1/2016 über die Rechtfertigung von Eingriffen in die Grundrechte auf Schutz der Privatsphäre und Datenschutz durch Überwachungsmaßnahmen bei der Übermittlung personenbezogener Daten (2016) 6.
34 Vgl. European Data Protection Supervisor, Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken: Ein Toolkit (2017), edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_de.pdf (23.8.2019) 13.
35 Vgl. *Meyer-Ladewig et al.*, EMRK[4] Art. 10 Rz. 2.
36 Vgl. *Hallinan*, Effects of surveillance on freedom of assembly, association and expression, in Wright/Kreissl (Hrsg.), Surveillance in Europe (2015) 270.
37 *Mayer et al.*, Bundesverfassungsrecht[11] Rz. 1457.
38 Vgl. *Paefgen*, Persönlichkeitsrechte im Internet 18.
39 Vgl. *Meyer-Ladewig et al.*, EMRK[4] Art. 10 Rz. 8–18.
40 Vgl. *Mayer et al.*, Bundesverfassungsrecht[11] Rz. 1456.
41 Ebd.
42 Art. 11 EMRK geht als lex specialis der Prüfung von Art. 10 EMRK als lex generalis vor, vgl. EGMR 26.04.1991, 11800/85, Ezelin gegen Frankreich Rz. 35.

43 Vgl. *Meyer-Ladewig et al.*, EMRK[4] Art. 11 Rz. 5.
44 Ebd. 15.
45 *Arzt/Ullrich*, Versammlungsfreiheit versus polizeiliche Kontroll- und Überwachungspraxis, in: Vorgänge Nr. 213 (2016) 53.
46 Vgl. INCLO, Spying on Dissent. Surveillance Technologies and Protest (2019), policehumanrightsresources.org/content/uploads/2019/06/spying-on-dissent-Report_EN.pdf?x39143 (Zugriff 23.8.2019) 9 f.
47 Vgl. *Aston*, State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives, in European Journal of Law and Technology, Bd 8 Nr 1 (2017) 9–12.
48 Vgl. VfSlg 15.109.
49 Ebd.
50 Vgl. *Mayer et al.*, Bundesverfassungsrecht[11] Rz. 1466.
51 Vgl. *Meyer-Ladewig et al.*, EMRK[4] Art. 6 Rz. 90.
52 Vgl. *Meyer-Ladewig et al.*, EMRK[4] Art. 6 Rz. 129.
53 Vgl. *Zerbes*, Spitzeln, Spähen, Spionieren. Sprengung strafprozessualer Grenzen durch geheime Zugriffe auf Kommunikation (2010) 78.
54 Ebd. 79.
55 Ebd. 85.
56 Vgl. *Adensamer/Sagmeister*, Das polizeiliche Staatsschutzgesetz. Darstellung und Kritik, in *Bundesministerium für Justiz* (Hrsg), recht.tolerant. RicherInnenwoche in Hermagor/Tröpolach (2016) 84 f.

10 Datenschutz im Polizeibereich

Ausnahme nach Art. 2 Abs 2 lit d DSGVO

RL 680/2016 oder Polizei-DSRL

Auch die Polizei muss sich an datenschutzrechtliche Vorgaben halten, wenn sie personenbezogene Daten verarbeitet. Zwar gilt die Datenschutzgrundverordnung (DSGVO) für sie grundsätzlich nicht, dafür aber eine eigene EU-Richtlinie, die den Datenschutz der Polizei regelt (Polizei-DSRL). Diese wurde in Österreich mit dem Datenschutzgesetz 2018 (DSG) umgesetzt, insbesondere in dessen 3. Hauptstück. Da die Richtlinie EU-Recht ist, bezieht sie sich nur auf Rechtsbereiche, die in der Kompetenz der EU liegen. Davon ist u.a. die nationale Sicherheit ausgenommen, also z.B. Geheimdienste ohne polizeiliche Befugnisse. Diese gibt es in Österreich nur im militärischen Bereich. Sollte sich dies ändern, z.B. durch eine umfassende Geheimdienstreform mit der Schaffung eines von der Polizei völlig entkoppelten Geheimdienstes, hätte dies zur Folge, dass die Rechte und Pflichten, die in diesem Kapitel näher beschrieben werden, für einen weiten Bereich polizeilicher Ermittlungsarbeit nicht mehr gelten.

10.1 Grundsätze

§ 37 DSG

Im DSG wird eine Reihe von Grundsätzen festgelegt, nach denen sich die Polizei bei der Datenverarbeitung zu richten hat.

Rechtmäßige Verarbeitung nach **Treu und Glauben:** Rechtmäßig ist die Verarbeitung personenbezogener Daten dann, wenn

- dies für eine Person lebenswichtig ist

  oder

- dies gesetzlich vorgesehen ist, und
- zur Erfüllung einer gesetzlichen Aufgabe der Sicherheitspolizei, Kriminalpolizei oder des Verfassungsschutzes erforderlich ist, und
- verhältnismäßig ist.

➲ *4.1 Rechtsgrundlagen*

Zweckbindung: Daten dürfen nur für bestimmte Zwecke erhoben werden und dürfen in Folge auch nur für die Zwecke verwendet werden, für die sie erhoben wurden.
Datenminimierung: Es dürfen nur Daten erhoben werden, die dem angegebenen (insb. dem gesetzlich vorgesehenen) Zweck tatsächlich dienen, und nur in dem Umfang, wie zur Erfüllung des Zwecks erforderlich ist.
Sachliche Richtigkeit: Die Daten müssen nach Möglichkeit sachlich richtig sein, und es muss Möglichkeiten geben, sie zu berichtigen oder zu löschen, wenn sie falsch sind.
Speicherbegrenzung: Die Daten dürfen nicht länger gespeichert werden als sie für die Zwecke, für die sie gesammelt wurden, gebraucht werden.
Datensicherheit, Integrität und Vertraulichkeit: Die Daten müssen vor unbefugten Zugriffen (auch innerhalb einer Organisation) geschützt werden.
Zwischen faktenbasierten und persönlichen Einschätzungen muss **unterschieden** werden.

10.1.1 Besondere Kategorien von Daten

§ 38 DSG

Bestimmte besondere Kategorien von Daten (früher „sensible Daten“) dürfen nur unter besonders strengen Voraussetzungen verarbeitet werden. Diese Kategorien sind dieselben, die zum Teil auch durch das Diskriminierungsrecht geschützt sind. Das problematische und überholte Wort „rassisch“ ist – solange es sich noch in Gesetzestexten findet – als diskriminierende Zuschreibung zu verstehen, nicht als Fakt. Dies sind:

- Daten, die Aufschluss geben über „rassische“ (so in § 39 DSG) oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit
- genetische Daten
- biometrische Daten zur eindeutigen Identifikation
- Gesundheitsdaten
- Daten zum Sexualleben oder zur sexuellen Orientierung

🕮 *Genetische Daten*
§ 36 Abs. 2 Z 12 DSG
🕮 *Biometrische Daten*
§ 36 Abs. 2 Z 13 DSG

10.1.2 Automatisierte Entscheidungen

Entscheidungen zum Nachteil einer Person (z.B. im Zuge von Profiling) dürfen nur dann rein automatisch getroffen werden, wenn dies eigens gesetzlich vorgesehen ist. Solche Entscheidungen dürfen nicht auf den besonders sensiblen Kategorien beruhen. Darüber hinaus müssen in allen Fällen von automatischen Entscheidungen geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen bereits im Gesetz geboten sein. Automatische Entscheidungen auf Basis der besonders sensiblen Kategorien dürfen nur getroffen werden, wenn dies konkret und ausdrücklich gesetzlich vorgesehen ist, der_die Verantwortliche persönlich eingreifen kann und im Gesetz geeignete Garantien für die Rechte und Freiheiten der Betroffenen geboten werden. Letzteres bedeutet insbesondere, dass betroffene Personen das Recht haben, unterrichtet zu werden (Recht auf Information), das Eingreifen einer Person zu verlangen, ihren eigenen Standpunkt darzulegen und die Entscheidung anzufechten.
Profiling, das aufgrund der besonderen Kategorien diskriminiert, ist auf jeden Fall verboten.

🕮 *Profiling*
§ 36 Abs. 2 Z 4 DSG

§ 41 DSG, Art. 11 Polizei-DSRL

Erwägungsgrund 38 der Polizei-DSRL

10.2 Betroffenenrechte

Viele Rechte, die von polizeilicher Überwachung Betroffene haben, kommen aus dem Datenschutzrecht: das Recht auf Informationen und auf Auskunft, auf Berichtigung, Löschung und Einschränkung der Verarbeitung. Es ist sehr zu begrüßen, dass diese auch für den polizeilichen Bereich im EU-Recht verankert sind.

10.2.1 Grundsätze der Ausübung von Datenschutzrechten

Transparenz: Informationen über Rechte und ihre Ausübung müssen leicht verständlich sein. Sie sollten, wenn möglich, in der gleichen Form wie der Antrag erfolgen (also z.B. per Mail oder per Post).
Monatsfrist: Informationen über Auskunfts-, Lösch- oder Berichtigungsbegehren müssen unverzüglich gegeben werden, spätestens aber nach einer Frist von einem Monat. Diese Monatsfrist kann um zwei Monate (also auf insgesamt drei Monate) verlängert werden, wenn aufgrund der Komplexität oder Anzahl der Anträge nötig.
Unentgeltlichkeit: Die Informationen sind gratis zur Verfügung zu stellen, außer die Anträge sind „offenkundig unbegründet“ oder „exzessiv“, insbesondere bei häufigen wiederholten Anträgen.

§ 42 Abs. 1 DSG, Art 12 Polizei-DSRL

Ist die automatisierte Entscheidung zulässig?

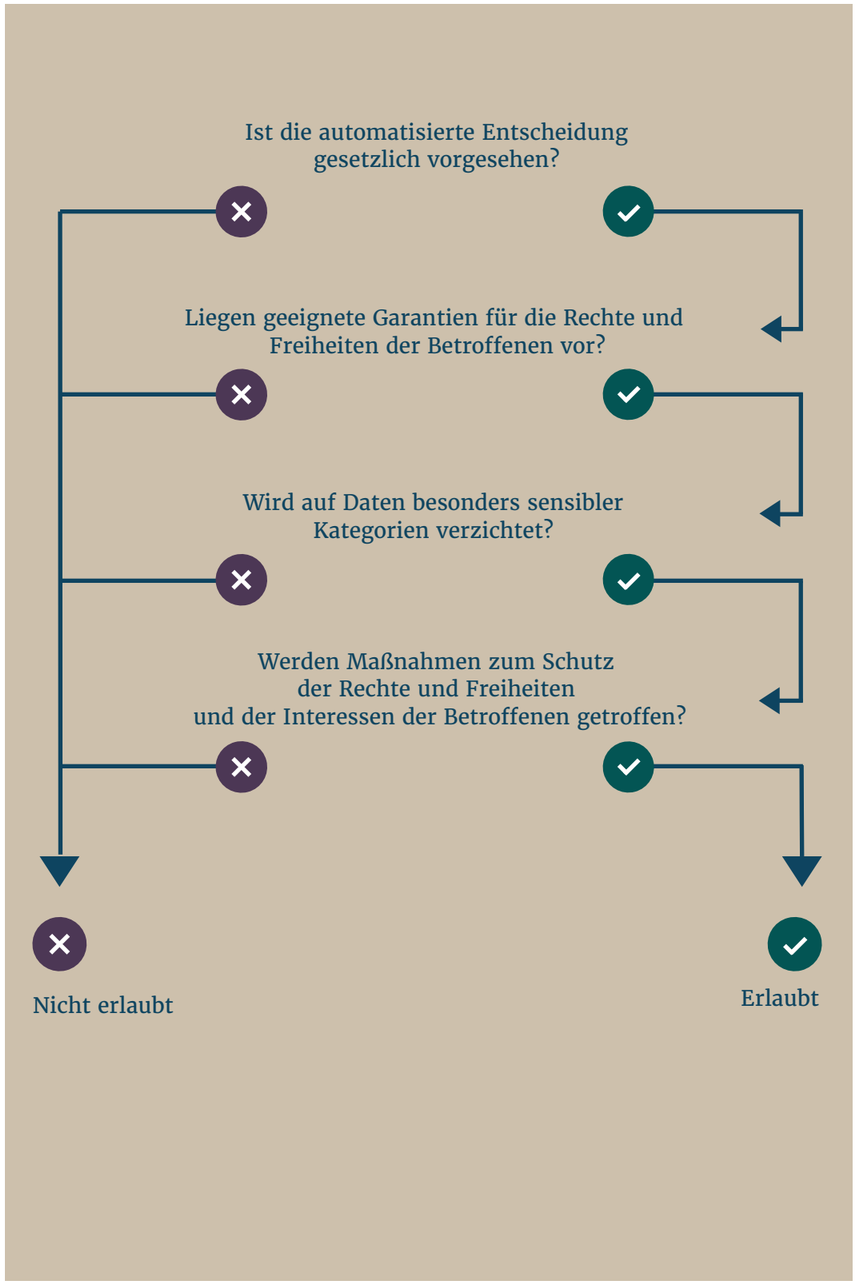


Abb. 13
Dieses Prüfungsschema wird angewandt, wenn nicht ausgeschlossen ist, dass die automatisierten Entscheidungen nachteilige Rechtsfolgen für die Betroffenen haben und dass das Profiling aufgrund von besonders sensiblen Kategorien diskriminierend wirkt.

Identitätsnachweis: Die Behörde kann die Bestätigung der Identität des_der Antragsteller_in verlangen, wenn berechtigte Zweifel über die Identität bestehen. Dies dient dem Verhindern eines Missbrauchs (des Rechts auf Information) und des Erlangen von Informationen über andere Personen. Diese Information zur Identitätsbestätigung (z.B. Passkopie) darf nicht länger als notwendig gespeichert werden und für keinen anderen als diesen ursprünglichen Zweck verwendet werden.

10.2.2 Recht auf Information

Im Gegensatz zur Auskunft (siehe 10.2.3), die man selbst beantragt, muss die Polizei die im Folgenden aufgezählten Informationen von sich aus geben. Das Recht auf Information ist also insbesondere dann wichtig, wenn die betroffene Person von der Datenverarbeitung ansonsten gar nichts wüsste. Sonstige Datenschutzrechte bleiben eine rein theoretische Gewährleistung, wenn man praktisch gar nicht weiß, dass die Polizei Daten über einen selbst verarbeitet.
Jede Person, über die Daten durch die Polizei verarbeitet werden, hat ein Recht auf Information über

Keine Datenverarbeitung ohne Informieren der betroffenen Person

§ 43 DSG, Art. 13 Polizei-DSRL

- Kontaktdaten des_der für die Verarbeitung Verantwortlichen
- Kontaktdaten des_der Datenschutzbeauftragten
- die Zwecke der Datenverarbeitung
- das Recht auf Beschwerde, und dafür die Kontaktdaten der Datenschutzbehörde
- das Recht auf Auskunft
- das Recht auf Berichtigung
- das Recht auf Löschung
- das Recht auf Einschränkung der Verarbeitung
- die Rechtsgrundlage der Verarbeitung (in Einzelfällen)
- die Dauer der Speicherung (in Einzelfällen)
- die Kategorien von Empfänger_innen (auch im Ausland), im Falle einer Datenübermittlung (in Einzelfällen)
- erforderlichenfalls weitere Informationen (in Einzelfällen)

Wenn die Daten direkt bei der betroffenen Person erhoben werden, müssen diese Informationen sofort zum Zeitpunkt der Erhebung gegeben werden. Wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, müssen diese Informationen durch den_die Verantwortliche bis spätestens ein Monat nach Erlangung der Daten gegeben werden (jedoch innerhalb dieses Monats spätestens zum Zeitpunkt der ersten Kommunikation mit der betroffenen Person nach Erlangung der Daten, wenn zu dieser Kommunikationsaufnahme die erhobenen personenbezogenen Daten verwendet werden). Falls die Daten an eine_n andere_n Empfänger_in offengelegt werden, muss das Informieren der betroffenen Person spätestens zum Zeitpunkt der ersten Offenlegung stattfinden.

Fristen für die Ausgabe der Informationen

Die Information kann entfallen, wenn die Daten innerhalb der Behörde weitergeleitet wurden. In diesem Fall hatte schon die erste Stelle, die die Daten ermittelt hat, die Pflicht die Betroffenen zu informieren. Außerdem kann die Information entfallen, wenn die Daten von einem_einer anderen Datenverantwortlichen stammen und die Datenverarbeitung durch ein Gesetz vorgesehen ist. Hier besteht die Gefahr, dass durch Übermittlungen die Informationspflichten unterlaufen werden.

Ausnahmen

Unter bestimmten Voraussetzungen kann die Information ebenfalls entfallen, wenn sie Ermittlungen beeinträchtigen würde, zum Schutz der öffentlichen Sicherheit oder zum Schutz der Rechte und Freiheiten anderer Menschen. Dies gilt aber nur, wenn die Einschränkung verhältnismäßig ist.

➲ *9.1.3 Verhältnismäßigkeitsprüfung*

10.2.3 Recht auf Auskunft

§ 44 DSG, Art. 14, 15 Polizei-DSRL

Im Gegensatz zur Information (siehe 7.2.2), die die Polizei von sich aus geben muss, wird Auskunft auf Verlangen der betroffenen Person an diese erteilt.
Jede Person, über die Daten durch die Polizei verarbeitet werden, hat das Recht, Auskunft zu erhalten über

- die Zwecke der Datenverarbeitung
- die Kategorien von Daten, die verarbeitet wurden
- das Bestehen des Beschwerderechts bei der Datenschutzbehörde
- das Bestehen des Rechts auf Berichtigung, Löschung und Einschränkung
- die Speicherdauer
- die Empfänger_innen (auch im Ausland), falls die Daten übermittelt werden
- alle verfügbaren Informationen über die Herkunft der Daten

Diese Auskunft muss innerhalb von einem Monat ab Antrag auf Auskunftserteilung gegeben werden, die Frist kann aber um zwei Monate verlängert werden, wenn dies aufgrund der Anzahl der Anträge oder der Komplexität erforderlich ist.

➲ *9.1.3 Verhältnismäßigkeitsprüfung*

Unter bestimmten Voraussetzungen kann die Auskunft unterlassen werden, z.B. wenn dies Ermittlungen beeinträchtigen würde, zum Schutz der öffentlichen Sicherheit oder zum Schutz der Rechte und Freiheiten anderer Menschen. Dies gilt aber nur, wenn die Einschränkung verhältnismäßig ist. In so einem Fall muss die betroffene Person aber von der Verweigerung und den Gründen dafür informiert werden, außer die obengenannten Voraussetzungen treffen auf diese Information selbst zu. Allerdings muss auch bei geheimen Ermittlungen nachträglich über eine Datenerhebung informiert werden, wenn die Gründe der – zunächst rechtmäßigen – Geheimhaltung weggefallen sind, insbesondere weil bereits offiziell ein Strafverfahren eingeleitet wurde und den Betroffenen nun die Akteneinsicht freistehen muss. Die Akteneinsicht selbst richtet sich nach den Regeln des jeweiligen Verfahrens. Soweit sich Akteneinsicht und Auskunftsrecht überschneiden, sind die Verfahrensbestimmungen (bspw. nach der Strafprozessordnung) zu beachten, das heißt, das Auskunftsrecht kann nicht weiter gehen als die Akteneinsicht. Soweit Daten vorliegen, die vom Recht auf Akteneinsicht gar nicht berührt sind, besteht ein Auskunftsrecht nach den Vorschriften des § 44 DSG. (Siehe nebenstehende Abbildung)

Akteneinsicht

10.2.4 Recht auf Berichtigung, Löschung und Einschränkung

§ 45 DSG, Art. 16 Polizei-DSRL

Betroffene haben das Recht auf Berichtigung bzw. Vervollständigung ihrer Daten. Außerdem müssen die Daten gelöscht werden, wenn sie nicht mehr notwendig sind, wenn sie unrechtmäßig verarbeitet wurden, oder wenn eine rechtliche Verpflichtung zur Löschung besteht. Es gibt außerdem das Recht auf Einschränkung der Verarbeitung. Dies ist für den Fall vorgesehen, dass die Speicherung notwendig ist, um die Rechte der betroffenen Person zu wahren, z. B. wenn sie als Beweismittel notwendig sind. In diesem Fall dürfen die Daten nur gespeichert und eingeschränkt für den Zweck, der der Löschung noch entgegensteht, verarbeitet werden. Werden diese Rechte verweigert, muss die betroffene Person darüber sowie über die Gründe der Verweigerung und die Möglichkeit einer Beschwerde informiert werden.

Antrag auf Auskunftserteilung

Joan Doe
Rennweg 93
1030 Wien

Landespolizeidirektion Wien
Schottenring 7-9
1010 Wien
lpd-w@polizei.gv.at

Wien, am 1.1.2020

Betreff: Auskunftsbegehren über meine personenbezogene Daten

Sehr geehrte Damen und Herren,

Ich stelle hiermit gem. § 44 DSG einen Antrag auf Auskunft über meine personenbezogenen Daten.

Zum Nachweis meiner Identität lege ich die Kopie meines Ausweises bei.

Mit freundlichen Grüßen

Joan Doe (Unterschrift)

Abb. 14
Briefbeispiel für Antrag auf Auskunftserteilung

10.3. Beschwerden und Rechtsbehelfe

Der Schutz des Datenschutzrechts ist auch dadurch gewährleistet, dass die Betroffenen sich eigenständig gegen das gesetzwidrige Verarbeiten von Daten durch die Behörden wehren können. Im Folgenden wird ein Überblick über die verschiedenen Beschwerdemöglichkeiten und Rechtsbehelfe verschafft.

10.3.1 Beschwerde an die Datenschutzbehörde

§ § 24, 32 Abs. 1 Z 4 DSG, § 90 SPG, Art. 17 Polizei-DSRL

Beschwerdefälle: In den untenstehenden Fällen kann eine betroffene Person Beschwerde bei der Datenschutzbehörde erheben. Dazu braucht man keine_n Anwält_in und es fallen auch keine Gebühren an.

- Die Verarbeitung verstößt gegen das Grundrecht auf Datenschutz. (§ 24 Abs. 1 DSG)
- Es wurden keine oder nur eingeschränkte Informationen gegeben. (§ 42 Abs. 8 DSG)
- Es wurden keine oder nur eingeschränkte Auskünfte gegeben. (§ 42 Abs. 8 DSG)
- Die Berichtigung, Löschung oder Einschränkung wurde verweigert. (§ 42 Abs. 8 DSG)
- Die Verarbeitung verstößt gegen die Polizei-DSRL. (Art. 52 Polizei-DSRL)
- Im Bereich der Sicherheitspolizei wurden die Vorschriften des DSG nicht eingehalten und dadurch Rechte des_der Betroffenen verletzt. (§ 90 SPG)

§ 24 Abs. 2 DSG

Bestandteile der Beschwerde: Beim Verfassen einer Beschwerde an die Datenschutzbehörde muss man darauf achten, dass die unten aufgezählten Bestandteile enthalten sind. Sie kann schließlich per Post oder per E-Mail eingebracht werden.

Adresse: Österreichische Datenschutzbehörde Barichgasse 40-42 1030 Wien oder dsb@dsb.gv.at

- Welches Recht wurde verletzt? (z.B. Geheimhaltung, Auskunft, Richtigstellung, Löschung)
- Wer ist dafür verantwortlich?
- Was ist der zugrundeliegende Sachverhalt?
- Aus welchen Gründen ist der Sachverhalt rechtswidrig?
- Was ist die Beschwerdefrist? Wurde sie eingehalten? Seit wann ist das Ereignis bekannt?
- Der Satz: „Ich beantrage die Feststellung, dass mein Recht auf … verletzt worden ist.“
- Ort, Datum
- Unterschrift!

🕮 *Fristen und Vorraussetzungen für Beschwerden*

Fristen: Eingebracht werden muss die Beschwerde bis spätestens ein Jahr nachdem die betroffene Person von dem der Beschwerde zugrundeliegendem Umstand erfahren hat, und spätestens drei Jahre nach dem ereigneten Umstand selbst.
Innerhalb von drei Monaten nachdem die Beschwerde eingebracht wurde, muss die Datenschutzbehörde die betroffene Person über den Stand und das Ergebnis der Ermittlungen informieren.

10.3.2 Beschwerde an das Bundesverwaltungsgericht

In den folgenden Fällen kann eine betroffene Person eine Beschwerde an das Bundesverwaltungsgericht richten. Es besteht keine Anwaltspflicht. Es fallen €30 an Gebühren an.

- Die Entscheidung der Datenschutzbehörde war rechtswidrig. (§ 27 DSG)
- Die Datenschutzbehörde hat sich nicht mit der Beschwerde befasst. (§ 28 Abs. 8 DSG)
- Die Datenschutzbehörde hat nicht innerhalb von drei Monaten nach einer Beschwerde über deren Stand oder Ergebnis informiert. (§ 28 Abs. 8 DSG)

Die Beschwerde muss innerhalb von vier Wochen nach Zustellung des Bescheids bei der Datenschutzbehörde selbst eingebracht werden, und wird dann von dieser an das Bundesverwaltungsgericht weitergeleitet. Die Beschwerde muss Folgendes enthalten:

- Genaue Bezeichnung des Bescheids (z.B. Geschäftszahl)
- Bezeichnung der Behörde gegen die sich die Beschwerde richtet, in diesem Fall also die Datenschutzbehörde
- Die Begründung, wieso der Bescheid rechtswidrig ist
- Was man erreichen möchte, also z.B. Feststellung der Rechtswidrigkeit oder Aufhebung des Bescheides
- Angaben zur Frist und ihrer Einhaltung, also wann der Bescheid zugestellt wurde und das Datum der Beschwerde

10.3.3 Schadenersatz und sonstige Rechtsbehelfe

Es gibt ein Recht auf Schadenersatz bei datenschutzrechtlichen Verstößen. Dieser kann über den Zivilrechtsweg eingeklagt werden. Bei Schäden aus hoheitlichem Handeln staatlicher Behörden sieht die Zivilrechtsordnung dafür eine sogenannte Amtshaftungsklage vor. *§ 29 DSG, Art. 46 Polizei-DSRL*

Vertretung durch NGOs: Es ist möglich, sich in Datenschutzbeschwerden von einer Grundrecht-NGO, wie z.B. epicenter.works vertreten zu lassen. Eine solche Organisation darf nicht gewinnorientiert sein und ihre Ziele müssen im öffentlichen Interesse liegen. Verfahren wegen Schadenersatz sind von der Vertretung ausgenommen. *Vertretung durch NGOs § 28 DSG, Art. 55 Polizei-DSRL*

Gerichtlicher Rechtsbehelf: Man hat außerdem das Recht, sich bei einer Verletzung der Polizei-DSRL an ein Gericht zu wenden. *Art. 54 Polizei-DSRL*

Einspruch wegen Rechtsverletzung: Ist man im Zuge eines kriminalpolizeilichen Ermittlungsverfahren in Rechten verletzt worden, kann man beim Gericht Einspruch dagegen erheben. Man muss den Einspruch innerhalb von sechs Wochen, nachdem man von der Rechtsverletzung erfahren hat, bei der Staatsanwaltschaft einbringen. Auch gegen die Bewilligung einer Ermittlungsmaßnahme kann man Beschwerde erheben. *§ 106 StPO*

10.4 Interne Vorgaben

Auch in ihren internen Systemen und Strukturen müssen sich die Polizeibehörden an das EU-Datenschutzrecht halten.

Datenschutz durch Technikgestaltung und datenschutzrechtliche Voreinstellungen: Diese Begriffe heißen im Englischen Privacy by Design und Privacy by Default und sind so auch in deutschen Texten gängig. Die damit gemeinten technischen Ausgestaltungen und Voreinstellungen der Datenbanken der Behörden sollen sicherstellen, dass nur notwendige Daten, und diese nicht länger als erforderlich, verarbeitet werden können. Das gilt bei Eigenentwicklungen ebenso wie bei zugekauften Datenverarbeitungssystemen.

Verarbeitungsverzeichnis: Die Behörden müssen detaillierte Verzeichnisse darüber führen, welche Daten zu welchen Zwecken sie mit welchen Mitteln verarbeiten. *§ 49 DSG, Art. 24 Polizei-DSRL*

Protokollierung: Alle Vorgänge in Datenbanken müssen protokolliert werden. Dies betrifft Erhebungen, Veränderungen, Abfragen, Offenlegungen, inkl. *§ 50 DSG, Art. 25 Polizei-DSRL*

Begründung, Datum und Uhrzeit und Identität der Person, die diese vorgenommen hat. Diese Protokolle sind notwendig, um bei rechtswidrigen Zugriffen feststellen zu können, was passiert ist, und sie dürfen auch nur zu diesem Zweck verwendet werden.

§ 52 DSG, Art. 27 Polizei-DSRL

Datenschutzfolgenabschätzung: Wenn eine neue Art der Datenverarbeitung (z. B. beim Einsatz neuer Überwachungstechnologien) ein hohes Risiko für die Rechte der Betroffenen darstellt, muss die Behörde im Voraus eine Folgenabschätzung durchführen.

§ 53 DSG, Art. 28 Polizei-DSRL

Vorgaben der Datenschutzbehörde: Ergibt die Datenschutzfolgenabschätzung, dass ein hohes Risiko besteht, kann die Datenschutzbehörde besondere Maßnahmen vorschreiben, die die Behörde innerhalb von sechs Wochen umsetzen muss. Die Frist kann, wenn notwendig, um ein Monat verlängert werden.

§ 54 DSG, Art. 29 Polizei-DSRL

Datensicherheitsmaßnahmen: Die Behörden müssen technische und organisatorische Maßnahmen treffen, um rechtswidrigen Zugriff und Veränderungen oder die unbeabsichtigte Vernichtung von Daten zu verhindern. Dazu zählen z.B. Zugangs- und Zugriffskontrollen.

Sicherheitsmaßnahmen und Datenschutzbeauftragte

Datenschutzbeauftragte_r: Jede Behörde muss eine_n Datenschutzbeauftragte_n bestellen, der_die die Behörden und ihre Mitarbeiter_innen über ihre datenschutzrechtlichen Pflichten aufklären, ihre Einhaltung kontrollieren, bei Datenschutzfolgenabschätzungen beraten, sowie mit der Datenschutzbehörde zusammenarbeiten muss. Im öffentlichen Bereich ist der_die Datenschutzbeauftragte weisungsfrei. Datenschutzbeauftragte fungieren beratend zur Einhaltung der Datenschutz-Vorschriften und erfüllen wichtige Aufgaben im Datenschutz-Management. Sie sind aber nicht für die Verarbeitung verantwortlich oder haften dafür persönlich, diese Rolle bleibt der Behörde bzw. der Körperschaft öffentlichen Rechts vorbehalten.

§§ 5, 57 DSG, Art. 32 - 43 Polizei-DSRL

10.5 Datenübermittlung an Nicht-EU-Länder

Länderunterschiede im Datenschutzniveau

Die Übermittlung von personenbezogenen Daten an Nicht-EU-Länder ist umstritten, weil es in vielen Ländern ein niedrigeres Datenschutzniveau gibt als in Europa. Gibt es in einem Nicht-EU-Land z. B. keine Löschverpflichtungen und zugleich einen beidseitigen Datenaustausch, wird es über den Austausch möglich, die eigenen Datenschutzbestimmungen zu umgehen, indem man die Daten teilt, im Inland löscht und nach Jahren aus dem anderen Land im Wege der internationalen Rechtshilfe wieder anfordert. Der Datenaustausch mit einem Land mit niedrigerem Schutzniveau kann so als eine Art Backup dienen, welches im Inland rechtlich nicht zulässig wäre.

§§ 58-61 DSG, Art. 35-40 Polizei-DSRL

Die Übermittlung an Drittländer und internationale Organisationen (z. B. United Nations) ist grundsätzlich unter folgenden Voraussetzungen möglich (alle müssen vorliegen):

- Sie ist für polizeiliche Zwecke erforderlich.
- Sie erfolgt an eine Polizeibehörde.
- Wenn die Daten aus einem anderen Land stammen, erfolgt die Übermittlung mit Zustimmung dieses Landes.
- Es liegt ein Angemessenheitsbeschluss vor. Diesen trifft die EU-Kommission, wenn ein Nicht-EU-Land oder eine internationale Organisation ein angemessenes Schutzniveau hat, um an dieses Daten zu übermitteln. Alternativ dazu kann die Übermittlung erfolgen, wenn geeignete Garantien bestehen, die den Datenschutz gewährleisten.

Ausnahmen dieser grundsätzlichen Voraussetzungen bestehen, wenn durch die Übermittlung das Leben oder wichtige Interessen der betroffenen Person geschützt werden oder die Übermittlung der Abwehr von Gefahren für die öffentliche Sicherheit in einem anderen Land dient, aber auch in Einzelfällen, wenn durch die Übermittlung keine Grundrechte verletzt werden.

10.6 Informationen und Meldungen über Datenschutzverletzungen

Benachrichtigungen, §§ 55, 56 DSG, Art 31 Polizei-DSRL

Wenn der Schutz von personenbezogenen Daten verletzt wird, z.B. durch rechtswidrige Datenweitergabe (Leaks) oder Hackerangriffe, und dadurch für die betroffenen Personen voraussichtlich ein hohes Risiko entsteht, müssen diese darüber benachrichtigt werden.

Benachrichtigung der Betroffenen von geleakten Daten

Die Benachrichtigung muss in klarer und einfacher Sprache gehalten sein. Sie muss den Namen und die Kontaktdaten der richtigen Anlaufstelle für weitere Informationen sowie eine Beschreibung der wahrscheinlichen Folgen und der ergriffenen Maßnahmen enthalten.
Die Benachrichtigung kann in bestimmten Fällen entfallen, z.B. wenn die Daten verschlüsselt waren und deshalb für die Betroffenen kein Risiko besteht. Sie kann außerdem durch eine öffentliche Bekanntmachung erfolgen, wenn der Aufwand zu groß wäre, alle Betroffenen einzeln oder als geschlossene Gruppe zu informieren.

Meldungen, § 55 DSG, Art. 30 Polizei-DSRL

Auch an die Datenschutzbehörde muss diese Schutzverletzungen gemeldet werden. Wenn die betroffenen Daten von einem anderen EU-Land übermittelt worden sind, sind auch die Behörden in diesem Land darüber zu verständigen.

§ 34 DSG, Art. 48 Polizei-DSRL

Whistleblowing: Die Behörden müssen dafür sorgen, dass es möglich ist, vertraulich Meldungen über datenschutzrechtliche Verstöße zu erstatten.

Whistleblowing

10.7 Sanktionen

§ 62 DSG, Art. 57 Polizei-DSRL

Wenn Mitarbeiter_innen der Behörden rechtswidrig auf Daten zugreifen, diese weitergeben oder veröffentlichen, drohen ihnen Verwaltungsstrafen von bis zu €50. 000. Diese Strafen werden von der Datenschutzbehörde verhängt. Auch wegen Verstößen gegen alle anderen Vorschriften nach der Polizei-DSRL (z.B. gegen die internen Sicherheitsvorkehrungen oder bei Nichteinhaltung von Vorgaben der Datenschutzbehörde) müssen wirksame, verhältnismäßige und abschreckende Sanktionen verhängt werden. Dies muss im nationalen Recht vorgesehen sein.

Die Österreichische Rechtsordnung kennt verschiedene Sanktionen des gerichtlichen Strafrechts, die einen besonderen Schutz bei der Verarbeitung von (insbesondere personenbezogenen) Daten bewirken sollen. Ohne Anspruch auf Vollständigkeit hier nur die wichtigsten Straftatbestände:

§ 63 DSG

Datenverarbeitung in Gewinn- oder Schädigungsabsicht: Eine Person, die mit dem Vorsatz einer unrechtmäßigen Bereicherung (ihrerselbst oder Dritter) oder der Absicht, jemandes Geheimhaltungsanspruch zu verletzen, personenbezogene Daten selbst benützt, einer anderen zugänglich macht oder veröffentlicht, und diese Daten ihr ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder sie sich diese Daten widerrechtlich verschafft hat, obwohl die betroffene Person an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist vom Gericht mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

Tagessätze

§ 118a StGB

Widerrechtlicher Zugriff auf ein Computersystem: Wer ohne Erlaubnis auf eine Datenbank zugreift, die mit Sicherheitsvorkehrungen geschützt wurde (z.B. durch ein Passwort), kann mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen bestraft werden. Ist die Datenbank ein wesentlicher Bestandteil der kritischen Infrastruktur (z.B. ein wesentliches System zur Aufrechterhaltung der öffentlichen Sicherheit) kann eine Freiheitsstrafe von bis zu zwei Jahren verhängt werden. Wenn die Tat im Rahmen einer kriminellen Vereinigung begangen wird, sogar bis zu drei Jahre Freiheitsstrafe.

§ 302 StGB

Missbrauch der Amtsgewalt: Ein_e Beamt_in, der_die mit dem Vorsatz, dadurch eine andere Person an ihren Rechten zu schädigen, seine_ihre amtlichen Befugnisse wissentlich missbraucht, ist mit einer Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.
Steht die Tat in Verbindung mit Amtsgeschäften mit einem anderen Land oder einer über- oder zwischenstaatlichen Einrichtung, kann die Freiheitsstrafe ein bis zehn Jahre betragen. Das gleiche gilt, wenn die Tat einen €50.000 übersteigenden Schaden verursacht.

EVALUIERUNG VON GESETZEN

In einem Staat, der tendenziell
jedes Sicherheitsrisiko mit einem
Plus an (Überwachungs-)Eingriffen
beantwortet, leben letzten Endes
unfreie Bürger. … Also lautet die
Gegenformel: Keine Freiheit ohne
Risiko.

Ingeborg Zerbes

11 Gesetzesevaluierung

Im Folgenden werden verschiedene bestehende Ansätze der Gesetzesevaluierung zusammengefasst. Dies führt von der vorparlamentarischen Partizipation, die parlamentarische Begutachtungsverfahren und den Konsultationsmechanismus umfasst, zu gesetzlichen Evaluierungsvorschriften wie insbesondere jene zur Wirkungsfolgeabschätzung und zur Datenschutzfolgenabschätzung.

Staatsgrundgesetz

11.1 Vorparlamentarische Partizipation

Die Mehrheit der Gesetzesbeschlüsse in Österreich geht auf Regierungsvorlagen zurück. Zwischen 1975 und 2001 betraf dies 70 % der Gesetzesbeschlüsse im Parlament.[1] Diesen Regierungsvorlagen geht der sogenannte vorparlamentarische Prozess voraus.[2] Dieser vorparlamentarische Prozess bildet also die Grundlage der meisten Gesetze, daher hat ein Handbuch zur besseren Rechtsetzung auch ihn zu umfassen. Die primäre Rechtsgrundlage ergibt sich aus der „Vereinbarung zwischen dem Bund, den Ländern und den Gemeinden über einen Konsultationsmechanismus und einen künftigen Stabilitätspakt der Gebietskörperschaften“, daneben ergeben sich aus dem Deregulierungsgrundsätzegesetz und den bereits behandelten Rechtsgrundlagen zur wirkungsorientierten Folgenabschätzung (WFA, siehe unten 11.2) weitere rechtliche Rahmenbedingungen für den vorparlamentarischen Prozess.

BGBl. I Nr. 35/1999

BGBl. I Nr. 45/2017

11.1.1 Begutachtungsverfahren

Kern dieses vorparlamentarischen Prozesses ist das gesetzlich nicht näher geregelte öffentliche Begutachtungsverfahren.[3] Es gibt jedoch Rundschreiben des Bundeskanzler_innenamtes, die Mindeststandards wie die Begutachtungsdauer festlegen. Allerdings kann von diesen Mindeststandards abgewichen werden.[4] Grundsätzlich entwirft das zuständige Ministerium zuerst einen so genannten Ministerialentwurf. Dieser wird dann auf der Parlamentswebseite öffentlich zugänglich gemacht[5]. Zu diesen Ministerialentwürfen kann dann jede juristische und natürliche Person eine Stellungnahme abgeben, in der sie ihre Zustimmung, Ablehnung oder Detailkritik ausformuliert. Diese Stellungnahmen werden wiederum ebenfalls auf der Parlamentshomepage veröffentlicht. Nach Ablauf der Frist überarbeitet das Ministerium darauf erneut den Entwurf, wobei es bis dahin eingelangte Stellungnahmen berücksichtigen kann. Der finale Entwurf wird dann vom Minister_innenrat abgestimmt und mit einstimmiger Mehrheit als Regierungsvorlage im Parlament eingereicht.[6] Durch die Einbindung der Rechtsunterworfenen wird das Begutachtungsverfahren als wertvolles Instrument der österreichischen Demokratie bewertet.[7] In der XXV. Legislaturperiode gab es 329 solcher Begutachtungen bei 454 Regierungsvorlagen. Wobei nur 77 der 197 nicht begutachteten Vorlagen gewöhnliche Gesetze darstellten, der Rest waren Staatsverträge, Minister_innenratserlässe und 15a-Vereinbarungen. Eine Sonderform der Begutachtung stellt die Ausschussbegutachtung dar. Diese kann von einem Ausschuss auf Grundlage des § 40 GOG beschlossen werden und läuft nach demselben Schema der gewöhnlichen Begutachtung ab. Sie findet jedoch nicht im vorparlamentarischen sondern im parlamentarischen Prozess statt und kann auch für selbstständige Anträge angewendet werden.
Die Begutachtung bietet Bürger_innen und Grundrechtsorganisationen die Möglichkeit, vorab ihre Kritik zu einem Gesetzesvorhaben kund zu tun[8]. Oftmals findet jedoch keine Begutachtung statt; insbesondere werden Initiativanträge der Regierungsparteien genutzt, um die öffentliche Begutachtung und den Konsultationsmechanismus zu umgehen.[9]

BGBl. Nr. 410/1975 zuletzt geändert durch BGBl. Nr. 720/1988

11.1.2 Konsultationsmechanismus

Im Gegensatz zur nicht verpflichtenden öffentlichen Begutachtung ist der Konsultationsmechanismus gesetzlich festgelegt. Hierbei haben die Bundesministerien den Ämtern der Landesregierungen, dem Österreichischen Gemeindebund und dem Österreichischen Städtebund Gesetzesentwürfe zu übermitteln. Diese können wiederum in einem Konsultationsgremium innerhalb einer gewissen Frist ein Verlangen auf Verhandlungen stellen, wenn dem_der Antragsteller_in durch den Entwurf finanzielle Mehrausgaben drohen würden. Der Konsultationsmechanismus deckt nur finanzielle Bedenken ab, nicht aber z.B. Grundrechtsbedenken zu Gesetzesentwürfen.

BGBl. I Nr. 35/1999

Art. 1 Abs. 1 KMSPG, BGBl. I Nr. 35/1999

Art. 2 Abs. 1 KMSPG BGBl. I Nr. 35/1999

11.2 Wirkungsorientierte Folgenabschätzung (WFA)

Gesetze mit der Zielsetzung der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit sind fast immer mit Erlaubnistatbeständen für Grundrechtseingriffe verbunden. Die erlaubten Grundrechtseingriffe sind aber in der Regel nicht nur für die Personen bedeutsam, die unmittelbar von der Vollziehung betroffen sind. Es besteht eine Wechselwirkung auf die gesamte Gesellschaft. Je komplexer die Zusammenhänge sowohl sozial-, als auch rechtswissenschaftlich sind, desto umsichtiger muss das Vorgehen bei der Einführung neuer Eingriffe besonders durch neue Technologien zur Überwachung und Ermittlung gestaltet sein. Frei nach dem Motto „Technologie ist die Antwort – aber was war nochmal die Frage?“ muss stets klar sein, dass die Technologie dem Menschen und der Wahrung seiner Würde dient. Nur legitime Ziele dürfen ausschließlich mit verhältnismäßigen Mitteln auf Basis demokratischer Gesetze verfolgt werden.[10] Diese Mittel-Zweck-Beziehung muss sachlich nachvollziehbar sein, also rational begründet, das erfordert letztlich schon der Gleichheitsgrundsatz der auch als objektives Prinzip der Sachlichkeit verstanden wird. Die Wirkungsorientierung soll ein Analyse- und Steuerungsinstrument für die Planung von Maßnahmen zur Beseitigung oder zur Verminderung gesellschaftlicher Problemlagen bieten; sie liefert im Idealfall „systematisch Informationen über Herausforderungen, Handlungsmöglichkeiten und deren Auswirkungen. Sie orientiert sich an gesellschaftlichen und ökonomischen Notwendigkeiten und ist nach innen und außen so angelegt, dass Innovation und Entwicklung systematisch eingebaut sind und integrativ gedacht werden können.“[11] Die wirkungsorientierte Folgenabschätzung ist ein Verfahren, in dem die Regelungs- oder Vorhabensziele und -maßnahmen formuliert, sowie die wesentlichen Auswirkungen eines Regelungsvorhabens oder Vorhabens von außerordentlicher finanzieller Bedeutung in konkreten Wirkungsdimensionen systematisch untersucht, bewertet und aufbereitet werden. Bei Entwürfen für Rechtsvorschriften des Bundes ist die wirkungsorientierte Folgenabschätzung grundsätzlich so früh wie möglich zu beginnen. Sie hat mit dem Regelungsvorhaben Schritt zu halten. Die Ergebnisdarstellung hat bei jedem Eintritt in ein neues Verfahrensstadium (Versendung zur Begutachtung, Einbringung in den Minister_innenrat) vorzuliegen. Es müssen also insbesondere die legistischen Mitarbeiter_innen der Bundesministerien handeln, aber auch das Kabinett der jeweiligen Minister_innen steht in der Pflicht.

Vgl. den Eingriffsvorbehalt in Art. 8 Abs. 2 EMRK

Art. 7 B-VG

§ 17 BHG 2013, § 4 Z 1 WFA-Grundsatz-Verordnung – WFA-GV

11.2.1 Dimensionen der WFA

§ 6 WFA-GV Wirkungsdimensionen

Der breite gesellschaftspolitische Ansatz der wirkungsorientierten Folgenabschätzung (WFA) bei Gesetzesvorhaben ist grundsätzlich richtig. In der Praxis der österreichischen Gesetzgebung zeigt sich jedoch, dass dieser wohlgemeinte Ansatz häufig ins Leere läuft. Insbesondere bei eingriffsintensiven Gesetzesvorhaben der jüngeren Vergangenheit, bspw. beim Polizeilichen Staatsschutzgesetz (PStSG) oder dem sog. Sicherheitspaket inklusive der Ermittlungsmaßnahme „Überwachung von verschlüsselten Nachrichten“, zeigt sich, dass die grundrechtlichen Auswirkungen dieser Gesetzesvorhaben in der WFA überhaupt nicht berücksichtigt wurden. Dies führt auch dazu, dass es in der Folge gerade in letzter Zeit häufiger zu erfolgreichen Gesetzesprüfungsanträgen vor dem Verfassungsgerichtshof kommt[12], nicht selten durch einen Schulterschluss zwischen Abgeordneten zum Parlament und zivilgesellschaftlichen Organisationen. In den genannten Fällen beziehen sich die WFAs in der Regel ausschließlich auf finanzielle bzw. budgetäre Auswirkungen und lassen die Auswirkungen von Beschränkungen der Freiheitsrechte für das Individuum und sowie eine demokratische Gesellschaft insgesamt außen vor. Dabei enthält die Rechtsordnung ausdrückliche Vorgaben, welche Wirkungsdimensionen eine WFA zu berücksichtigen hat:

Sicherheitspaket

Bundestrojaner

§ 6 Abs. 2 WFA-GV iVm § 17 Abs. 4 Z 3 BHG 2013 iVm WFA-Finanzielle-Auswirkungen-Verordnung (WFA-FinAV), BGBl. II Nr. 490/2012

Verweis: § 6 (WFA-Grundsatz-Verordnung – WFA-GV) iVm § 17 Abs. 1 BHG 2013

1. Gesamtwirtschaft,
2. Unternehmen,
3. Umwelt,
4. Konsumentenschutzpolitik,
5. Verwaltungskosten für Bürgerinnen und Bürger und für Unternehmen,
6. Soziales,
7. Kinder und Jugend,
8. Tatsächliche Gleichstellung von Frauen und Männern

Die Grundrechte spielen bei all diesen Dimensionen – mehr oder weniger ausgeprägt – eine wesentliche Rolle und definieren gewissermaßen auch absolute materielle Grenzen. Dieser Katalog sollte aber nicht als Beschränkung verstanden werden. So bietet etwa der Punkt „Soziales“ den Spielraum, sich mit gewichtigen Grundrechtseingriffen auseinanderzusetzen, auch wenn dies keine der sonst aufgezählten Dimensionen unmittelbar betrifft.
Für die Beurteilung der Zulässigkeit der gesetzlich normierten Grundrechtseingriffe ist dabei auch wesentlich, dass eine isolierte Betrachtung einzelner Befugnisse nicht ausreicht. Vielmehr sind einerseits die konkreten Ermittlungs- und Eingriffsbefugnisse in Zusammenschau mit den Tatbeständen des materiellen Strafrechts sowie mit komplementären und überlappenden Befugnissen derselben Organe nach anderen Gesetzen (StPO, SPG) zu sehen. Andererseits sind auch die verfügbaren Technologien, deren mehr oder weniger präzise gesetzliche Erfassung sowie deren Eignung für Grundrechtseingriffe zu berücksichtigen.
Das deutsche Bundesverfassungsgericht hat in dessen Urteil zur Aufhebung der deutschen nationalen Umsetzung der Vorratsdatenspeicherung ausgeführt, dass eine staatliche Überwachungsmaßnahme bzw. deren Verhältnismäßigkeit nur beurteilt werden kann, wenn man diese in Zusammenschau mit anderen, bereits bestehenden Befugnissen betrachtet. Durch die Summe aller Eingriffe könne sich ergeben, dass der Spielraum des Gesetzgebers zur Normierung neuer Befugnisse enger wird. Damit beschreibt das deutsche Bundesverfassungsgericht im Prinzip die Notwendigkeit einer Art „Überwachungs-Gesamtrechnung“. Die Verordnung des Bundeskanzlers über Grundsätze der wirkungsorientierten Folgenabschätzung bei Regelungsvorhaben und sonstigen Vorhaben (WFA-Grundsatz-Verordnung – WFA-GV) ist zwar ein wichtiger Ansatz, schafft aber offenbar keinen hinreichenden Anreiz, den umfassenden Zugang in der Praxis umzusetzen.

BVerfG, 1 BvR 256/08 u.a. vom 2.3.2010 (FN 64), Rz 218.

Überwachungsgesamtrechnung

BGBl. II Nr. 67/2015

11.2.2 Grundrechtliche Gewährleistungspflichten und technische Gestaltungspflichten

Der hier fokussierte Bereich der öffentlichen Sicherheit steht praktisch in einem permanenten Spannungsverhältnis von Grundrechts-Kollisionen, die der Staat bestmöglich nach dem Verhältnismäßigkeitsgrundsatz ausbalancieren muss. Eingriffe in die Grundrechte der Subjekte der Ermittlungshandlungen sind in der Regel erforderlich, weil sie dem Schutz der Rechte und Freiheiten anderer Menschen, deren Rechtsgüter bedroht sind, dienen. Der Staat muss Gesetze so ausgestalten, dass die Rechtsordnung einen wirksamen Schutz der verschiedenen Grundrechtspositionen bietet. Die Grundrechte enthalten dabei immer nur normative Anordnungen und beziehen sich insofern auf eine bestimmte Gestaltung von Rechtsnormen. Die Grundrechte haben damit in ihren unterschiedlichen Wirkungsdimensionen Einfluss auf die Entwicklung neuer Technologien und deren Innovationspfade, ungewollte Schäden sollen durch grundrechtliche Schutz- und Gewährleistungspflichten verhindert werden.[13] Verändert hat sich der normative Druck zur Durchführung einer Folgenabschätzung durch die EU Datenschutz-Reform, nach der in bestimmten Fällen zwingenden Vorgabe zur Durchführung einer umfassenden Datenschutz-Folgenabschätzung. Soweit mit einem Gesetzesvorhaben besonders hohe Risiken bei der Verarbeitung personenbezogener Daten zu erwarten sind, muss eine vorgelagerte Datenschutz-Folgenabschätzung als Voraussetzung der Rechtmäßigkeit durchgeführt und dokumentiert werden.

➲ *9.1.3 Verhältnismäßigkeitsprüfung*

Personenbezogene Daten

11.2.3 Datenschutzrecht als Modell

Das Datenschutzrecht eignet sich gut als Modell für einen risikobasierten Ansatz mit verpflichtender Folgenabschätzung. Das Grundrecht auf Datenschutz ist nicht Selbstzweck. Nicht die Daten sind schutzwürdig, sondern die Personen, auf welche sie sich beziehen. Schutzwürdige Positionen erwachsen dabei vor allem aus den verschiedenen Grundrechtsgarantien. Häufig lässt sich eine direkte Beziehung zwischen einem festgestellten Risiko und einer durch ein bestimmtes Grundrecht geschützten Sphäre des betroffenen Menschen herstellen. Insofern ist Datenschutz eine Art „Katalysator-Grundrecht“, das seinen eigentlichen Gehalt aus der gesamten Grundrechtsordnung und letztlich dem Schutz der Würde des Menschen bezieht. Das Datenschutzgrundrecht und dessen Ausgestaltung durch Sekundärrecht und nationales Recht eignet sich insbesondere als Modell für einen modernen Ansatz in der Gestaltung von IT-Systemen im Dienste der Hoheitsverwaltung. Es bietet ein dynamisches, risikobasiertes Konzept, welches jede Systemgestaltung in seinem Anwendungsbereich ab der ersten Planung normativ erfasst und leitet. Datenschutz ist dabei nicht nur auf den Schutz der Privatsphäre sondern generisch auf den Schutz aller Grundrechte gerichtet. Bezogen auf IT-Systeme zum Einsatz in der Hoheitsverwaltung besteht außerdem eine sehr große Schnittmenge von Datenverarbeitungen innerhalb und außerhalb des Schutzbereichs des Datenschutzrechts. In der Regel werden personenbezogene Daten verarbeitet und das Datenschutzrecht ist unmittelbar auf die Sachverhalte anwendbar.
Sofern die jeweils beachtlichen Verfahrensvorschriften ein wesentliches Element des Grundrechtsschutzes darstellen (Risikobezug), sind diese in der

➲ *9.2 Privatleben und Datenschutz*

Technikgestaltung auch umzusetzen. Im Kontext moderner Informationstechnologie sind Fragen technologischer Sicherungsmechanismen untrennbar mit den Risiken für die Menschen und die Gesellschaft verknüpft. So ist etwa die tatsächliche Umsetzung von (Zugriffs-)Dokumentations- und Informationspflichten eine unabdingbare Voraussetzung für einen effektiven Rechtsschutz im Hinblick auf die Gewährleistung der „informationellen Selbstbestimmung". Wenn diese nicht im System automatisiert umgesetzt werden, sondern allein auf Basis organisatorischer Vorgaben durch menschliches Zutun erfolgen sollen, ist die Wirksamkeit in Zweifel zu ziehen, insbesondere bei hoch skalierenden und komplexen Systemen. Die Einhaltung komplexer Vorgaben kann in den Informationsprozessen nicht primär davon abhängig gemacht werden, dass die Rechts- und Systemanwender jederzeit explizite Kenntnis der normativen Vorgaben haben.
Angesichts einer unüberschaubaren Zahl von Informationsverarbeitungsprozessen in ebenso unzähligen Verwaltungsbereichen lassen sich diese Aufgaben nur mit Hilfe entsprechender elektronischer Hilfsmittel bewältigen. Je komplexer die Aufgabenstellung und je höher die Risiken für die Beteiligten, desto mehr Aufwand ist geboten, um die Einhaltung der verfahrensrechtlichen Sicherungsvorschriften so in ein System einzubauen, dass die Anwender_innen gar nicht anders können als rechtlich korrekt zu handeln. Dort, wo notwendigerweise Handlungs- und Entscheidungsspielräume bestehen bleiben müssen, ist mit flankierenden organisatorischen (und technisch abgesicherten) Maßnahmen in die Bahnen für rechtlich und sachlich richtige Entscheidungen zu lenken.

11.2.4 Datenschutzrecht für Polizei und Justiz

Polizei-DSRL
➲
10.1 Datenschutz im Polizeibereich

Der Anwendungsbereich der Polizei-DSRL umfasst die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Auf jede andere Verarbeitung solcher Daten, und somit insbesondere auch für jede Datenverarbeitung durch Private – auch zu einem der genannten Zwecke – ist die DSGVO (unmittelbar) anzuwenden.[14]
Der wichtigste Grundsatz der Polizei-DSRL ist in Art. 8 vorgesehen und entspricht Art. 8 Abs. 2 Grundrechtecharta (GRC) sowie Art. 8 Abs. 2 der Europäischen Menschenrechtskonvention (EMRK): Die Verarbeitung personenbezogener Daten ist nur dann rechtmäßig, wenn sie für einen der in Art. 1 Abs. 1 Polizei-DSRL genannten Zwecke erforderlich ist und auf und auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten erfolgt. Eine solche Regelung eines Mitgliedstaats hat zumindest die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung festzulegen.
Zur Datenverarbeitung durch Polizeibehörden existieren darüber hinaus noch die folgenden spezifischen Regeln:

- INTERPOL: Rules on the Processing of Data (RPD), neu seit 1. Juli 2012, bieten klare Datenschutzregeln in Bezug auf jede einzelne Datenkategorie und beinhalten eine technische Abbildung der Datenschutzregeln im Design.[15]

- Europol – SIENA (Secure Information Exchange Network Application) basierend auf dem Beschluss des Rates 2009/371/JHA, normiert das Europol Information System (Art. 11), Datensicherheitsmaßnahmen (Art. 35), sowie automatisierte Durchsetzung von „handling codes".

- Schengen Information System (SIS) / das Schengener Durchführungsübereinkommen (SDÜ) normiert Datenschutz in Art. 103 und Art. 126 SDÜ und enthält einen Verweis auf die Empfehlung Nr R (87) 15 sowie einen strengen Zweckbindungsgrundsatz (Art. 102 SDÜ).

- Empfehlung Nr R (87) 15 des Minister_innenkomitees des Europarates vom 17.09.1987 zur Regelung der Benutzung personenbezogener Daten im Polizeibereich.[16] Sie ist nicht unmittelbar rechtsverbindlich aber materiell gültig durch zahlreiche Verweise im EU Recht, z.B. Europol, „Swedish Initiative" (Rahmenbeschluss 2006/960/JHA).

Die vorgestellten Regelwerke sind keine Grundrechtsnormen. Sie enthalten aber vielfach konkrete Vorgaben, die in der Praxis durch eine rechtskonforme Technologiegestaltung, zu der das Recht selbst an vielen Stellen konkrete Anleitungen enthält, faktisch die größte mögliche Wirksamkeit erreichen[17]. Eine Technologiegestaltung, die auf solche Maßnahmen verzichtet, ist nicht auf dem Stand der Technik[18].

rechtskonforme Technologiegestaltung in der Praxis

11.2.5 Datenschutz-Folgenabschätzung im Bereich Strafrecht und Sicherheitspolizeirecht

Sowohl Art. 35 DSGVO als auch Art. 27 Polizei-DSRL (umgesetzt in § 52 DSG, der wiederum auf Art. 35 Abs. 1, 2, 3, 7 und 11 DSGVO verweist) sehen für eine Form der Verarbeitung (insbesondere bei Verwendung neuer Technologien), die aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, die vorherige Durchführung einer Datenschutz-Folgenabschätzung (DSFA) vor.[19] Die Pflicht zur Durchführung einer DSFA intendiert die Erkennung und Evaluierung möglicher mit der geplanten Verarbeitung einhergehender Risiken für die Rechte und Freiheiten natürlicher Personen, insbesondere hinsichtlich ihrer Ursache, Art, Besonderheit und Schwere, vor Aufnahme der Verarbeitung. Somit kann diese von vorn herein so gestaltet werden, dass diese Risiken möglichst minimiert werden. Die DSFA nach Art. 35 DSGVO und § 52 DSG steht in engem Zusammenhang mit den Art. 24, 25 und 32 DSGVO, respektive §§ 46 und 54 DSG. Insbesondere sollen sich die Ergebnisse einer DSFA in den Privacy-by-Design-Maßnahmen niederschlagen, die nach § 46 DSG bzw. Art. 25 DSGVO zu treffen sind.[20]

Erforderlichkeit einer Datenschutz-Folgenabschätzung

Art. 35 Abs. 1 DSGVO bzw. Art. 27 Abs. 1 Polizei-DSRL iVm § 52 DSG

Die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) ist nicht für alle Verarbeitungsvorgänge vorgeschrieben, bei denen die (bloße) Möglichkeit eines Risikos für die Rechte und Freiheiten natürlicher Personen besteht. Notwendig wird die Durchführung einer DSFA jedoch in Fällen, wo „die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge [hat]"[21].

Vgl. auch § 52 DSG

In Art. 35 Abs. 3 DSGVO sind beispielhaft einige Situationen angeführt, in denen ein Verarbeitungsvorgang „voraussichtlich ein hohes Risiko mit sich bringt":

> a) Die systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

🕮
Profiling

➲
10.1.1 Besondere Kategorien von Daten

b) Die umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10;

c) Die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Laut Erwägungsgrund 52 der Polizei-DSRL ist ein hohes Risiko „ein besonderes Risiko der Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen."
Darüber hinaus hat die Artikel-29-Datenschutzgruppe – das ist die Vorgänger-Institution des nunmehrigen Europäischen Datenschutzausschusses (EDSA)[22], in dem alle Datenschutzbehörden der EU Mitgliedsstaaten koordiniert sind – neun Kriterien ermittelt, bei deren Vorliegen aufgrund des immanenten hohen Risikos die Durchführung einer Datenschutz-Folgenabschätzung erforderlich sein kann:[23]

EU-weite Kriterien als Indikatoren für eine nötige DSFA

- Profiling/Scoring natürlicher Personen („Bewerten oder Einstufen" z.B. durch Verhaltens- oder Marketingprofile)
- Automatisierte Entscheidungen, die rechtliche oder vergleichbare Wirkung gegenüber natürlichen Personen entfalten
- Systematische Überwachung

Art. 10 DSGVO

- Vertrauliche Daten oder höchst persönliche Daten: besonders sensible Kategorien personenbezogener Daten sowie personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten
- Datenverarbeitung in großem Umfang
- Verknüpfung verschiedener Datenbestände (Abgleichen oder Zusammenführen)
- Daten schutzbedürftiger natürlicher Personen (Kinder, Arbeitnehmer_innen, Patient_innen etc.)
- Innovative Anwendung neuer technologischer oder organisatorischer Lösungen
- Datenverarbeitungen, die Betroffene an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrages hindern

Erfüllt ein Verarbeitungsvorgang laut Artikel-29-Datenschutzgruppe mindestens zwei dieser Kriterien, muss der für die Datenverarbeitung Verantwortliche in den meisten Fällen zu dem Schluss kommen, dass eine DSFA verpflichtend ist. Es liegen folgende drei der oben genannten Kriterien in fast allen Vorhaben im Bereich Polizei und Justiz, in denen Technologie involviert ist, vor: Datenverarbeitung in großem Umfang, Verknüpfung verschiedener Datenbestände (Abgleichen oder Zusammenführen von Datensätzen), Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen.
Selbst für den Fall, dass unklar wäre, ob eine DSFA erforderlich ist, empfiehlt die Artikel-29-Datenschutzgruppe dennoch die Durchführung einer DSFA, weil den für die Verarbeitung Verantwortlichen damit ein hilfreiches Instrument für die Einhaltung der Datenschutzgesetze zur Verfügung steht.[24]

DSFA-AV und DSFA-V

Wichtige innerstaatliche Quellen zur Beurteilung der Notwendigkeit einer DSFA sind zwei Verordnungen der österreichischen Datenschutzbehörde mit Geltung für Österreich. Dies ist einerseits die Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV), die eine Liste der Arten von Verarbeitungsvorgängen enthält, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Andererseits beachtlich ist die Verordnung über Verarbeitungsvorgänge, für die eine Datenschutz-Folgeabschätzung erforderlich ist (DSFA-V). Letztere enthält eine Liste der Arten von Verarbeitungsvorgängen, für die jedenfalls eine Datenschutz-Folgenabschätzung erforderlich ist. Weil § 52 DSG für den Bereich der Polizei-DSRL einfach nur auf Art. 35 DSGVO verweist, ist anzunehmen, dass beide Verordnungen auch in diesem Anwendungsbereich gelten. Praktisch wichtig sind hier vor allem die Fälle der Videoüberwachung, die Aufgrund der DSFA-V im öffentlichen Bereich in den meisten Konstellationen die Pflicht zur DSFA auslösen. Die Ausnahmen sind dagegen hauptsächlich sog. Standard-Anwendungen, die nach der früheren Rechtslage im Datenschutzrecht von einer Meldepflicht ausgenommen waren.

Art. 35 Abs. 5 DSGVO

Art. 35 Abs. 4 DSGVO

11.3 Menschenwürde und Rechtsstaatlichkeit durch Technikgestaltung[25]

Die Wirkungsfolgenabschätzung (WFA) soll sich also am Datenschutzrecht orientieren, weil es hier eine hohe Regelungsdichte gibt und die Vorgaben sehr streng sind. Im Hinblick auf einen umfassenden (gesamtheitlichen) Zugang einer WFA sollte dieser methodische Ansatz aber nicht streng auf den Anwendungsbereich des Datenschutzrechts beschränkt sein. Vielmehr sollte darauf abgestellt werden, ob es durch die geplanten Vorhaben zu Grundrechtseingriffen kommt und ob diesbezüglich verfahrensrechtliche Garantien zur Absicherung existieren.
Die WFA an der Datenschutz-Folgenabschätzung zu orientieren bringt vor allem den Vorteil, dass dort auch die technische Gestaltung von Systemen zur Datenverarbeitung adressiert ist. Ihre Schutzbedürftigkeit ist von den dahinterstehenden Zusammenhängen und den damit verbundenen Risiken her zu beurteilen.
Diesem Ansatz wird der neue in Art. 25 DSGVO und Art. 20 Polizei-DSRL verankerte Grundsatz „Datenschutz durch Technikgestaltung" in vorbildlicher Weise gerecht. Eine vorgelagerte Datenschutz-Folgenabschätzung macht die Risiken transparent und verlangt die Formulierung technischer und organisatorischer Maßnahmen zur Reduktion oder bestenfalls Elimination dieser Risiken. Der Grundsatz „Datenschutz durch Technikgestaltung" sorgt nun dafür, dass diese Maßnahmen (bei sonstigen Sanktionen gegen den Verantwortlichen) auch unmittelbar in die Systeme „eingebaut" werden.[26] Damit ist logisch zwingend verbunden, die Grundsätze bereits in der Normierung des Systems zu konkretisieren.
Die Wurzel aller Grundrechtsgarantien ist die unantastbare Würde des Menschen. Weil der Datenschutz nicht Selbstzweck ist und immer im Hinblick auf den Schutzzweck und die Risiken der Betroffenen auszulegen ist, liegt in der Gewährleistung der Menschenwürde bei der Verarbeitung personenbezogener Daten der ultimative Schutzzweck des Datenschutzrechts begründet. Gut sichtbar wird dies im großen Feld der Datenverarbeitung im Beschäftigungskontext (Arbeitnehmer_innen-Datenschutz).
Die Situation am Arbeitsplatz ist gewissermaßen eine Art Mikrokosmos im Verhältnis zum Staat und zur Gesellschaft. Dieselben Fragen stellen sich auf der gesamt-gesellschaftlichen Ebene, weshalb das Arbeitsrecht hier eine gute Orientierung bietet. Außerdem hat der Oberste Gerichtshof in diesem Zusammenhang den Begriff der „Würde des Menschen" bereits durch Judikatur konkretisiert.[27] „Human Dignity by Design" oder „eingebaute Menschenwürde" heißt, solche konkreten Kriterien der Menschenwürde vom ersten Moment der Gestaltung von Eingriffen – durch Normen oder durch Technologieentwicklung – zu Berücksichtigen und den Vorgaben möglichst effektiv zur Umsetzung zu verhelfen.

Das hier weiters vorgestellte Konzept „Rechtsstaatlichkeit durch Technikgestaltung“ versucht zu begründen, dass eine möglichst präzise Umsetzung rechtlicher Vorgaben durch Technologie ein verfassungsrechtlicher Imperativ ist, wenn die Vorgaben dem Schutz bestimmter Grundrechte dienen. Ein solches Prinzip – unabhängig vom Datenschutzgrundrecht oder den neuen Regeln nach der DSGVO und der Polizei-DSRL– ist für den allgemeinen Bereich des Verwaltungshandelns speziell im Hinblick auf die Absicherung von Verfahrensvorschriften aus der Verfassung abzuleiten.
Ein konkretes Beispiel hierfür ist das Konzept der Durchlaufstelle (DLS), die Schnittstelle zur Übergabe der Daten zwischen Behörden und Telekommunikationsanbietern. Diese stellt eine Art elektronisches Postfach dar, über das anfragende und angefragte Stellen miteinander kommunizieren und Informationen sicher austauschen. Die DLS ist ein Modell für technische und prozedurale Abläufe, nicht jedoch eine Art neue Behörde oder Dienststelle. Normiert wurde die DLS durch die „Verordnung der Bundesministerin für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO)“[28]. Die DLS normiert zahlreiche Vorschriften, beispielsweise zu Protokollierung, uniq-ID, Anforderungsvoraussetzungen wie ein Gerichtsbeschluss oder eine Anordnung der StA oder die zwingende Zuordnung vorgegebener Rechtsgrundlagen, die letztlich bezwecken, die Rechtsstaatlichkeit in der Anwendung sicherzustellen.

11.4 Schlussfolgerungen

Vorhaben des Gesetzgebers müssen durch eine umfassende WFA zur Sachlichkeit und Verhältnismäßigkeit geführt werden. Aus Sicht der Grundrechte ist die WFA umfassend durchzuführen und wenn Grundrechtseingriffe dies nahelegen auch über die Kriterien der WFA-GV hinaus zu behandeln. Das Datenschutzrecht bietet mit dem neuen – bei hohen Risiken verpflichtenden – Konzept der Datenschutz-Folgenabschätzung einen sehr detaillierten Orientierungsrahmen hierfür. Nach den hier knapp dargestellten neuen Ansätzen „Rechtsstaatlichkeit durch Technik“ und „Menschenwürde durch Technik“ ist der Gestaltungsansatz, den das Datenschutzrecht mittlerweile bietet, auch zur Übertragung auf Bereiche geeignet, bei denen die Anwendbarkeit des Datenschutzrechts nicht (uneingeschränkt) gegeben ist. Der Ansatz ist insofern verallgemeinerungsfähig und soll helfen, das Konzept der WFA in der Praxis effektiver umsetzen zu können und dafür nachvollziehbare Strukturen zu finden.

Endnoten

1 Vgl. *Bischof*, Der Verbandseinfluss auf die Gesetzgebung in Österreich und Deutschland (2004) 5f.
2 Vgl. *Pelinka*, Das politische System Österreichs, in *Ismayr* (Hrsg.) Die politischen Systeme Westeuropas[4] (2009) 618.
3 Vgl. *Stephan*, Öffentlichkeitsbeteiligung im Gesetzgebungsprozess (2015) 56.
4 Vgl. Rundschreiben des Bundeskanzleramts, Begutachtungsverfahren; Festsetzung angemessener Begutachtungsfristen, BKA-600.614/0002-V/2/2008, (https://www.ris.bka.gv.at/Dokumente/Erlaesse/ERL_BKA_20080602_BKA_600_614_0002_V_2_2008/ERL_BKA_20080602_BKA_600_614_0002_V_2_2008.pdf). https://web.archive.org/web/20090207201911/http://www.bka.gv.at/site/3513/default.aspx (04.02.2020).
5 Vgl. Österreichisches Parlament, Begutachtungsverfahren und Stellungnahmen, https://www.parlament.gv.at/PAKT/MESN/ (04.02.2020).
6 Vgl. *Pelinka*, Das politische System Österreichs, in *Ismayr* (Hrsg.) Die politischen Systeme Westeuropas (2009[4]) 618.
7 Vgl. *Stephan*, Öffentlichkeitsbeteiligung im Gesetzgebungsprozess (2015) 35.
8 Vgl. ebd.
9 Vgl. *Pelinka*, Das politische System Österreichs, in *Ismayr* (Hrsg.) Die politischen Systeme Westeuropas (2009[4])
10 Vgl. die Grundrechtsprüfung des EuGH insbesondere in den Fällen einer Abwägung zwischen den in den Art. 7 und 8 GRC verankerten Grundrechten auf Achtung des Privatlebens und auf Schutz personenbezogener Daten und dem durch Art. 11 GRC gewährleisteten Grundrecht auf freie Information, z.B. EuGH 24. 9. 2019, C136/17, CNIL vs Google, Rz 58 ff; siehe auch *Hötzendorfer/Tschohl/Kastelitz* in *Knyrim*, DatKomm Art. 5 DSGVO, Rz 7.
11 *Ostermayer*, Vorwort des Bundesministers für Kunst und Kultur, Verfassung und öffentlichen Dienst, Bundeskanzleramt, Bericht über die wirkungsorientierte Folgenabschätzung (2014). (https://www.oeffentlicherdienst.gv.at/wirkungsorientierte_verwaltung/berichte_service/WFA-Bericht_2014.pdf?6wd88r, 3)
12 Vgl. VfGH 11.12.2019, G 72-74/2019-48, G 181-182/2019-18, Rz 195; vgl. Verfassungsgerichtshof, Kfz-Kennzeichenerfassung und „Bundestrojaner“ verfassungswidrig, 11.12.2019, https://www.vfgh.gv.at/medien/Kfz-Kennzeichenerfassung_und___Bundestrojaner___verfass.de.php (19.12.2019).
13 Vgl. *Eisenberger*, Technik der Grundrechte – Grundrechte der Technik, in *Holoubek/Martin/Schwarzer* (Hrsg.), Die Zukunft der Verfassung – Die Verfassung der Zukunft? Festschrift für Karl Korinek zum 70. Geburtstag (2010) 128.
14 Zur Abgrenzung zwischen DSGVO und Polizei-DSRL siehe *Dörnhofer*, Datenschutz im Strafverfolgungsbereich: Schnittstellen und Abgrenzungsfragen – Das Zusammenspiel zwischen DSGVO und Polizei-DSRL, in *Knyrim* (Hrsg.), Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, (2016) 401–411.
15 Vgl. Online bei Interpol https://www.interpol.int/News-and-Events/News/2019/INTERPOL-reviews-its-rules-for-the-international-exchange-of-criminal-data (30.01.2020).
16 Vgl. http://ec.europa.eu/justice/dataprotection/law/files/coe-fra-rpt-2670-en-471.pdf (30.01.2020).
17 Vgl. dazu *Hötzendorfer*, zum Verhältnis von Recht und Technik: Rechtsdurchsetzung durch Technikgestaltung, in Hötzendorfer/Tschohl/Kummer (Hrsg.), International Trends in Legal Informatics, Festschrift für Erich Schweighofer (2020) Kapitel B Grundlagen.
18 Vgl. *Martini* in *Paal/Pauly* (Hrsg.), Datenschutz-Grundverordnung, (2017) Art. 25 Rz 39 mwN.
19 Siehe ausführlich *Kastelitz/Tschohl/Hötzendorfer*: (Datenschutz-)Rechtliche Aspekte der polizeilichen Verarbeitung von Videomassendaten, in *Jahnel* (Hrsg.), Jahrbuch Datenschutzrecht 2019, (2019) 344.
20 Vgl. *Hötzendorfer/Kastelitz* in *Gantschacher/Jelinek/Schmidl/Spanberger* (Hrsg.), Datenschutzgesetz, § 52 vor Anm 1.
21 Siehe Art. 35 Abs. 1 erster Halbsatz DSGVO und wortgleich Art. 27 Abs. 1 erster Halbsatz Polizei-DSRL.
22 *Europäischer Datenschutzausschuss*, Über den EDSA, https://edpb.europa.eu/about-edpb/about-edpb_de (31.01.2020).
23 *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ (WP 248 Rev. 01) 10ff. (https://www.dsb.gv.at/

documents/22758/112500/Leitlinien+zur+Datenschutz-Folgenabschaetzung-wp248-rev-01_de.pdf/2246301e-ffbb-4a03-bf23-797fee89174e)

24 Vgl. *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ (WP 248 Rev. 01) 9.

25 Siehe *Tschohl*, Zum Verhältnis von Recht und Technik: Rechtsstaatlichkeit durch Technikgestaltung, in *Hötzendorfer/Tschohl/Kummer* (Hrsg.), International Trends in Legal Informatics, Festschrift für Erich Schweighofer (2020), Anm.: in Druck zur Zeit des Redaktionsschlusses.

26 Vgl. dazu ausführlich *Hötzendorfer*, Zum Verhältnis von Recht und Technik: Rechtsdurchsetzung durch Technikgestaltung, in *Hötzendorfer/Tschohl/Kummer* (Hrsg.), International Trends in Legal Informatics, Festschrift für Erich Schweighofer (2020), Anm.: in Druck zur Zeit des Redaktionsschlusses.

27 8 ObA 288/01p; 9 ObA 109/06d = SZ 2002/83; Ausführlich zum Erfordernis einer Betriebsvereinbarung gem. § 96 Abs. 1 Z 3 ArbVG: *Knyrim/Tien,* Die Datenschutz-Grundverordnung im Beschäftigtenkontext. Auswirkungen der DSGVO auf den Arbeitnehmerdatenschutz, ASoK 2017, 10/2017, 363.

28 BGBl. II Nr. 402/2011, zur DLS siehe insbesondere §§ 8 bis 24 der Verordnung sowie der Verweis in § 25 auf die Schnittstellendefinition EP020 in der Anlage zur Verordnung.

12 Ziel- und Ergebnisorientierung in der Rechtssetzung

Rechtssetzung ist kein Selbstzweck. Jedes einzelne Vorhaben sollte Teil einer politischen Strategie zur Weiterentwicklung eines gedeihlichen Zusammenwirkens und Weiterentwicklung aller Kräfte der Gesellschaft sein. Jedes einzelne Vorhaben und jede einzelne Maßnahme muss daher einem gesamtgesellschaftlichen Wertekatalog zugeordnet werden können. In Österreich müssen beabsichtigte Weiterentwicklungen in den jährlichen „aktuellen Wirkungszielen“ in überschaubare Einzelschritte heruntergebrochen werden. Umgekehrt entstehen zahlreiche Gesetzesinitiativen als Reaktion auf Tagesereignisse und Ad-hoc-Erklärungen von Verantwortungsträgern. Solche Ad-hoc-Entwicklungen mangeln zumeist einer Analyse objektiver Fakten und orientieren sich oft an subjektivem Empfinden, Emotionen und Vorstellungen. Ohne faktenbasierte qualifizierte Abstimmung mit den Zielen für eine strategische Gesellschaftsentwicklung führen solche Vorhaben zu massiven Verschiebungen der demokratischen Grundstrukturen der Republik. Um solchen Entwicklungen keinen Raum zu geben, ist eine qualitative Verbesserung des Gesetzwerdungsprozesses nötig. Gesetzwerdung ist ein gesamthafter, zyklischer Prozess, der von der Zielformulierung über Planung, Umsetzung, Anwendung, Evaluierung und Anpassung (nächster Schritt der Verbesserung) durchgängig zu gestalten ist.

Zahlreiche Ansätze und Einzelmaßnahmen wurden in den letzten Jahren gesetzt, um den Gesetzwerdungsprozess zu verbessern sowie methodische und technologische Unterstützung zu bieten. Hier ist insbesondere auf die Wirkungsfolgen-Grundsatzverordnung (WF-GV) und E-Recht verwiesen, die dabei wichtige Beiträge liefern. Diese beiden Initiativen setzen im Gesamtprozess jedoch sehr spät an. Versäumnisse aus frühen Phasen der einzelnen Vorhaben können hierbei nur in geringem Umfang und mit unnötig großem Aufwand ausgeglichen werden.

Wenn die diese Anforderungen der WF-GV nach Zieldefinition und Problembeschreibung nicht früh genug, sondern z.B. erst im Rahmen der legistischen Umsetzung, als Vorbereitung des Begutachtungsprozesses, erarbeitet werden, fehlen zahlreiche Informationen aus Vorphasen. Indikatoren für eine Erfolgsmessung, die spätere Evaluation, sollten z.B. bereits in der Zieldefinition enthalten sein und bereits bei der legistischen Konzeption berücksichtigt werden. Wir stellen im folgenden Abschnitt einen möglichen, groben Rahmen für die Gestaltung von Gesetzesvorhaben vor.

12.1 Gesetzwerdung als Prozess

Abgeleitet aus einer politischen Gesamtstrategie und den eingemeldeten Anforderungen von Interessensträger_innen (stakeholder) sind Vorhabensbündel und Themenbereiche zu beschreiben, die einer Umsetzung zugeführt werden sollen. Diese Vorhabensbündel versehen mit einer Prioritätsreihung bilden die Elemente des „Portfolios“ für die Vorhabensplanung. Die jeweils betreffenden Teile des Portfolios sind den Verantwortungsträger_innen (zumeist Verantwortliche in Ministerien) zu übergeben.

Plan – Do – Check – Act (PDCA) ist eine Methode für kontinuierliche Weiterentwicklung, die die zyklische Abfolge von einzelnen Entwicklungsvorhaben zeigt. Diese Methode, ursprünglich aus der Qualitätssicherung, wird heute allgemein auf Entwicklungs- und Verbesserungsprozesse angewandt. Diese prozesshafte Weiterentwicklung ist – unabhängig davon, ob sie als solche wahrgenommen und angewandt wird – für jede Art der Weiterentwicklung, die nicht zu einem Stillstand führt, wichtig. Daher ist es sinnvoll, dieses zyklische Vorgehen jedem Entwicklungsprozess zu Grunde zu legen.

12.2 Die einzelnen Schritte

1. Vorhabensanalyse: Aus der Gesamtstrategie sind einzelne umsetzungsrelevante Themen- und Vorhabensbündel abzuleiten, grob inhaltlich zu beschreiben, gegeneinander abzugrenzen und zu dokumentieren. Jedes Vorhaben ist mit Problembeschreibung, Zielsetzung, Priorität, Grobschätzung des erwartetet Umsetzungs- und Betriebsaufwandes als Teil des Gesamtportfolios zu dokumentieren. Ergebnis sollte eine Formulierung der Definition von Wirkungsmechanismen und Aufgabenbündeln sein.

2. Zieldefinition: Mit einer Zieldefinition, die klar, deutlich und detailliert dargestellt, abgestimmt und kommuniziert ist, wird ein wichtiger Teil der Vorhabenserklärung geschaffen. Wenn Verantwortliche und Entscheidungsträger_innen keine konkrete Zielvorgabe haben, kommt es bei der Umsetzung zu Unstimmigkeiten, Meinungsverzweigungen und Fehlinterpretationen. In weiterer Folge führen unklare Zieldefinitionen oft zu Zeit- und Kostenüberschreitungen und Qualitätsmängeln. Eine saubere, grundlegende, stimmige und realistische Zieldefinition ist daher ein must-have für jedes Vorhaben, für Entscheidungsträger und für Umsetzungsverantwortliche. Je nach Situation und Begebenheit kann der Prozess und die eigentliche Zieldefinition mehr oder weniger umfangreich ausfallen. Detailliert und realistisch sollte das Ergebnis jedoch immer ausfallen.
Eine praxisbewährte Methode zur Zielfindung ist z.B. die SMART-Analyse. Die Reduktion auf fünf wesentliche Kriterien unterstützt bei der Erstellung überschaubarer und dennoch hinreichend genauer Zieldefinitionen. Diese Methode kann auch als Controlling-Tool eingesetzt werden, um die Zieldefinition abschließend zu überprüfen: Man fragt sich, sind die Zielangaben S=spezifisch, M=messbar, A=angemessen, R=realistisch und relevant, T=terminierbar.
Ist die Zieldefinition gefunden, formuliert und dokumentiert, sollte sie final an die Entscheidungsträger_innen kommuniziert werden. Alle Informationen sollten detailliert abgestimmt werden, sodass die Freigabe gesetzt und der Startschuss für das Vorhaben erfolgen kann.[1]

3. Zuweisung der Verantwortung für Themenbereiche: Aus dem Gesamtportfolio werden Vorhabensbündel und Einzelvorhaben den adäquaten Verantwortungsträger_innen – zumeist innerhalb der Hierarchie der jeweiligen Fachministerienentsprechend der allgemeinen Aufgabenzuordnung (Bundesministeriengesetz) – zugewiesen. Im Rahmen der Themenverantwortlichkeit wird ein_e Verantwortliche_r je einzelnem Vorhaben festgelegt. Diese Vorhabensverantwortlichen begleiten die ihnen zugewiesenen Vorhaben bis zur Umsetzung und sichern dabei Kontinuität und Vollständigkeit der Dokumentation für den gesamten Vorhabensablauf.
Ergebnis sollte die Aufgabenverteilung und Zuweisung zu Fachbereichen (Ministerien) sein: Die Verantwortung für Aufgaben und Aufgabenbündel sind innerhalb der Verantwortungsbereiche (zumeist Ministerien) konkreten Personen für die weitere Gestaltung der Vorhaben zuzuweisen.

4. Vorhabensdesign: Im Rahmen der zugewiesenen Verantwortung entwickeln die Vorhabensverantwortlichen ein erstes Konzept, das die Vorgaben (Problembeschreibung, Zieldefinition) präzisiert, notwendige Elemente der Umsetzung und der Auswirkung innerhalb und außerhalb des Vorhabens beschreibt. Dieses Dokument ist nach Qualitätssicherung durch die zuständige vorgesetzte Instanz freizugeben und gilt als Basis für die nächsten Vorhabensschritte. In diesem Bearbeitungsschritt werden auch die Ziel- und Wirkungsbeschreibung erweitert und mit den Interessensträgern abgestimmt. Kriterien für die Evaluation werden überprüft, erweitert und mit den Interessensträgern abgestimmt.
Ergebnis sollte ein abgestimmtes fachliches Konzept je Vorhaben sein, sowie eine erweiterte Ziel- und Wirkungsbeschreibung je Vorhaben.

5. Bürger_innenbeteiligung: Möglichst frühzeitig, jedenfalls unmittelbar nach Vorliegen eines ersten Konzepts zur Vorhabensumsetzung, sind alle beteiligten oder möglicherweise betroffenen Interessensträger_innen (Stakeholder) zu identifizieren und zur Abstimmung der weiteren Umsetzungsschritte beizuziehen.
Ergebnis sollte die Einigung – inklusive nicht ausgeräumter Bedenken – mit den Interessensträger_innen sein. Dieses Dokument ist nach Qualitätssicherung durch die zuständige vorgesetzte Instanz freizugeben und gilt als Basis für die nächsten Vorhabensschritte.

➲ *11.1.1 Begutachtungsverfahren*

6. Vorhabensumsetzung und -einführung: Aus dem Vorhabensdesign und dem Ergebnis der Einigungen mit den Interessensträger_innen werden das Vorhaben und die notwendigen Elemente weiterentwickelt und umgesetzt. Hierzu gehören die notwendigen Schritte im parlamentarischen Verfahren: Begutachtung, parlamentarische Diskussion, Nachbesserung, Abstimmung. Ergebnis sollte ein gültiger Rechtsakt zur Umsetzung des Vorhabens (Gesetzesbeschluss; Verordnung; Kundmachung; Dienstanweisung …) sein.

7. Regelbetrieb: Mit Rechtswerdung geht die Verantwortung für den laufenden Betrieb in die Verantwortung der zuständigen Behörde über. Diese Behörde hat regelmäßig über die aus der Umsetzung des Vorhabens gewonnenen Erfahrungen zu berichten (sinnvollerweise auch an jene Instanz, die im Rahmen des Gesamtportfolios für diesen Themenbereich die Verantwortung trägt), die Informationen für eine Evaluation aufzubereiten und eine Evaluation zu veranlassen. Ergebnis sollte die regelmäßige Berichterstattung/Reporting sein, sowie ein Soll/Ist-Vergleich über Ziel- und Wirkungsbeschreibung je Vorhaben: Informationen entsprechend der Ziel- und Wirkungsbeschreibung und den Vorgaben zur Evaluation sind aufzubereiten und zu veröffentlichen.

8. Zyklische Evaluation des Vorhabens: Im Rahmen der zyklischen Evaluation wird festgestellt, ob und in welchem Umfang die Ziele eines Vorhabens erreicht wurden. Bei einer unabhängigen Evaluation ist auch zu prüfen, ob es zu Auswirkungen außerhalb des eigentlichen Zielbereichs des Vorhabens gekommen ist. Die Gesamtwirkung ist einzuschätzen und zu bewerten. Das Ergebnis der Evaluation und die zusammenfassende Bewertung sind zu veröffentlichen. Ergebnis sollte ein Plan/Ist Vergleich über wesentliche Erfolge des Vorhabens sein: Abweichungen von den erwarteten/geplanten Ergebnissen sind zu erklären.

9. Identifikation von Verbesserungspotential und Anpassungen: Spätestens nach der Evaluation sind der Grad der Zielerreichung und die Qualität der Auswirkungen eines umgesetzten Vorhabens zu bewerten. In diese Bewertung haben auch ggf. positive und negative Auswirkungen des Vorhabens außerhalb des ursprünglichen Zielbereichs einzufließen. Aus dieser Beurteilung sind mögliche Verbesserungsvorschläge, sinnvolle Änderungen oder der Bedarf an zusätzlichen Vorhaben abzuleiten und in das Portfolio einzumelden.

Endnoten

1 Siehe z.B. *Bannick*, Zieldefinition – ein Kern-Teilprojekt im Projektmanagement (oder auch: ohne Ziel kein Start und kein Ende), http://on-operations.com/2011/02/21/zieldefinition-%E2%80%93-ein-kern-teilprojekt-im-projektmanagement-oder-auch-ohne-ziel-kein-start-und-kein-ende/ (26.02.2020).

13 Checkliste zur Evaluierung von Maßnahmen

Diese Checkliste folgt aus den vorhergehenden Kapiteln und kann verwendet werden, um neue Gesetzesvorhaben oder auch bestehende Befugnisse zu prüfen. Die Fragen betreffen hier vor allem Gesetzgebungsverfahren, können so oder ähnlich aber auch für einfache Maßnahmen ohne Gesetzesänderung angewendet werden. Manche Fragen wiederholen sich, weil sie im Kontext verschiedener Rechtsgebiete relevant sind. So wird z.B. sowohl in Bezug auf die Grundrechtsmäßigkeit als auch im Datenschutzrecht nach dem Zweck der Maßnahme gefragt. Manche Fragen können für bestimmte Gesetzesvorhaben leicht beantwortbar sein und die Antworten quasi auf der Hand liegen, bei anderen werden sie jedoch große Probleme bereiten. Die Grundrechtsprüfung wird hier nicht im Detail abgebildet, allgemeine Fragen können in diesem Bereich aber auch eine Richtung vorgeben.

1. Vorhaben

- Was ist der Zweck des Vorhabens?
- Welcher gesellschaftliche Wert wird dadurch befördert?
- Welches Ziel wird mit dem Vorhaben verfolgt?
- Welches Problem wird dadurch gelöst?
- Welche Maßnahmen sind in dem Vorhaben vorgesehen?
- Ist das Vorhaben geeignet, den Zweck zu erreichen?

2. Kompetenz

- Ist das Gesetzesvorhaben Bundes- oder Landeskompetenz?
- Welches Ministerium ist mit den betreffenden Aufgaben betraut?
- Welche Abteilung des Ministeriums ist damit betraut?

3. Wirksamkeit

- Woran ist die Wirksamkeit des Vorhabens zu erkennen?
- Was wird erreicht, wenn das Vorhaben erfolgreich ist?
- Wie wird die Wirksamkeit des Vorhabens gemessen?

- Welche Daten sind dafür verfügbar?
- Welche Daten sind dafür zu erheben?
- Welche Daten sind dafür regelmäßig zu veröffentlichen?

4. Datenschutz

- Werden bei dem Vorhaben personenbezogene Daten verarbeitet?
- Gibt es eine klare gesetzliche Grundlage für die Datenverarbeitung?
- Werden die Datenschutz-Grundsätze beachtet?
  - Erfolgt die Verarbeitung rechtmäßig und nach Treu und Glauben?
  - Werden die Daten für denselben Zweck verwendet, für den sie erhoben wurden?
  - Werden nur die Daten erhoben, die für die Erfüllung des Zwecks notwendig sind?
  - Sind die erhobenen Daten sachlich richtig? Gibt es die Möglichkeit, sie zu berichtigen und zu löschen, falls sie falsch sind?
  - Werden die Daten nicht länger gespeichert als für den Zweck, zu dem sie erhoben wurden, notwendig?
  - Werden die Daten vor unbefugten Zugriffen geschützt?
  - Wird zwischen faktenbasierten und persönlichen Einschätzungen unterschieden?
- Welche Arten von Daten werden beim Einsatz der Maßnahme verarbeitet (z.B. Stammdaten, Verkehrsdaten, Zugriffsdaten...)
- Sind die Voraussetzungen für die Datenverarbeitung klar definiert?
- Werden besonders sensible Kategorien von Daten verarbeitet?
  - Werden die besonderen Voraussetzungen für die Verarbeitung eingehalten?
- Werden automatisierte Entscheidungen getroffen?
- Bei einem Datenabgleich: Mit welcher Datenbank werden die Daten abgeglichen? Informationen welcher Personen sind in dieser Datenbank?
- Werden die Betroffenen über die Datenverarbeitung informiert?
  - Ist die Information einfach verständlich?
  - Erfolgt die Information automatisch?
  - Sind die Informationen vollständig gem. § 36 Abs. 2 Z 1 DSG?
  - Falls nein, sind die Voraussetzungen von Art. 13 Abs. 3 Polizei-RL für das Entfallen der Information erfüllt?

- Sind die Rechte der Betroffenen gewährleistet und durchsetzbar?
  - Das Recht auf Auskunft
  - Das Recht auf Berichtigung oder Löschung und auf Einschränkung
- Wer ist Verantwortliche_r für die Datenverarbeitung?
  Gibt es eine_n Auftragsverarbeiter_in?

Im Falle unrechtmäßiger Datenverarbeitung

- Besteht ein Beschwerderecht an die Datenschutzbehörde?
- Besteht ein gerichtlicher Rechtsbehelf?
- Besteht eine Möglichkeit Schadenersatz zu verlangen?

Bei Verwendung von Daten aus anderen Quellen

- Ist die Datenverarbeitung gesetzlich zulässig?
- Zu welchem Zweck wurden die Daten ursprünglich erhoben und gespeichert?
  - Entspricht die neue Verwendung diesem Zweck?
- Werden Daten aus öffentlichen Registern verwendet?
  - Gibt es dafür eine eigene gesetzliche Grundlage?
- Werden Daten aus privaten Quellen verwendet?
  - Gibt es für die Übermittlung eine gesetzliche Grundlage?

Bei einer Datenübermittlung

- Wurde geprüft, ob auch ein Datenzugriff ohne Übermittlung möglich und weniger eingriffsintensiv wäre?
- Ist der Datenzugriff/die Datenübermittlung gesetzlich gedeckt?
- Wird der Datenzugriff/die Datenübermittlung nachvollziehbar dokumentiert?

Besonders geschützte Berufsgruppen (Berufsgeheimnisträger_innen wie Ärzte_innen, Priester_innen, Rechtsanwält_innen, Journalist_innen, ...)

- Gibt es angemessene Prozesse, um sicherzustellen, ob dies der Fall ist?
- Wer ist dafür verantwortlich, diese Prozesse einzuhalten?
- Sollen Daten der geschützten Berufsgruppen erhoben werden und wie wird dabei vorgegangen?
- Wie wird der Schutz der geschützten Berufsgruppen gewährleistet?
- Gibt es Sanktionen, falls der Schutz nicht gewährleistet werden konnte?

Bei Datenübermittlungen in Nicht-EU-Länder

- Ist die Übermittlung rechtlich zulässig?
- Besteht mit diesem Land ein Angemessenheitsbeschluss?
- Ist die Übermittlung für polizeiliche Zwecke erforderlich?
- Erfolgt die Übermittlung an eine andere Polizeibehörde?
- Wenn die Daten aus einem anderen Land stammen, hat dieses zugestimmt?

Speicherfristen

- Sind die Speicherfristen klar definiert?
- Wer ist nach Ablauf der Frist für die Löschung der Daten verantwortlich?
- Gibt es automatische Prozesse, die die Löschung der Daten gewährleisten?
- Welche Sanktionen gibt es, wenn die Daten nicht vor Ablauf der Frist gelöscht wurden?

Datenzugriff und Protokollierung

- Sind die Zugriffsberechtigten präzise und vollständig bezeichnet?
- Ist die Anzahl der Zugriffsberechtigten klar absehbar?
- Gibt es eine klare, nachvollziehbare und sanktionierbare Dokumentation von Datenzugriffen, die auch Änderungen umfassen?
- Gibt es auch für die personenbezogenen Daten in diesen Protokollen klare Speicherfristen?

Sicherheit der Verarbeitung

- Sind die Daten ausreichend geschützt vor:
  - unbefugtem Zugriff von innerhalb und außerhalb der Organisation?
  - unbefugter Weitergabe?
  - unbefugter Veränderung?
- Gibt es automatisch Prozesse sowie technische und organisatorische Maßnahmen, die gewährleisten, dass unbefugte Zugriffe, Weitergaben oder Veränderungen auffallen?

Datenschutz durch Technikgestaltung und datenschutzrechtliche Voreinstellungen

- Wurde durch die Technikgestaltung und die Voreinstellungen sichergestellt, dass die datenschutzrechtlichen Vorgaben eingehalten werden?

Organisatorische Maßnahmen

- Gibt es ein Verarbeitungsverzeichnis? Scheint die Maßnahme darin auf?
- Werden alle Vorgänge in den Datenbanken protokolliert? (inkl. Erhebungen, Veränderungen, Abfragen, Offenlegungen, inkl. Begründung, Datum und Uhrzeit und Identität der Person, die dies vorgenommen hat)?
- Gibt es eine_n zuständige_n Datenschutzbeauftragte_n?
- Gibt es Verhaltensregeln für die Personen mit Zugriff auf die Daten?
- Gibt es Verschwiegenheitserklärungen?
- Gibt es Schulungen zu Datenschutz und Sicherheit?

Prozesse für den Fall von Datenschutzverletzungen

- Wird gewährleistet, dass von Datenschutzverletzungen betroffene Personen darüber informiert werden?
- Wer ist für diese Information zuständig?
- Wie erfolgt diese Information?

Datenschutzfolgenabschätzung

- Ist eine Datenschutzfolgenabschätzung erforderlich?
- Liegt ein für die Betroffenen hohes Risiko vor?
- Wurde die Datenschutzfolgenabschätzung ordnungsgemäß durchgeführt?

Erweiterung der Wirkungsfolgeabschätzung (WFA)

Werden die Auswirkungen auf die folgenden Wirkungsdimensionen beachtet?

- Gesamtwirtschaft
- Unternehmen
- Umwelt
- Konsument_innenschutzpolitik
- Verwaltungskosten für Bürger_innen und für Unternehmen
- Soziales
- Kinder und Jugend
- Tatsächliche Gleichstellung von Frauen und Männern

5. Betroffene

- Sind die betroffenen Personen klar, eindeutig und nachvollziehbar definiert?
  - Bestehen klare Vorgaben, wer Betroffene_r sein kann?
  - Wird nach Kategorien von Betroffenen unterschieden (z.B. Verdächtige_r, Kontaktperson, etc.)?
  - Wie viele Menschen sind von der Maßnahme betroffen?
- Ist eine vor Diskriminierung geschützte Gruppe von der Maßnahme stärker betroffen als andere Gruppen?
  - Hat das Vorhaben negative Auswirkungen auf diese Gruppe?

6. Öffentliche Konsultation

- Wer wird im Gesetzgebungsverfahren konsultiert?
  - Die Zivilgesellschaft?
  - Interessenvertretungen?
  - Der Datenschutzrat?
  - Die Datenschutzbehörde?
  - Der Verfassungsdienst?
- Gibt es eine parlamentarische Begutachtung? Wenn ja, ist diese mindestens sechs Wochen lang?

7. Grundrechtsschutz und individuelle Rechte

- Ist der Anwendungsbereich der GRC, der EMRK oder anderer Grundrechte gegeben?
  - Recht auf Achtung des Privat- und Familienlebens (Art. 8 EMRK, Art. 7 GRC)
  - Schutz personenbezogener Daten (§ 1 DSG, Art. 8. GRC)
  - Schutz des Briefgeheimnisses (Art. 10 StGG, Art. 8 EMRK)
  - Schutz des Fernmeldegeheimnisses (Art. 10a StGG, Art. 8 EMRK)
  - Unverletzlichkeit des Hausrechtes (Art. 9 StGG, Gesetz zum Schutze des Hausrechts)
  - Freiheit der Meinungsäußerung (Art. 10 EMRK, Art. 13 StGG, Art. 11 GRC)
  - Versammlungsfreiheit (Art. 11 EMRK, Art. 12 StGG, Art. 12 GRC)
  - Recht auf ein faires Verfahren (Art. 6 EMRK)

- Nichtdiskriminierung (Art. 21 - 23 GRC)

- Wir konnten im Rahmen dieses Handbuchs nicht alle bestehenden Betroffenenrechte näher ausführen. Es gibt noch andere Bereiche, zusätzlich zu den obenstehenden, die von Überwachungsmaßnahmen auch am Rande berührt werden könnten, und deren Prüfung zielführend sein kann:

  - Gedanken-, Gewissens- und Religionsfreiheit (Art. 14 StGG, Art. 16 StGG, Art. 9 EMRK, Art. 10 GRC)

  - Gleichheit (Art. 2 StGG, Art 7 B-VG, Art. 20 GRC)

  - Recht auf Freiheit und Sicherheit (Art. 5 GRC)

  - Recht auf eine gute Verwaltung (Art. 41 GRC)

  - Recht auf Zugang zu Dokumenten (Art. 42 GRC)

  - Arbeitnehmer_innenschutz, Umweltschutz, Verbraucher_innenschutz (Art. 27-38 GRC)

  - Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht (Art. 47 GRC)

  - Unschuldsvermutung und Verteidigungsrechte (Art. 48 GRC)

  - Grundsätze der Gesetzmäßigkeit und der Verhältnismäßigkeit im Zusammenhang mit Straftaten und Strafen (Art. 49 GRC)

  - Rechte der Minderheiten (Art. 62ff Staatsvertrag von Saint-Germain-en-Laye)

  - Erwerbs- und unternehmerische Freiheit (Art. 18 GRC)

  - Eigentumsrecht (Art. 17 GRC)

- Werden personenbezogene Daten verarbeitet?

- Sind durch die Maßnahme Rückschlüsse auf die Persönlichkeit und das Privatleben der betroffenen Personen möglich?

- Ist der höchstpersönliche Lebensbereich der Personen berührt?

- Erfolgt die Maßnahme im Geheimen?

  - Wenn ja, wurde die Art der Straftaten festgelegt, die die Überwachung rechtfertigen können?

  - Sind die betroffenen Personengruppen festgelegt worden?

  - Ist die Dauer der Maßnahme begrenzt?

  - Ist das Verfahren für die Auswertung, Verwendung und Speicherung der Daten festgelegt?

  - Gelten für sensible Daten erhöhte Anforderungen an verfahrensrechtliche Sicherungsmaßnahmen?

  - Wurden Vorsichtsmaßnahmen für die Übermittlung der Daten an Dritte festgelegt?

  - Wurden die Umstände festgelegt, unter denen die Daten gelöscht werden müssen?

- Werden Berufsgeheimnisse gewahrt?

- Wird die Kommunikation mit Anwält_innen überwacht?

- Ist der Grundrechtseingriff gerechtfertigt (Verhältnismäßigkeitsprüfung)?

  - Ist der Eingriff gesetzlich vorgesehen?

    - Ist dieses Gesetz mit der Rechtsstaatlichkeit vereinbar?

    - Ist dieses Gesetz zugänglich?

    - Ist dieses Gesetz bestimmt und vorhersehbar?

      - Sind Art, Umfang und Dauer der Maßnahme klar bestimmt?

      - Sind die Gründe, aus denen die Maßnahme angeordnet werden kann, klar definiert?

      - Ist eindeutig, welche Behörden für die Genehmigung, Durchführung und Überwachung solcher Maßnahmen zuständig sind?

      - Ist die Art des Rechtsbehelfs eindeutig bestimmt?

  - Ist das Gesetz in einer demokratischen Gesellschaft notwendig? Gibt es ein dringendes soziales Bedürfnis, das durch die Maßnahme erfüllt wird?

  - Steht der Eingriff im Verhältnis zu den Zielen der Maßnahme, ist er adäquat?

8. Verfahrensgarantien

- Bei wem liegt die Verantwortung

  - für das Einleiten und Beantragen der Maßnahme?

  - für die Bewilligung der Maßnahme?

    - Ist ein Richter_innenvorbehalt gegeben?

    - Wenn nein, warum nicht? Wer tritt für Betroffene rechtewahrend (kommissarisch) ein? Wie können Fehlentscheidungen erkannt und bekämpft werden?

    - Muss die Zustimmung explizit begründet werden?

    - Ist die Ablehnung einfach möglich?

    - Ist die Ablehnung schwieriger als eine Zustimmung?

  - für die Durchführung der Maßnahme?

- für begleitende Kontrolle?
- für Nachkontrolle und Evaluierung der Maßnahme?
- für den Rechtsschutz von durch die Maßnahme Betroffene?

9. Technologie

- Wie präzise ist die angewandte Technologie beschrieben?
- Entsprechen die technischen Möglichkeiten der angewandten Technologie den gesetzlichen Einschränkungen?
  - Wenn nein, wie wird sichergestellt, dass sie gesetzlichen Einschränkungen eingehalten werden?
  - Werden funktionelle, organisatorische oder technische Einschränkungen gesetzt, um die gesetzwidrige Anwendung unmöglich zu machen?

10. Risikoanalyse

- Welche Risikoszenarien bestehen in Bezug auf die Datenverarbeitung?
- Wie hoch ist das Risiko?
- Wie wahrscheinlich ist es, dass sich das Risiko verwirklicht?
- Werden Maßnahmen getroffen, um den Risiken zu begegnen und sie zu verringern?

11. Gesamtrechnung

- Welche Überwachungsmaßnahmen betreffen besonders viele Menschen?
- Wie viele Personen sind zu jedem Zeitpunkt von wie vielen Überwachungsmaßnahmen betroffen?
- Wie sind die Ergebnisse aus diesen Maßnahmen verknüpfbar?
- Welche Datenbanken sind miteinander verknüpft?
- Wie hoch ist die Eingriffsintensität bei Verknüpfung verschiedener Überwachungsmaßnahmen?

12. Berichte und Evaluierung

- Wird regelmäßig berichtet über
  - den Einsatz der Maßnahme?
  - Effizienz bzw. den Erfolg der Maßnahme?
  - die Kosten der Maßnahme?

- Werden die Maßnahme und ihr Einsatz regelmäßig evaluiert und verbessert?

13. Fragestellungen für jeden Punkt

- Von wem wird dies gewährleistet?
- In wessen persönlicher Verantwortung liegt dies?
- Wird die Nichterfüllung wird sanktioniert durch
  - gerichtliches Strafrecht? Mit welchem Strafrahmen?
  - Verwaltungsstrafrecht? Mit welchem Strafrahmen?
  - Disziplinarrecht?
  - zivilrechtliche Haftung?

ANHANG

Leseempfehlungen

Monografien

Eubanks, Algorithms of Inequality. How High-Tech Tools Profile, Police and Punish the Poor (2017).
Eine detaillierte Darstellung mehrerer Einsätze von Algorithmen im US-amerikanischen Sozialsystem, an denen sich zeigt, wie dadurch soziale Ungerechtigkeit verhärtet wird.

European Union Agency for Fundamental Rights, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume I: Member States' legal frameworks (2015).
Ein Bericht der europäischen Grundrechteagentur über Geheimdienste und deren Kontrolle und Aufsicht im EU Vergleich.
(online frei verfügbar)

Ewans/Lewis, Undercover. The true story of Britain's secret police (2013).
Die mitreißende und skandalöse Geschichte von britischen verdeckten Ermittlern und deren unlauteren Methoden, erzählt von ihren Aufdeckern.

Ferguson, The Rise of Big Data Policing. Surveillance, Race and the Future of Law Enforcement (2017).
Eine Darstellung der Geschichte des Einsatzes von Big Data durch die Polizei in den USA und einer Reihe von Problemen, die sich dadurch ergeben.

Gesellschaft für Menschenrechte von Marginalisierten und MigrantInnen, 1000 Jahre Haft Operation Spring und institutioneller Rassismus (2005).
Ein Bericht u.a. über strukturellen Rassismus in der österreichischen Justiz anhand der Ermittlungen gegen die afrikanische Community Ende der 90er in Österreich.

Heißl, Überwachungen und Ermittlungen im Internet. Sicherheitspolizei, Militärische Nachrichtendienste, Kriminalpolizei (2017).
Ein hilfreicher juristischer Überblick über die Rechtslage von Überwachung im digitalen Raum in Österreich.

Landau, Listening In. Cybersecurity in an Insecure Age (2017).
Eine spannende Erklärung, wieso Überwachungstechnologien wie Bundestrojaner oder andere staatliche Eingriffe in Verschlüsselungssysteme die Cybersicherheit Aller gefährden können, mit Beispielen aus den USA.

O'Neil, Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy (2016).
Ein kurzweiliges Plädoyer dafür, nicht zuzulassen, dass Algorithmen und Big Data gesellschaftliche Ungleichheiten verfestigen, anhand verschiedener Beispiele aus den USA.

Schneier, Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World (2016).
Eine komplette Übersicht über und einer guter Einstieg in die politischen Debatten über Überwachung, Privatsphäre und Regulierung von privaten und staatlichen Akteuren, aus einer US-Perspektive.

Snowden, Permanent Record (2019).
Ein persönlicher Bericht von Edward Snowden über seine Arbeit im US-amerikanischen Geheimdienst NSA und seine Beweggründe, für die Freiheit der Menschen Alles aufs Spiel zu setzen.

Singelnstein/Stolle, Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert (2006).
Ein Werk, in dem die Ausweitung der Überwachung im größeren Rahmen gesellschaftlicher Veränderungen gezeigt wird.

Wetzling/Vieth, Upping the Ante on Bulk Surveillance. An International Compendium of Good Legal Safeguards and Oversight Innovations (2018).
Ein Überblick über Befugnisse zur Massenüberwachung von Kommunikation in Europa und die gesetzlichen Einschränkungen der verschiedenen Länder.
(online frei verfügbar)

Zerbes, Spitzeln, Spähen Spionieren. Sprengung strafprozessualer Grenzen durch geheime Zugriffe auf Kommunikation (2010).
Eine juristische Analyse der rechtlichen Zulässigkeit von geheimer Telekommunikationsüberwachung in Österreich.

Sammelbände

Ball/Haggerty/Lyon (Hrsg.), Routledge Handbook of Surveillance Studies (2012).
Ein Sammelband mit Beiträgen zu den verschiedensten Aspekten von Überwachung; von gesellschaftlicher Segregation, Gender, über Kolonialismus bis hin zur Überwachungsindustrie.

Kreissl/Wright (Hrsg.) Surveillance in Europe (2015).
Eine interdisziplinäre Sammlung von Aufsätzen über Überwachung in Europa, mit Fokus auf Sozialwissenschaften und Grundrechte.

Mackinger/Pack (Hrsg.) § 278a: Gemeint sind wir alle! (2011).
Die Geschichte der Überwachung und Repression der Tierrechtsbewegung in Österreich, einer der großen Justizskandale der letzten Jahrzehnte.

Monahan/Murakami Wood (Hrsg.) Surveillance Studies. A Reader (2018).
Eine Auswahl der wichtigsten sozialwissenschaftlichen Texte über Überwachung aus verschiedenen Themenbereichen von Staat und Autorität, über Identität, Sicherheit und Polizei, bis zu Arbeit, gesellschaftlichen Ausgrenzungen, Kunst und Kultur.

Singelnstein/Puschke (Hrsg.), Der Staat und die Sicherheitsgesellschaft (2018).
Ein Band mit Aufsätzen über staatliche Überwachung und die politischen Entwicklungen, die zu ihrer Ausweitung führen, mit besonderem Blick auf Deutschland.

Steinhauser (Hrsg.), Nie mehr allein... Überwachungsbericht 2017.
Ein von der Partei „Die Grünen" herausgegebener Bericht über die Häufigkeit und Schwerpunkte von Überwachung in Österreich sowie über aktuelle Debatten.

Zeitschriften & Blogs

CILIP - Bürgerrechte & Polizei. Eine deutsche Zeitschrift, die regelmäßig kritisch über polizeiliche Überwachung berichtet. Viele Artikel sind online frei verfügbar.

juridikum – zeitschrift für kritik | recht | gesellschaft. Eine österreichische Rechtszeitschrift mit interdisziplinärem Einschlag, die vierteljährlich erscheint und regelmäßig über Themen der Überwachung, Repression, Meinungs- und Versammlungsfreiheit publiziert. Ausgaben, die älter als zwei Jahre sind, sind online frei zugänglich.

Netzpolitik.org. Ein redaktioneller Blog, der gehaltvoll über netzpolitische Themen - oft auch über Überwachung - berichtet, mit besonderem Fokus auf Deutschland.

Glossar

Access-Provider
[7.4.2, Telekommunikationsüberwachung] Vermitteln Zugang zu einem Kommunikationsnetz wie dem Internet oder übermitteln Information an ein solches.
Ein Access-Provider kann gleichzeitig auch durch andere Tätigkeiten Host-Provider sein.

Anlassdatenspeicherung
[2.11, Überwachungsbefugnisse im Zeitraffer; Sicherheitspaket] [3.2, Überwachungstechnologien; Speicherverpflichtungen] [7.5, Telekommunikationsüberwachung; Anlassdatenspeicherung]
Eine Speicherung von Daten, deren Wirkungsbereich örtlich, zeitlich und/oder auf einen spezifischen Personenkreis und auf einen bestimmten Anlass (z.B. eine Straftat) beschränkt ist.

Big Data
[3(3.4), Überwachungstechnologien; Diskriminierung durch Algorithmen] [8.4, Umstrittene Befugnisse; Rasterfahndung] Große Datenmengen, die mitunter so schnelllebig und komplex sind, dass eine manuelle Auswertung gar nicht mehr möglich scheint. Oft sind damit auch komplexe Algorithmen zur Analyse dieser großen Datenmengen mitgemeint.

Body Worn Cameras
[2.9, Überwachungsbefugnisse im Zeitraffer; Polizeiliches Staatsschutzgesetz] [4.3, Überwachung im Überblick] [6.1.1., Videoüberwachung] [9.4.1, Grundrechte; EMRK siehe Eingriff]
Auch: Bodycams, Körperkameras. Kameras, die klein sind, am Körper (meist im Brustbereich) getragen werden, und oft in hoher Qualität lange aufzeichnen können.

Bundestrojaner
[2.11, Überwachungsbefugnisse im Zeitraffer, Sicherheitspaket] [4.3, Überwachung im Überblick] [7.3.1, Telekommunikationsüberwachung] [8.1, Umstrittene Befugnisse; Bundestrojaner] [11.2.1, Gesetzesevaluierung]
Eine Überwachungssoftware, die ohne Wissen der überwachten Person auf ihren Geräten installiert wird und auf diesen sämtliche Zugriffsrechte hat. Meist geschieht die Installation unter Ausnutzung spezifischer Sicherheitslücken.

Drittland
[9.2.4, Grundrechte; Recht auf Schutz personenbezogener Daten (Art. 7 und Art 8. GRC)] Auch Drittstaat.
Ein Staat, der nicht Vertragspartner eines völkerrechtlichen Vertrages ist. Im Fall der EU also jeder Staat, der nicht Mitglied der Union ist.

Ende-zu-Ende-Verschlüsselung
[8.1, Umstrittene Befugnisse; Bundestrojaner] Die Verschlüsselung der zu übertragenden Daten von Endpunkt zu Endpunkt (z.B. von Handy zu Handy) ohne, dass die Dateien dazwischen entschlüsselt werden können.

Europäische Menschenrechtskonvention (EMRK)
[4.4, Überwachung im Überblick; Berufsgeheimnis] [8.3; 8.4, Umstrittene Befugnisse; Kfz-Überwachung; Beschlagnahmung von Briefen] [9, Grundrechte] [11.2.4, Gesetzesevaluierung; Datenschutzrecht für Polizei und Justiz] [13, Checkliste; Grundrechtsschutz]
Die EMRK ist ein Grundrechtskatalog. Sie ist ein völkerrechtlicher Vertrag zwischen 47 Staaten, die alle Mitglieder des Europarates sind, so auch Österreich. Sie verpflichtet den Staat, bestimmte Rechte der Einzelnen zu wahren, und ist Teil der österreichischen Bundesverfassung.

Europäischer Gerichtshof (EuGH)
[7.5, Telekommunikationsüberwachung; Anlassdatenspeicherung] [9, Grundrechte]
Der europäische Gerichtshof ist das oberste rechtsprechende Organ der EU. Er ist vor allem dafür zuständig, dass das Recht der Europäischen Union einheitlich angewendet wird. Im Vorabentscheidungsverfahren bspw. müssen nationale Gerichte bei Unklarheiten bei der Anwendung von Unionsrecht den EuGH anrufen und nachfragen.

Europäischer Gerichtshof für Menschenrechte (EGMR)
[9, Grundrechte]
Der EGMR überprüft, ob jene Staaten, die die EMRK (siehe Europ. Menschenrechtskonvention) unterzeichnet haben, diese in ihrer Gesetzgebung, Rechtsprechung und Verwaltung einhalten. Dabei kann er etwa als Höchstgericht von einem Einzelnen angerufen werden, aber auch Staaten können sich über andere Vertragsstaaten beschweren.

Exploits
[2.11, Überwachungsbefugnisse im Zeitraffer; Sicherheitspaket]
Eine Software, die eine Sicherheitslücke ausnutzt, welche auf Computern und Handys aufgrund von Programmierfehlern oder Designfehlern existiert, um in die Geräte einzudringen.

Fluggastdatenverarbeitung, PNR
[3(3.4), Überwachungstechnologien; Diskriminierung durch Algorithmen] [4.1, Überwachung im Überblick; Rechtsgrundlagen] [8.2, Umstrittene Befugnisse] [9.2.4, Grundrechte; Recht auf Schutz personenbezogener Daten.]
PNR steht für Passenger Name Record, auf Deutsch Fluggastdaten. Dabei handelt es sich um Datensätze zu einer Person, die einen Flug unternimmt. Nach der EU-PNR-Richtlinie von 2016 müssen die Daten von allen Menschen, die aus oder in die EU fliegen von den Fluglinien an Sicherheitsbehörden der EU-Mitgliedstaaten weitergeleitet werden.

Gesetzesvorbehalt
[9.2.1–9.4.1, Grundrechte]
Bedeutet die gesetzliche Möglichkeit, unter gewissen Voraussetzungen Grundrechte einzuschränken. Ein solcher Gesetzesvorbehalt kann dem Gesetzgeber unterschiedliche Spielräume einräumen – je nachdem, ob es sich um einen formellen oder materiellen Gesetzesvorbehalt handelt.

Gesetzesvorbehalt, formeller
[9.2.1–9.4.1, Grundrechte] Bedeutet: Gewisse Grundrechte können eingeschränkt werden, sofern dies in Gesetzesform geschieht. Es bestehen keine inhaltlichen Voraussetzungen.

Gesetzesvorbehalt, materieller
[9.2.1–9.4.1, Grundrechte] Bedeutet: Gewisse Grundrechte können nur unter bestimmten inhaltlichen Voraussetzungen eingeschränkt werden, bspw. wenn dies zur Aufrechterhaltung der nationalen Sicherheit notwendig ist.

Grauer Markt
[8.1, Umstrittene Befugnisse; Bundestrojaner] Verbindet legale und illegale Marktsegmente miteinander. Die Grenzen zwischen grauen Markt und Schwarzmarkt sind fließend und daher schwer voneinander abzugrenzen. Beim Beispiel Bundestrojaner ist mit Grauer Markt ein Verkauf von Sicherheitslücken gemeint, deren Einsatz durch staatliche Strafverfolgungsbehörden legitim scheint, der jedoch einerseits ebenso Hacker_innengruppen bedient oder finanziert, andererseits auch durch undemokratische Staaten zur Verfolgung von Regimegegner_innen oder zur Wirtschaftsspionage verwendet wird.

Grundrechtecharta (GRC)
[9, Grundrechte] [11.2.4, Gesetzesevaluierung; Datenschutzrecht für Polizei und Justiz] Die Charta der Grundrechte der Europäischen Union ist ein Grundrechtskatalog, der für alle Staaten der EU, außer Polen und Großbritannien, gilt in Österreich sogar als österreichisches Gesetz. Der Vertrag über die Europäische Union (EUV) verweist auf die Grundrechtecharta, womit ihr Rechtsverbindlichkeit zukommt.

Host-Provider
[7.4.2; 7.6, Telekommunikationsüberwachung] Stellen online Speicherplatz zur Verfügung. Beispiele sind Cloud-Computing-Services oder E-Mail- und SMS-Dienste mit

einer Speichermöglichkeit. Bei sozialen Medien wie Facebook werden unter Umständen auch Seitenbetreiber_innen und Inhaber_innen von privaten Profilen als Host-Provider angesehen.

IMSI-Catcher
[2.11, Überwachungsbefugnisse im Zeitraffer; Sicherheitspaket] [4.3, Überwachung im Überblick; Kontrolle und Aufsicht] [7.4.1; 7.4.3; 7.4.4, Telekommunikationsüberwachung; Auskünfte; 7.7, IMSI-Catcher]
Ein Überwachungsgerät, welches sich im Mobilfunk zwischen Sender (Handymast) und Empfänger (Handy) schaltet, um den Standort eines Gerätes festzustellen oder Kommunikation abzufangen.

Inhaltsdaten
[7.1–7.4; 7.7, Telekommunikationsüberwachung] Bezeichnen den tatsächlichen Inhalt von Nachrichten, also jeder Information, die über einen öffentlichen Kommunikationsdienst an eine beschränkte Zahl an Empfänger_innen weitergegeben wird.

Internet of Things
[3.2, Überwachungstechnologien; Speicherverpflichtungen] [8.1, Umstrittene Befugnisse; Bundestrojaner]
Ein eher unscharfer Sammelbegriff für Geräte mit Funkverbindungen. Da dies immer günstiger, kleiner und stromsparender möglich ist, gibt es immer mehr Geräte, die in einem lokalen Netzwerk oder im Internet verfügbar sind und miteinander, mit Apps oder über spezifische Services kommunizieren.

Keylogger
[8.1, Umstrittene Befugnisse; Bundestrojaner]
Ein Programm oder ein Bausatz, der es ermöglicht sämtliche Tastatur-, Maus- und/oder Bildschirmeingaben eines Gerätes zu erfassen und zu speichern.

Kommunikationsdienste
[7.1; 7.2; 7.4.2,Telekommunikationsüberwachung]
Sind gewerbliche Dienstleistungen, die in der Übertragung von Signalen in Kommunikationsnetzen bestehen, ausgenommen Dienste, die Inhalte über Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben, also z.B. A1 oder UPC, nicht aber Betreiber_innen einer Website.

Konfident_innen
[2, Überwachungsbefugnisse im Zeitraffer] [4.3, Überwachung im Überblick; Kontrolle und Aufsicht] [5, Verdeckte Ermittlung]
Auch **Vertrauensperson**. Eine Person, die im Auftrag der Polizei Informationen oder Daten erhebt, die sie durch Vertrauen in Gesprächen oder durch Kontakt mit Personen erlangt. Es handelt sich dabei um eine private Vertrauensperson, nicht um eine_n verdeckte_n Ermittler_in.

Lauschangriff (Großer, kleiner, Späh- und Lauschangriff)
[2.2, Überwachungsbefugnisse im Zeitraffer]
[6.5.1; 6.5.2, Videoüberwachung] bezeichnet die akustische und/oder optische Überwachung im nichtöffentlichen Raum durch Strafverfolgungsbehörden.

Metadaten
[9.2.2, Grundrechte]
Überbegriff für strukturierte Daten, die Information über die Merkmale anderer Daten enthalten. Also z.B. das Datum, der Ort der Aufnahme von Fotos, die Länge von Telefonverbindungen, oder die IP-Adresse des_der Absender_in eines E-Mails.

Personenbezogene Daten
[4.3; 4.8; 4.9, Überwachung im Überblick; Kontrolle, Aufsicht, polizeiliche Datenbanken] [6.1.2; 6.1.3; 6.3, Videoüberwachung] [7.2; 7.6.2, Telekommunikationsüberwachung] [8.4, Umstrittene Befugnisse; Rasterfahndung] [9.2.4, Grundrechte; Recht auf Schutz personenbezogener Daten] [11.1; 11.3, Gesetzesevaluierung] [13, Checkliste]
Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Z 1 DSGVO) z.B. Name, Adresse, Geburtsdatum, Einkommen und Vermögensverhältnisse, Beruf, Ausbildung oder Gesundheitszustand.

Prävalenzfehler
[3(3.4), Überwachungstechnologien; Diskriminierung durch Algorithmen] [8.2, Umstrittene Befugnisse; Fluggastdaten] Auch: Basisratenfehler, Basisratenmissachtung oder **Base Rate Fallacy**.
Ein Interpretationsfehler in der statistischen Wahrscheinlichkeitsrechnung mit bedingten Abhängigkeiten. Er tritt auf, wenn eine bedingte Abhängigkeit zweier Variablen A+B berechnet wird ohne die A-Priori-Wahrscheinlichkeit (Prävalenz) der Variable A zu berücksichtigen.

Profiling
[3.4, Überwachungstechnologien; Diskriminierung durch Algorithmen] [10.1.2, Datenschutz im Polizeibereich; Automatisierte Entscheidungen] [11.2.5, Gesetzesevaluierung; Datenschutz-Folgenabschätzung]
Das Zusammenführen und Analysieren von Daten für eine zweckbezogene Auswertung anhand bestimmter – oft demographischer – Kategorien, z.B. die Suche nach Täter_innen oder Verdächtigen. (Vgl. auch Art. 3 Z 4 Polizei-DSRL)

Rasterfahndung
[2.2, Überwachungsbefugnisse im Zeitraffer; Lauschangriff] [8.4, Umstrittene Befugnisse]
Eine Art der Fahndung ohne bestimmte Zielperson: Es soll nur die Gruppe der zu überprüfenden Personen eingeschränkt werden. Dazu werden große Mengen an Daten automatisiert verarbeitet, indem Datenbestände miteinander abgeglichen werden.

Rechtsschutzbeauftragte (RSB)
[4.1.2; 4.3, Überwachung im Überblick] [5. Verdeckte Ermittlung] [6.1.1; 6.1.3; 6.2.2; 6.3, Videoüberwachung] [8.1, Umstrittene Befugnisse; Bundestrojaner]
Sind Aufsichtsorgane, die bestimmte Ermittlungsmaßnahmen im Vorhinein genehmigen bzw. im Nachhinein überprüfen müssen und deren Einsatz kontrollieren können. Ihre Befugnisse sind sowohl nach dem SPG, der StPO, als auch dem PStSG und PNR-G geregelt.

Rechtsstaatlichkeit
[9 (spez. 9.2.1 u. 9.5), Grundrechte [11.3, Gesetzesevaluierung; Menschenwürde und Rechtsstaatlichkeit durch Technikgestaltung] [13, Checkliste] Verfassungsprinzip, nach dem jedes staatliche Handeln eine rechtliche Grundlage benötigt: Gesetze dürfen nur auf Grundlage der Verfassung erlassen werden, Gerichte und Verwaltungsbehörden dürfen nur auf Grundlage von Gesetzen und der Verfassung handeln.

Rechtsträger_innen
[4.5, Überwachung im Überblick; Finanztransaktionen/Bankgeheimnis] [6.2.1; 6.2.2, Videoüberwachung; Informationspflicht, Speicherpflicht, Verwendung d. Materials] Rechtsträger_in ist, wer ein Recht innehat, wer also gesetzlich etwas Bestimmtes darf.

Sicherheitspaket
[2.7; 2.11, Überwachungsbefugnisse im Zeitraffer] [6, Videoüberwachung; Speicherverpflichtung] [11.2.1, Gesetzesevaluierung]
Auch: **Überwachungspaket**.
Ein Gesetzespaket zur Verschärfung der Überwachung in Österreich, welches 2018 mit den Stimmen von ÖVP und FPÖ beschlossen wurde.
Sicherheitspolizeigesetz (SPG)
[4 (spez. 4.1), Überwachung im Überblick] [5 Verdeckte Ermittlung] [6.1.1–6.4; Videoüberwachung] [7.1–7.4.; 7.7, Telekommunikationsüberwachung] [9.4.1, Grundrechte; Eingriff in Art. 11 EMRK]
Das Sicherheitspolizeigesetz regelt die Sicherheitsverwaltung und die Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit durch die Sicherheitsbehörden und die Polizei.

Staatsgrundgesetz (StGG)
[8.5, Umstrittene Befugnisse; Beschlagnahme von Briefen] [9.1.2; 9.2.2, Grundrechte]
Das Staatsgrundgesetz über die allgemeinen Rechte der

Staatsbürger ist ein Grundrechtskatalog von 1867. Als solcher ist es Teil der österreichischen Bundesverfassung und verpflichtet den Staat, bestimmte Grundrechte der Einzelnen zu wahren.

Stammdaten
[7.1; 7.2; 7.4.2, Telekommunikationsüberwachung; Datenarten und Auskunft] [13, Checkliste]
Alle Daten, die für den Vertrag zwischen dem_ der Benutzer_in und dem_der Anbieter_in eines Telekommunikationsdienstes oder für ein Teilnehmer_innenverzeichnis erforderlich sind. Beispielsweise Vor- und Nachnamen, akademische Grade, Wohnadressen oder Geburtsdaten.

Unionsrecht
[9.1.2, Grundrechte] [11.2.4, Gesetzesevaluierung; Datenschutzrecht für Polizei und Justiz]
Das Recht der EU. Es ist zwar Völkerrecht, ist jedoch in den Mitgliedstaaten zum Teil (wie auch in Österreich) unmittelbar, das heißt ohne nationales Gesetz, anwendbar. Zudem genießt es immer Anwendungsvorrang, das bedeutet, wenn ein nationales Gesetz dem Unionsrecht widerspricht, ist statt des nationalen Gesetzes Unionsrecht anzuwenden.

Verfassungsgerichtshof (VfGH)
[7.3.1; 7.3.4, Telekommunikationsüberwachung]
[8, Umstrittene Befugnisse]
[9.1.2; 9.2.2; 9.4.2, Grundrechte]
Der Verfassungsgerichtshof wacht darüber, dass staatliches Handeln der Verfassung entspricht. Beispielsweise kann er Gesetze aufheben, wenn sie der Verfassung widersprechen. Er entscheidet jedoch auch als Höchstgericht über Beschwerden gegen Entscheidungen der Verwaltungsgerichte.

Verkehrsdaten
[7.1.; 7.2; 7.4.1; 7.4.4.; 7.5, Telekommunikationsüberwachung; Datenarten, Auskunft, Anlassdatenspeicherung] [13, Checkliste]
Werden zur Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zur Rechnungsstellung verarbeitet, z.B. Daten darüber, wer mit wem wann und wie lange in Kontakt war. Verkehrsdaten sind Metadaten.

Vertrag über die Arbeitsweise der EU (AEUV)
[9.1.2, Grundrechte]
Bildet zusammen mit dem Vertrag über die Europäische Union (EUV) die beiden Gründungsverträge der EU. Sie üben – im übertragenen Sinne – die Funktion einer Verfassung der EU aus, da sie die Grundlage für das politische System der EU bilden.

Vorratsdatenspeicherung
[2.8 (2.11), Überwachungsbefugnisse im Zeitraffer; Vorratsdatenspeicherung ca. 2010–2014]
[3.2, Überwachungstechnologien; Speicherverpflichtungen]
[7.5, Telekommunikationsüberwachung; Anlassdatenspeicherung]
[8.2–8.4, Umstrittene Befugnisse]
[9.2.4, Grundrechte; Recht auf Schutz personenbezogener Daten]
Massenspeicherung von Daten der Bevölkerung über einen längeren Zeitraum, ohne dass ein konkreter Anfangsverdacht bestand, also „auf Vorrat“. Mehrere EuGH Urteile bestätigen, dass eine solche anlasslose Massenüberwachung grundrechtswidrig ist.

WannaCry
[8.1, Umstrittene Befugnisse; Bundestrojaner]
Eine Schadsoftware, die Windows-Systeme befällt, private Daten verschlüsselt und für die Entschlüsselung Lösegeld fordert. Sie wurde im Mai 2017 in Umlauf gebracht und infizierte dabei 230.000 Computer in 150 Ländern, darunter auch solche in Krankenhäusern, Ministerien, Telekom-Konzernen, Tankstellen und Bahnhöfen. WannaCry basiert auf dem Exploit Eternal Blue, den die NSA entwickelt und fünf Jahre lang geheim gehalten hat.

Wegweiserecht
[2.1, Überwachungsbefugnisse im Überblick]
Ist das Recht, das die Polizei innehat, Personen unter Umständen, z.B. wenn sie die öffentliche Ordnung stören, von einem Ort wegzuweisen.

Whistleblower_in
[2.11, Überwachungsbefugnisse im Zeitraffer; Sicherheitspaket]
[9.3.1, Grundrechte; EMRK, siehe Exkurs]
Eine Person, die Informationen über unethisches oder rechtswidriges Verhalten hat und diese an die Öffentlichkeit weitergibt.

Zugangsdaten
[3.2, Überwachungstechnologien; Speicherverpflichtungen] [7.1.; 7.2; 7.4.1; 7.4.4; 7.5, Telekommunikationsüberwachung; Datenarten, Auskunft, Anlassdatenspeicherung] Jene Daten, die beim Zugang zu einem öffentlichen Kommunikationsnetz bei den Betreiber_innen entstehen und für die Zuordnung der für eine Kommunikation verwendeten Netzwerkadressierungen notwendig sind, z.B. IP-Adressen; eine Unterkategorie der Verkehrsdaten.

Rechtsquellenverzeichnis

Überwachungs-befugnis	Auskunftspflicht	Ermittlungsbefugnis	Rand-ziffer
Eingriff in das Briefgeheimnis			
Öffnen und Zurückbehalten von Sendungen am Postweg		§ 135 Abs. 1 iVm § 134 Z 1 StPO iVm § 137 Abs. 1 StPO	8.5
Telekommunikationsdatenauskunft			
Stammdatenauskunft			7.2
Stammdaten	§ 92 Abs. 3 Z 3 TKG		7.1
an Verwaltungs-behörden	§ 90 Abs. 6 TKG		
an Gericht, Staatsanwaltschaft, Kriminalpolizei	§ 90 Abs. 7 TKG	§ 76a Abs. 1 StPO	7.4.2
an Sicherheitsbehörden	§ 90 Abs. 7 TKG	§ 53 Abs. 3a Z 1 SPG, § 11 Abs. 1 Z 5 PStSG	7.4.3 f
an Finanzstraf-behörden	§ 90 Abs. 7 TKG	§ 99 Abs. 3a FinStrG	
Inhaltsdatenauskunft			
Inhaltsdaten	§ 92 Abs. 3 Z 5 TKG		7.1
an Staatsan-waltschaft durch gerichtliche Anordnung		§135 Abs. 3 StPO iVm § 137 Abs. 1 StPO	7.3
Verkehrsdatenauskunft			
Verkehrsdaten	§ 92 Abs. 3 Z 4 TKG		7.1
an Staatsan-waltschaft durch gerichtliche Anordnung	§ 99 Abs. 5 Z 1 TKG	§ 135 Abs. 2 StPO iVm § 137 Abs. 1 StPO	7.4.1
an Sicherheitsbehörden	§ 99 Abs. 5 Z 3 bzw. 5 TKG	§ 53 Abs. 3a – 3b SPG, § 11 Abs. 1 Z 5 bzw. 7 PStSG	7.4.3 f
an Staatsan-waltschaft durch gerichtliche Anordnung	§ 99 Abs. 5 Z 1 TKG	§ 135 Abs. 2 StPO iVm § 137 Abs. 1 StPO	7.4.1
an Staatsan-waltschaft oder Gericht	§ 99 Abs. 5 Z 2 TKG	§ 76a Abs. 2 StPO	7.4.2
an Sicherheitsbehörden	§ 99 Abs. 5 Z 4 bzw. 5 TKG	§ 53 Abs. 3a Z 3 SPG, § 11 Abs. 1 Z 5 bzw. 7 PStSG	7.4.3 f
Standortdatenauskunft			
Standortdaten	§ 92 Abs. 3 Z 6 TKG		7.1
an Staatsan-waltschaft durch gerichtliche Anordnung	§ 99 Abs. 5 Z 1 TKG	§ 135 Abs. 2 bzw. 2a StPO iVm § 137 Abs. 1 StPO	7.4.1
an Sicherheitsbehörden	§ 99 Abs. 5 Z 3 bzw. 5 TKG	§ 53 Abs. 3a und 3b SPG, § 11 Abs. 1 Z 5 bzw. 7 PStSG	7.4.3 f
Fluggastdatenverarbeitung			
durch Sicherheits-behörden, Zollbehörden, Wehr- und Militärbehörden, militärischen Nachrichten-dienste, Staatsan-waltschaft, Gericht, Europol, u.a.	§ 4 Abs. 2 PNR-G	§ 2 Abs. 1 PNR-G, § 4 Abs. 2 PNR-G, § 7 Abs. 1 PNR-G	8.2

Überwachungs-befugnis	Auskunftspflicht	Ermittlungsbefugnis	Rand-ziffer
Verdeckte Ermittlung			
verdeckt durch Sicherheitsbehörden		§ 54 Abs. 3 SPG bzw. § 11 Abs. 1 Z 2 PStSG bzw. § 131 StPO	5.1
Bild- und Tonüberwachung			
offen durch Sicherheits-behörden (Body Worn Cameras)		§ 13a Abs. 3 SPG	6.1.1
offen durch Sicherheits-behörden (Demonstration)		§ 54 Abs. 5 iVm § 16 Abs. 2 SPG	6.1.2
offen durch Sicherheits-behörden (Hot-Spots)		§ 54 Abs. 6 iVm § 16 Abs. 2 SPG	6.1.3
Section Control (für Geschwindigkeits-übertretungen)	§ 98f Abs. 2 StVO	§ 98f Abs. 1 StVO	8.3
verdeckt durch Sicherheits-behörden (Vertrauensperson)		§ 54 Abs. 4 bzw. 4a iVm Abs. 3 SPG, § 11 Abs. 1 Z 3 PStSG, § 136 Abs. 1 Z 1 StPO	6.3
verdeckt durch Sicherheits-behörden (Vertrauensperson) auf gerichtliche Anordnung		§ 136 Abs. 1 Z 2 - 3 und Abs. 2 - 4 StPO	6.3
verdeckt durch Einbindung (öffentlicher und privater) Dritter	§ 93a SPG	§ 53 Abs. 5 SPG	6.2

Abbildungsverzeichnis

Ermittlungsmaßnahmen (III-170 der Beilagen XXV. GP), Bundesministerium für Justiz, Gesamtbericht 2014. Einsatz besonderer Ermittlungsmaßnahmen (III-256 der Beilagen XXV. GP), *Bundesministerium für Justiz*, Gesamtbericht 2015. Einsatz besonderer Ermittlungsmaßnahmen (III-319 der Beilagen XXV. GP), *Bundesministerium für Justiz*, Gesamtbericht 2016. Einsatz besonderer Ermittlungsmaßnahmen (III-63 der Beilagen XXVI. GP), *Bundesministerium Verfassung, Reformen, Deregulierung und Justiz*, Gesamtbericht 2017. Einsatz besonderer Ermittlungsmaßnahmen (III-219 der Beilagen XXVI. GP)

Abbildung 10 S. 102
Häufigkeit der Nachrichtenüberwachung nach § 135 Abs. 3 StPO, Quellen für die Jahre 2008 - 2016: *Bundesministerium für Justiz*, Anfragebeantwortung 12990/AB, XXV. GP vom 08.09.2017 zur Anfrage 13804/J, XXV. GP, https://www.parlament.gv.at/PAKT/VHG/XXV/AB/AB_12990/index.shtml (03.05.2020).

Für das Jahr 2017: *Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz*, Anfragebeantwortung 136/AB vom 16.03.2018, XXVI. GP zur Anfrage 131/J, XXVI. GP, vom 17.01.2018, https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_00136/index.shtml (03.05.2020).

Für das Jahr 2018: *Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz*, Anfragebeantwortung 2609/AB vom 15.03.2019, XXVI. GP zur Anfrage 2625/J, XXVI. GP, vom 16.01.2019, https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_02609/index.shtml (03.05.2020).

Für das erste Halbjahr 2019, in der Graphik hochgerechnet: *Bundesministerium für Justiz*, Anfragebeantwortung 3918/AB, XXVI. GP vom 04.09.2019 zur Anfrage 3899/J, XXVI. GP vom 09.07.2019, https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_03918/index.shtml (03.05.2020).

Abbildung 11 S. 104
Häufigkeit der Datenauskunft nach § 135 Abs. 2 StPO, Siehe die Quellen der Abbildung 10.

Abbildung 12 S. 130
Die Verhältnismäßigkeitsprüfung

Abbildung 13 S. 158
Prüfugsschema Zulässigkeit von automatisierten Entscheidungen

Abbildung 14 S. 161
Beispielbrief für einen Antrag auf Auskunft über die eigenen personenbezogenen Daten

Zitatnachweise

S. 23: „Freedoms we now take for granted were often viewed as threatening or even criminal by the past power structure. Those changes might never have happened if the authorities had been able to achieve social control through surveillance.“

Bruce Schneier, Data and Goliath (2015) S. 115f.

S. 51: „Es ist völlig klar, wenn es eine totale Überwachung gäbe, würde die Zahl der kriminellen Handlungen reduziert werden. Aber die Frage ist: Wollen wir in einer Welt leben, die den Einzelnen auf Schritt und Tritt bis ins Wohn- und Schlafzimmer überwacht?“

Gerhart Holzinger in Sterkl/Völker, VfGH-Präsident kritisiert Überwachungspläne der Regierung, derstandard.at v. 17.02.2017, https://www.derstandard.at/story/2000052786527/vfgh-praesident-holzinger-kritisiert-ueberwachungs-plaene-der-regierung (23.04.2020).

S. 127: „Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.“”

Edward Snowden, https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/?sort=top (23.04.2020).

S. 169: „In einem Staat, der tendenziell jedes Sicherheitsrisiko mit einem Plus an (Überwachungs-)Eingriffen beantwortet, leben letzten Endes unfreie Bürger. ... Also lautet die Gegenformel: Keine Freiheit ohne Risiko.“

Ingeborg Zerbes, Spitzeln, Spähen, Spionieren (2010) S. 376.