www.epicenter.works

HEAT

Handbuch zur Evaluation der Anti-Terror-Gesetze in Österreich 1.2

Christoph Tschohl
Ewald Scheucher
Dieter Kargl
Julia Luksan
Alexander Czadilek
Herbert Waloschek
Reinhard Kreissl
Kilian Klinger
Walter Hötzendorfer
Erich Möchel

EPICENTER .WORKS
for digital rights

research institute

Das Ausmaß der staatlichen Eingriffe in unsere Privatsphäre und in die informationelle Selbstbestimmung lässt sich nur durch die Betrachtung der Summe aller Eingriffe richtig erfassen. Diese wichtige Erkenntnis der Notwendigkeit einer „Überwachungs-Gesamtrechnung“ wurde erstmals vom deutschen Bundesverfassungsgericht im Urteil zur Aufhebung der deutschen Vorratsdatenspeicherung im März 2010 formuliert.
Das Projekt HEAT (Handbuch für die Evaluation der Anti-Terror-Gesetze in Österreich), getragen von epicenter.works (vormals Arbeitskreis Vorratsdaten Österreich - AKVorrat), listet alle Überwachungsgesetze Österreichs auf, kombiniert dies mit einer Aufarbeitung der relevanten Judikatur, einer Erhebung der für Sicherheitsbehörden verfügbaren sowie der tatsächlich eingesetzten Technologien und schließlich einer ersten groben Technikfolgenabschätzung. In den Schlussfolgerungen wird daraus ein Kriterienkatalog für eine Evaluation aller Anti-Terror-Gesetze abgeleitet. Dieses „Pflichtenheft“ soll staatlichen und zivilen Organisationen helfen, überschießende und damit potentiell verfassungswidrige Überwachungsbefugnisse zu identifizieren. HEAT wurde im Rahmen der „netidee“ durch die Internet Foundation Austria gefördert, das Konzept gewann außerdem den Sonderpreis in der Kategorie “Internet Privacy“.

Über epicenter.works - Plattform Grundrechtspolitik

Der Verein epicenter.works (früher AKVorrat) hat sich die Abschaffung der Vorratsdatenspeicherung und die Verhinderung ähnlicher Instrumente der anlasslosen Massenüberwachung zum Ziel gesetzt. Ein Etappenziel wurde mit der Aufhebung der EU-Richtlinie zur Vorratsdatenspeicherung durch den Europäischen Gerichtshof erreicht. Jetzt geht es epicenter.works vor allem darum, starken Datenschutz in unserer Gesellschaft zu verankern und auf die Einhaltung der Menschenrechte im Digitalen zu drängen.
epicenter.works finanziert seine Arbeit aus Spenden: https://spenden.epicenter.works/

Über Research Institute

Die Research Institute ist ein junges Forschungszentrum an der Schnittstelle von Technik, Recht und Gesellschaft, das sich aus multi- und interdisziplinärer Perspektive mit der Frage von Menschenrechten im digitalen Zeitalter beschäftigt. Dies umfasst technische und rechtliche Aspekte von Datenschutz und Datensicherheit ebenso wie Fragen zu Technikfolgenabschätzung, Cybercrime und Netzpolitik. Mit einem ausgewogenen Portfolio aus wissenschaftlicher Grundlagenforschung, R&D-Aktivitäten und Consulting konnte sich das Research Institute seit der Aufnahme seiner operativen Tätigkeit im November 2012 als erfolgreicher Neuzugang in der österreichischen Forschungslandschaft etablieren. Durch aktives Engagement in zivilgesellschaftlichen Initiativen wie epicenter.works ist das Research Institute auch eng mit der österreichischen Datenschutz- und Netzpolitikszene verbunden und versteht sich selbst als "Thinktank im Aufbau". www.researchinstitute.at

Impressum

epicenter.works - Plattform Grundrechtspolitik
Annagasse 8/1/8
1010 Wien
ZVR-Zahl: 140062668
UID: ATU66502037

Zuständige Vereinsbehörde:
Landespolizeidirektion Wien, Büro für Vereins-, Versammlungs- und Medienrechtsangelegenheiten

Dokumenteninformation	
Titel	**HEAT - H**andbuch zur **E**valuation der **A**nti-**T**error-Gesetze in Österreich
Editor	Christof Tschohl, Alexander Czadilek
Autoren	Christof Tschohl, Ewald Scheucher, Dieter Kargl, Julia Luksan, Alexander Czadilek, Herbert Waloschek, Reinhard Kreissl, Kilian Klinger, Walter Hötzendorfer, Erich Möchel
Beschreibung	HEAT 1.2 - Publikation von epicenter.works, basierend auf der Projektarbeit des (von der netidee geförderten) Projekts HEAT
Lizenz	Dieses Dokument wird unter einer CC-BY-SA 4.0-Lizenz veröffentlicht (Vollständiger Lizenztext unter: https://creativecommons.org/licenses/by-sa/4.0/)
Erstellt am	18.08.2016
Letzte Änderung am	31.08.2017
Status	☐ zur projektinternen Verwendung ☒ öffentlich – freigegeben von: epicenter.works/Research Institute ☐ eingeschränkter Zugriff für:

Versionshistorie			
Version	**Datum**	**Geändert von**	**Kommentar**
1.0	15.08.2016		Erstversion für die Abgabe bei „netidee“
1.1	11.09.2016	Christof Tschohl, Alexander Czadilek, Daniel Lohninger (Grafiken)	HEAT 1.1 (Erste öffentlich zugängliche Version)
1.2	30.08.2017	Andreas Czák, Daniel Lohninger (Grafiken), Werner Reiter (Cover Foto – Lizenz CC0 https://creativecommons.org/publicdomain/zero/1.0/deed.de)	Korrektur Rechtschreibfehler, Ersetzen AKVorrat -> epicenter.works, Einfügen des neuen Deckblattes+neuer Grafiken. Aktualisierung auf CI Cover-Foto Werner Reiter

Inhalt

1 Gegenstand und Motivation

1.1 Zielsetzung

Das übergeordnete Ziel von HEAT besteht darin, einen substantiellen Beitrag zu einer sachlichen und nachvollziehbaren Sicherheitspolitik und zu einem entsprechenden öffentlichen Diskurs zu leisten.

Die Arbeitshypothese lautet, dass die Sicherheits- und Strafrechtspolitik der letzten 15 Jahre laufend und meistens anlassbezogen neue Systeme und Befugnisse zur Gefahrenerkennung, zur Gefahrenabwehr und zur Strafverfolgung schafft und dabei wenig Bedacht darauf nimmt, wie sich der stetige normative und faktische Ausbau der Überwachungsmöglichkeiten auf die Gesellschaft als Ganzes sowie auf individuelle grundrechtlich geschützte Sphären auswirkt. Die verschiedenen Systeme, die ihre Rechtfertigung regelmäßig aus dem Kampf gegen den Terrorismus sowie gegen organisierte Kriminalität beziehen, werden dabei in aller Regel nur isoliert betrachtet und Zusammenhänge mit bereits bestehenden Instrumenten und Systemen finden keine besondere Berücksichtigung.

Im Oktober 2011 haben der Verein für Internet-Benutzer Österreichs (VIBE!AT) und der Arbeitskreis Vorratsdaten Österreich - AKVorrat.at (jetziger Name: epicenter.works) eine Bürgerinitiative gestartet. Das Anliegen umfasste zwei Teilbereiche:

„Der Nationalrat wird ersucht: die österreichische Regierung aufzufordern, sich für die ***Aufhebung der EU-Richtlinie zur verdachtsunabhängigen Vorratsdatenspeicherung*** (2006/24/EG) und für ein ***europaweites Verbot der verdachtsunabhängigen Vorratsdatenspeicherung*** einzusetzen. Darüber hinaus wird der Nationalrat ersucht die bestehenden ***Terrorgesetze (einschließlich der Vorratsdatenspeicherung) zu evaluieren*** und falls diese entweder nicht notwendig oder nicht verhältnismäßig sind, zurückzunehmen und das in der Verfassung verankerte Menschenrecht auf Privatsphäre wiederherzustellen."

Die Bürgerinitiative erhielt offizielle Unterstützung von 106.067 Personen. Der erste Teil der Initiative wurde durch die juristischen Bemühungen der Initiatoren selbst auf dem Rechtsweg erreicht – die EU-Richtlinie 2006/24/EG wurde vom EUGH im April 2014 zur Gänze aufgehoben, die österreichische innerstaatliche Umsetzung der Vorratsdatenspeicherungs-RL wurde vom Verfassungsgerichtshof im Juni 2014[1] für ungültig erklärt und aufgehoben.

Der zweite Teil der Bürgerinitiative wurde weder von der Legislative (Parlament) noch von der Exekutive (Bundesregierung) aufgegriffen. Auch nach der Aufhebung der

[1] VfGH 27.6.2014, G 47/2012-49 u.a.

Vorratsdatenspeicherung durch den VfGH zeigte darüber hinaus weder die Exekutive noch die Legislative ein echtes Interesse, bestehende und vor allem neue Instrumente zur Terror- und Kriminalitätsbekämpfung an den eben neu geschaffenen verfassungsrechtlichen Maßstäben zu messen und entsprechend zu handeln. Vielmehr wurden in der Zwischenzeit insbesondere mit dem Polizeilichen Staatsschutzgesetz (PStSG) und anderen legislativen Initiativen die Überwachungsbefugnisse weiter ausgebaut und die Streubreite weiter erhöht.

Daher besteht unverändert die Notwendigkeit, Grundlagen für die Evaluation der Anti-Terrorgesetze in Österreich zu erarbeiten. Zugleich zeigen die Antworten aus verschiedenen Ministerien auf parlamentarische Anfragen rund um das Thema Terrorbekämpfung und Überwachung, die im Rahmen von HEAT ausgearbeitet und in Kooperation mit Parlamentsabgeordneten der Regierung gestellt wurden, dass nicht selten Informationsdefizite und ein Mangel an statistischen Erhebungen zum Einsatz bestimmter Instrumente verhindern, ein vollständiges und richtiges Bild des Status quo zu einem bestimmten Instrument zu erheben.

HEAT will in dieser Situation nicht in der Kritik verharren, sondern konstruktiv vorlegen und – aus zivilgesellschaftlicher Initiative heraus – mit der geforderten Evaluationsarbeit im Sinne der „Überwachungsgesamtrechnung“ beginnen. Das Ergebnis ist das vorliegende Handbuch, das als Hilfestellung für weiterführende und fortlaufende Evaluationsarbeit dienen soll und dafür gleichzeitig die wichtigsten Vorarbeiten als Ausgangsbasis einer Bereichs- und Gesamtevaluation liefert.

Dementsprechend versteht sich HEAT als

- Grundlage und Motivation zur Evaluation aller Anti-Terror Gesetze in Österreich
- Hilfestellung für Zivilgesellschaft und Politik für eine sachliche und verhältnismäßige Sicherheitspolitik und einen entsprechenden öffentlichen Diskurs
- Beitrag für eine faktenbasierte und wirkungsorientierte Gesetzgebung
- Beitrag für neue Ideen zu Methoden, wie die wesentlichen Informationen für das Vorhaben aus komplexen juristischen und technischen Zusammenhängen gewonnen werden können
- Einmahnung der Rechtfertigungslast des Gesetzgebers bei Grundrechtseingriffen.

Gegenstand der Untersuchungen in diesem Handbuch sind:

- gesetzliche Befugnisse, die Grundrechtseingriffe zum Zweck der Bekämpfung von Terrorismus oder organisierter Kriminalität erlauben
- insbesondere verdeckte Maßnahmen und Überwachung
- die Abgrenzung zwischen Strafverfolgung (Repression) und Gefahrenabwehr (Prävention)
- Relevante Judikatur und bekannte Fallkonstellationen
- verfügbare und eingesetzte Technologien der Sicherheits- und Strafverfolgungsbehörden
- Gesellschaftliche Auswirkungen (erste Technikfolgenabschätzung)

In der Zielsetzung zu den Anwendungsbereichen lassen sich zwei wichtige Unterscheidungen treffen:

1. Gesamt-Evaluation („Überwachungs-Gesamtrechnung“)
2. Bereichs-Evaluation (z.B.: nur bestimmte Befugnisse/Instrumente)

Ad 1: Eine vollständige Evaluation im Sinne der „Überwachungs-Gesamtrechnung“ ist kein Unterfangen, das sich kurzfristig bewältigen lässt. Dafür bedarf es einer wohl durchdachten Systematik und vieler Vorarbeiten, von denen manche in diesem Handbuch bereits als Vorschlag enthalten sind. Die wichtigste Vorarbeit betrifft aber die Erhebung und Aufbereitung von Datenmaterial aus der Praxis der eingesetzten Instrumente. Solche Informationen sind die Grundlage für eine ernsthafte Evaluation wobei hier große Lücken offenbar auch in den Ministerien selbst bestehen.[2] Die Gesamtevaluation ist daher eine übergeordnete Zielsetzung, zu deren Erreichung erst ein Fahrplan auszuarbeiten ist, wofür HEAT einen ersten Vorschlag unterbreitet.

Ad 2: Bereichs-Evaluationen sollten theoretisch schon jetzt bei jeder neuen Gesetzesinitiative zur Schaffung neuer Instrumente und Ermittlungsmaßnahmen zum Standard-Prozedere gehören, nämlich in Form der „Wirkungsorientierten Folgenabschätzung“ (WFA). Diese ist im gegenwärtigen Zustand aber schon in der Konstruktion zu hinterfragen, weil sich selbst in Vorschlägen mit schwerwiegenden und breitgestreuten Grundrechtseingriffen die Ausführungen dort regelmäßig auf die Kostenfragen und Budgetauswirkungen beschränken. Praktisch besteht das Problem, dass die Fragen zur WFA nicht selten erstmals in der letzten Phase der legistischen Umsetzung überhaupt bearbeitet werden, obwohl in dieser Phase die sachlichen Grundlagen des Vorhabens eigentlich längst geklärt und ausgewiesen sein sollten. HEAT orientiert sich zwar an den bestehenden Strukturen der WFA, hält aber nicht daran fest, sondern macht einen eigenständigen Vorschlag unter Verwendung von Mindmaps und Checklisten. Abseits der Problematik der Folgenabschätzung bei neu eingeführten Maßnahmen werden konkrete und priorisierte Vorschläge formuliert, welche bestehenden Bereiche einer Evaluation zugeführt werden sollten.

Zwischen 1. und 2. bestehen insofern Zusammenhänge, als einerseits methodische weitgehende Überschneidungen bestehen und andererseits jede Bereichsevaluation einen Teilbeitrag für eine Gesamtevaluation darstellt, aus deren Erfahrung sich auch nützliche Lehren für eine Gesamtevaluation ziehen lassen. Der wichtigste Zusammenhang besteht aber darin, dass eine stetige und vollständige Anwendung der Folgenabschätzung im Sinne von HEAT die systematische Grundlage schaffen könnte, um

[2] So kann beispielsweise das Justizministerium nur Auskunft darüber geben, wie viele Überwachungsmaßnahmen auf Basis des § 135 StPO angeordnet wurden, aber eine genauere Unterscheidung, wie viele Fälle davon Inhaltsüberwachungen, wie viele Verkehrs- und Standortdatenauskünfte betroffen haben, ist bereits nicht mehr verfügbar.

fortlaufende Evaluationen auch im Hinblick auf die Gesamtsituation in der Zukunft mit relativ überschaubarem Aufwand bewältigen zu können.

1.2 Die Balance von Freiheit und Sicherheit

Der öffentliche politische Diskurs im Zusammenhang mit den auch in Europa häufiger werdenden Bedrohungen durch Terrorismus und Extremismus ist davon geprägt, dass insbesondere in Reaktion auf konkrete tragische Ereignisse geradezu reflexartig Sicherheit und Freiheit als Antipoden dargestellt werden. Dabei wird postuliert, dass eine Erhöhung oder auch nur Erhaltung der Sicherheit zwangsläufig mit Einschränkungen der Freiheit auch gegenüber der friedlichen Mehrheitsbevölkerung einhergehen. In einer von Angst beherrschten gesellschaftlichen Stimmung und mit dem Mantra dieser Prämissen wurden in den letzten fünfzehn Jahren Maßnahmen eingeführt, die noch kurz zuvor nicht mehrheitsfähig waren.

Das Paradigma dieser Dynamik, wenngleich nur als Spitze des Eisbergs, ist die Vorratsdatenspeicherung. Bei der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung (VDS-RL) handelte es sich um eine EU-Richtlinie zur verdachtsunabhängigen Speicherung von Kommunikationsdaten aller elektronisch kommunizierenden Menschen in der EU. Nach langer Untätigkeit und kurz vor fällig werden von Strafzahlungen an die EU, setzte schließlich auch der österreichische Gesetzgeber die VDS-RL durch Novellierungen des Telekommunikationsgesetzes (TKG), des Sicherheitspolizeigesetzes (SPG) und der Strafprozessordnung (StPO) um, die allesamt am 1. April 2012 in Kraft traten. Der Speicherpflicht unterlagen nach § 102a TKG sogenannte Verkehrsdaten „zur Rückverfolgung und Identifizierung der Quelle einer Nachricht“ sowie „zur Identifizierung des Adressaten“, „zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung“, „zur Bestimmung der Art einer Nachrichtenübermittlung“, zur Bestimmung der (vorgeblichen) Endeinrichtung und schließlich „zur Bestimmung des Standorts mobiler Geräte“. Dagegen durften schon nach Art 5 Abs 2 VDS-RL keinerlei Daten auf Vorrat gespeichert werden, „die Aufschluss über den Inhalt einer Kommunikation geben“.

Die Zugriffsberechtigungen, welche die Behörden durch diese Änderungen erhielten gingen jedoch über die unionsrechtlichen Mindestanforderungen hinaus. Problematisch erscheint in dieser Hinsicht insbesondere die Aufzeichnung von IP-Adressen, mit Hilfe derer die Behörden Rückschlüsse auf einen bestimmten Anschluss/Teilnehmer ziehen können. Die Auskünfte zu Name und Anschrift zu einer IP-Adresse wurden nämlich – entgegen der Zielsetzung der VDS-Richtlinie – nicht auf „schwere Straftaten“ beschränkt sind, sondern durften (und dürfen) zur Ermittlung, Feststellung und Verfolgung jeder gerichtlich strafbaren Handlung per Anordnung durch die Staatsanwaltschaft von den Telekommunikation-Anbietern verlangt werden. Dieselben Möglichkeiten standen auch der Polizei, ohne gerichtliche oder sonstige Bewilligung (z.B. durch einen Rechtsschutzbeauftragten) und ohne Einschränkung auf den Schutz bestimmter

höherwertiger Rechtsgüter, im Rahmen der Gefahrenabwehr zur Verfügung, obwohl in der VDS-RL bewusst die Vorratsdatenspeicherung bzw. der Zugriff auf Vorratsdaten nicht als Mittel zur Gefahrenabwehr vorgesehen war.

Am 08.04.2014 hob der Gerichtshof der EU (EuGH) die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung (VDS-RL), zur Gänze auf, weil die verdachtsunabhängige und anlasslose Überwachung der gesamten Bevölkerung gegen EU-Grundrechte verstieß. Der Diskurs, der durch die innerstaatliche Umsetzung und Abschaffung der VDS ins Rollen gekommen war, hatte wesentliche neue Erkenntnisse zur Bedeutung des Datenschutzgrundrechts geliefert und gleichzeitig die öffentliche Auseinandersetzung mit dem Verhältnis von Sicherheit zu Freiheit, in Österreich und ganz Europa wieder angefacht.[3]

Der EuGH erkennt in seiner Urteilsbegründung zwar ausdrücklich an, „*dass nach Art. 6 der Charta jeder Mensch nicht nur das Recht auf Freiheit, sondern auch auf Sicherheit hat*“[4]. Allerdings führt der Gerichtshof weder in dieser noch einer anderen Entscheidung weiter aus, welchen substantiellen Gehalt das individuell garantierte „Recht auf Sicherheit“ nach Art 6 EU Grundrechte-Charta hat.

Auch Art. 5 der Europäischen Menschenrechtskonvention garantiert im ersten Satz wortgleich: „*Jede Person hat das Recht auf Freiheit und Sicherheit*“. Die ausdrückliche Erwähnung des Rechts auf Sicherheit in den Freiheitsgewährleistungen ist eher als Katalysator für die Einhaltung der Gesetzmäßigkeit bei Freiheitsentziehungen zu verstehen. Der Verfassungsgesetzgeber des „Bundesverfassungsgesetzes zum Schutz der persönlichen Freiheit“ (BVG PersFrG) hat den Begriff unreflektiert aus der Konvention übernommen.[5] Nach herrschender Ansicht kommt ihm nach keiner der Grundrechtsgarantien eine eigenständige Bedeutung zu, das Schutzgut der „persönlichen Freiheit“ wird dadurch nicht erweitert.[6] Der Europäische Gerichtshof für Menschenrechte (EGMR) leitet daraus in seiner bislang einzigen ausdrücklichen Entscheidung zum „Recht auf Sicherheit“ einen gewissen Schutz vor staatlichen Maßnahmen außerhalb des Hoheitsgebietes des handelnden Konventionsstaates ab[7].

---

[3] Mit detaillierten Nachweisen siehe Tschohl, Vorratsdatenspeicherung - Aufstieg und Fall in Österreich, in: Jahrbuch Datenschutzrecht (2014), 31.

[4] Urteil des EuGHs In den verbundenen Rechtssachen C-293/12 und C-594/12, RN 42.

[5] Vgl. zur Ergänzung der Worte „und Sicherheit“, die in der Regierungsvorlage zum PersFrG noch nicht enthalten waren, *Laurer*, Verfassungsänderungen 1988 (1989) 28 f.

[6] *Berka*, Grundrechte, Rz 400 f; *Kopetzki*, in Korinek/Holoubek (Hrsg), Art 1 PersFrG, Rz 17; zur Straßburger Judikatur bis 1996 vgl. *Peukert*, in *Frohwein/Peukert*, EMRK², Art 5, Rz 4 f; vgl aus der jüngeren Rsp EGMR 1.6.2004, *Altun*, 24.561/94.

[7] Im Urteil *Öcalan* sah der EGMR das Recht auf Sicherheit durch die Verhaftung *Öcalans* durch türkische Organe in Kenia (ohne dessen Einverständnis) berührt. Vgl *Grabenwarter*, EMRK³, 161, Rz 3.

Der österreichische Verfassungsgerichtshof (VfGH) folgte in seinem Erkenntnis vom 27.06.2014 dem EuGH in Sachen Vorratsdatenspeicherung und hob auch die innerstaatliche Umsetzung der VDS-RL als verfassungswidrig auf. Allerdings fand der VfGH in seiner Urteilsbegründung[8] zum Spannungsfeld Sicherheit und Freiheit sehr viel klarere Worte:

„Ausgangspunkt der Beurteilung der Verhältnismäßigkeit der Vorratsdatenspeicherung ist die Einsicht, dass das Grundrecht auf Datenschutz in einer demokratischen Gesellschaft – in der hier bedeutsamen Schutzrichtung – auf die Ermöglichung und Sicherung vertraulicher Kommunikation zwischen den Menschen gerichtet ist. Der Einzelne und seine freie Persönlichkeitsentfaltung sind nicht nur auf die öffentliche, sondern auch auf die vertrauliche Kommunikation in der Gemeinschaft angewiesen;
die **Freiheit als Anspruch** des **Individuums** und **als Zustand** einer **Gesellschaft wird bestimmt von** der **Qualität** der **Informationsbeziehungen** (....)."[9]

Unbestritten ist, dass sowohl das Individuum als auch die Gemeinschaft unter bestimmten Umständen einen Anspruch darauf hat, durch staatliche Organe vor spezifischen Bedrohungen geschützt zu werden. Dieser Anspruch erwächst in der Form von positiven Schutz- und Gewährleistungspflichten im Hinblick auf alle garantierten Grundrechte, etwas das Recht auf Leben[10], das Verbot der Folter, das Recht auf Meinungsfreiheit, das Recht auf Privatsphäre und viele mehr. Das bedeutet, dass der Staat für Bedrohungen und Verletzungen der grundrechtlich geschützten Rechtsgüter, die an sich nicht dem Staat zurechenbar sind, dann trotzdem haftet, wenn er keinen angemessenen Schutz gegen Bedrohungen durch „Dritte" geboten hat. Daher ist es letztlich ein Ausfluss dieser staatlichen Schutzpflichten – Hand in Hand mit der Begründung eines grundsätzlichen staatlichen Gewaltmonopols – dass ein System der Strafverfolgung und der Sicherheitspolizei zur Prävention sowie zur Aufklärung von Straftaten eingerichtet wird.
Insofern ist die tägliche Arbeit der Strafverfolgungs- und Sicherheitsbehörden nicht nur als Eingriff in Grundrechte, sondern zugleich als stetiger (proaktiver und reaktiver) Schutz von Grundrechten zu verstehen. Die Herausforderung für das System ist dabei, die Balance nicht zu verlieren und rechtsstaatliche Grundprinzipien einzuhalten. Grundrechtseingriffe müssen in einem angemessenen Verhältnis zu den legitimen Zwecken stehen.

Das Rechtsstaatsprinzip und der Grundsatz der Verhältnismäßigkeit dürfen aber nicht zur leeren Formel verkommen. Der Gesetzgeber muss abstrakt vorzeichnen, wo die Pole einer Abwägungsentscheidung liegen und nach welchen Kriterien diese konkretisiert

[8] Unter Verweis auf Berka, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT, 2012, Band I/1, 22.
[9] VfGH 27.6.2014, G 47/2012-49 u.a., Rz 167.
[10] Urteil des EGMR vom 31.5.2007 im Fall Kontrová gg. die Slowakei (NL 2007, 133).

werden soll. Das System muss strukturelle Schutzvorkehrungen vorsehen, damit die Verhältnismäßigkeit auch im Einzelfall möglichst gewahrt bleibt.

Wenn es aber keinen effektiven Rechtsschutz gegen Grundrechtseingriffe von hoher Intensität gibt, können Ermittlungen gleichzeitig unkontrollierbar – wie bei einem Stein, den man ins Wasser wirft – immer weitere Kreise ziehen, wobei die Rechtsstaatlichkeit und am Ende der Rechtsstaat gefährdet sind. Schlussendlich wird aus dem Rechtsstaat ein Polizeistaat.

Das gegenständliche Handbuch soll einerseits identifizieren, in welchen Bereichen die Österreichische Rechtsordnung in dieser Hinsicht Defizite und bedenkliche Tendenzen aufweist, andererseits soll ein Leitfaden geboten werden, der mit einer immanenten Systematik zur Evaluation neuer Vorhaben oder bestehender Systeme dazu beitragen will, den demokratischen Rechtsstaat auch bei diffusen und ständigen Bedrohungen der Sicherheit nachhaltig abzusichern.

1.2.1 Ansätze zum Umgang mit Terrorismus und „Feindrechtsstaat“ [11]

Geht man, wie gemeinhin wohl angenommen, davon aus, dass Strafrecht vor Übeln schützt oder zumindest schützen sollte, muss man akzeptieren, dass der Schutz vor Angriffen oder Rechtsverletzungen notwendig zukunftsorientiert ist, da Verletztes oder Beschädigtes nicht mehr geschützt wird, sondern geheilt oder repariert werden muss. Die rechtsstaatlichen Garantien im Strafrecht (Unschuldsvermutung, Analogieverbot, Rückwirkungsverbot, Bestimmtheitsgebot, etc.) hingegen zeigen eine andere Blickrichtung – sie greifen erst post festum.[12]

Kaum ein Rechtsbereich bedarf so sehr einer theoretischen Begründung wie das Strafrecht. Beispielsweise beinhaltet ein aus vier Wörtern bestehender, tragender strafrechtlicher Grundsatz wie „Keine Strafe ohne Schuld“ zwei Begriffe, deren theoretische und praktische Aufarbeitung Bibliotheken füllen und Strafrechtswissenschafter ebenso herausfordern wie Philosophen und Theologen.

Straftheorien werden im Hinblick auf die Rechtfertigung(sfähigkeit) eines „Feindstrafrechts“ zu prüfen sein. Ein Problemaufriss in der gebotenen Kürze: Absolute Straftheorien sehen Sinn und Rechtfertigung der Strafe im Ausgleich des gesetzten Übels, relative Straftheorien orientieren sich an der Prävention. Vereinigungstheorien (in

[11] Scheucher, Dissertation Universität Liechtenstein, Feindrechtsstaat und Feindstrafrecht, Arbeitsversion, Fertigstellung Oktober 2016.

[12] Vgl. dazu etwa: Marcel Alexander *NIGGLI*/Stefan *MAEDER*, Was schützt eigentlich Strafrecht (und schützt es überhaupt etwas, in: *Mantscher/Pernthaler/Raffeiner* (Hrsg.), Ein Leben für Recht und Gerechtigkeit, Festschrift für Hans R. Klecatsky zum 90. Geburtstag, NWV, 2010.

unterschiedlichster Ausprägung) vereinigen den Präventiv- und den Vergeltungsgedanken.[13]

Die Relevanz dieser Überlegungen erklärt sich fast von selbst:
Sollen angesichts der neuen politischen Problemstellungen (Stichwort: sog. „Islamischer Staat") jene Gefahren für „unser Gemeinwesen", die von „unseren Feinden" ausgehen, abgewehrt werden, müssen strafrechtliche Garantien (wie Schuldprinzip, Rückwirkungsverbot, Unschuldsvermutung, etc.) abgebaut werden, da sie effizienten Ermittlungen und einer erfolgreichen Strafverfolgung im Wege stehen oder zumindest zu stehen scheinen. Da die Gefahrenabwehr in den Vordergrund der Überlegungen rückt, muss die Strafbarkeit soweit wie möglich in das „Vorfeld" des eigentlich bekämpften strafbaren Verhaltens verlagert werden. Hier muss regelmäßig das Argument herhalten, „unsere Feinde" hielten sich weder an staatliche noch an moralische Gesetze und seien daher immer einen Schritt voraus.[14]

Damit ist eines der wesentlichsten Elemente des modernen „Feindstrafrechts" angesprochen. Neben der allgemeinen Tendenz der Verschärfung der Strafdrohungen z.B. im Bereich der „organisierten Kriminalität" lassen sich vier Kriterien herausarbeiten, die das „Feindstrafrecht" kennzeichnen: (i) die Vorverlagerung der Strafbarkeit durch Schaffung neuer „Gefährdungsdelikte", (ii) keine der Vorverlagerung proportionale Reduktion der Strafe, (iii) der Übergang von der Strafrechtgesetzgebung zur „Bekämpfungsgesetzgebung" und (iv) der Abbau strafprozessualer Garantien.[15]

Auch wenn Befürworter eines „Feindstrafrechts" im rechtswissenschaftlichen Bereich (wenige[16]) und dessen Gegner im rechtspraktischen und -wissenschaftlichen Bereich (viele [17]) zu diesem Thema kaum einen grundsätzlichen Konsens finden können, steht außer Streit, dass es beim „Feindstrafrecht" im Kern um den Idealtypus eines Strafrechts geht, in welchem der „Feind" seinen Status als „Person" verliert und als „Gefahrenquelle" unschädlich gemacht werden muss.[18]

Mit der „organisierten (internationalen) Kriminalität", den Terroristen, den Extremisten, den Radikalen aller Schattierungen sind dem „freien Westen" und damit auch dem kleinen

[13] Auch dazu etwa: Marcel Alexander *NIGGLI*/Stefan *MAEDER*, a.a.O.
[14] In diesem Sinne etwa Jakobs, Kriminalisierung im Vorfeld einer Rechtsgutverletzung, ZStW 97,1985, S. 751-785.
[15] *Jakobs* im Rahmen einer Tagung an der Akademie der Wissenschaften Berlin-Brandenburg; dokumentiert in: Eser/Hassemer (Hg.), Die deutsche Strafrechtswissenschaft vor der Jahrtausendwende, 2000, S. 47ff.
[16] Z.B. *Depenheuer*, Selbstbehauptung des Rechtsstaates, Schöningh, 2. Auflage (2008).
[17] *Uwer / Organisationsbüro (Hrsg.),* Bitte bewahren Sie Ruhe, Leben im Feindrechtsstaat, Vereinigung Berliner Strafverteidiger, 1. Auflage (2006).
[18] „Der prinzipiell Abweichende bietet keine Garantie personalen Verhaltens; deshalb kann er nicht als Bürger behandelt, sondern muss als Feind bekriegt werden" (Jakobs, Bürgerstrafrecht und Feindstrafrecht, in: HRRS Ausgabe 3/2004, S. 90).

Österreich offenbar so viele „Feinde“ erwachsen, dass deren – tatsächliche oder behauptete – Gefährlichkeit von der Politik und den staatlichen und supranationalen Sicherheitsapparaten nur mehr durch eine ständig gesteigerte Intensität von Grundrechtseingriffen durch eine massive „Sicherheitsgesetzgebung“ begegnet werden kann. Natürlich nur, um „Sicherheit“ zu gewährleisten. Angesichts dieser Gefahren für „unser Gemeinwesen“, die von „unseren Feinden“ ausgehen, erhalten effiziente Ermittlungen und eine erfolgreiche Strafverfolgung offensichtlich oberste Priorität, was immer auch die Folgen für unser Gemeinwesen sein mögen. Wir befinden uns im Übergang weg von einer „Strafrechtgesetzgebung“, die inkriminiertes Verhalten sanktioniert, hin zu einer „Bekämpfungsgesetzgebung“, die „unsere Feinde“ schon im Vorfeld erkennen und ausschalten soll.

Da spätestens seit dem 11. September 2001 die Gefahrenabwehr in den Vordergrund der Sicherheits- und Justizpolitik rückte, wurde, wie schon erwähnt, bereits die Strafbarkeit soweit wie möglich in das „Vorfeld“ des eigentlich bekämpften strafbaren Verhaltens verlagert. Mit dem jüngsten, im Juli 2016 in Kraft getretenen, Gesetz zur Terrorismusbekämpfung, dem Polizeilichen Staatsschutzgesetz (PStSG), sollen das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) und die sicherheitspolizeilichen Behörden zur vermeintlichen Kompensation des Problems, dass „unsere Feinde“ sicher weder an staatliche noch an moralische Gesetze halten und uns immer einen Schritt voraus sind, nun über mancherlei rechtsstaatliche „Hindernisse“ erhaben werden.

Als Beispiele vorverlagerter Strafbarkeit mögen die Bestimmungen des § 278b („Terroristische Vereinigung“), § 278d („Terrorismusfinanzierung“), § 278e („Ausbildung für terroristische Zwecke“) und § 278f („Anleitung zur Begehung einer terroristischen Straftat“) jeweils des österreichischen StGB dienen. Der ehedem geplante § 278g öStGB („Gutheißen einer terroristischen Straftat“) scheiterte 2011 (vorläufig) am heftigen Widerstand insbesondere auch der Medien (bis in den Bereich konservativer Publizistik), wegen befürchteter repressiver Eingriffe in die Meinungs- und Pressefreiheit (hinsichtlich kritischer Berichterstattung und Kommentierung)[19].

Die Vorverlagerung der Strafbarkeit, die Schaffung neuer Straftatbestände wie des § 278d öStGB („Terrorismusfinanzierung“) oder § 278b öStGB („Terroristische Vereinigung“) werfen aber praktische Probleme auf. Die Ermittler, die „Staatsschutzorgane“, brauchen Informationen, sie brauchen Daten, um Verdächtige aus der Masse der harmlosen Bürgerinnen und Bürger „herausfiltern“ zu können.

Soweit es finanzielle Transaktionen betrifft, reichen die internationalen Bestrebungen hier weit zurück. Die im Juni 1989 von den Staatschefs der G7-Staaten und dem

[19] Vgl. dazu auch FN 2, der „Rahmenbeschluss“ hatte Anregungen in diese Richtung enthalten.

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)“[20] verabschiedete 40 „Empfehlungen“ [21], (und 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 drei „Geldwäsche-Richtlinien“, eine vierte ist in Vorbereitung. Die EU-Kommission ist der Meinung[22], dass es zur Umsetzung der Empfehlungen der FATF zur Terrorismusfinanzierung erforderlich ist, den Rahmenbeschluss 2002/475/JI zur Terrorismusbekämpfung zu überarbeiten. Diese Überarbeitung soll in Bestimmungen der Anti-Terror Richtlinie[23] der EU ihren Niederschlag finden, die sich derzeit in den Trilog-Verhandlungen zwischen Kommission, Rat und Europäischem Parlament befinden.

Einen echten qualitativen „Beitrag“ in Richtung „Überwachungsstaat“ brachte die 3. Geldwäsche-Richtlinie.[24] War die Bekämpfung der organisierten Kriminalität und hier insbesondere des internationalen Suchtgifthandels zentraler Gegenstand der 1. Geldwäsche-Richtlinie 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 – das sind praktisch alle, wie ein Blick zumindest in das österreichische Strafgesetzbuch zeigt.

Die „Terrorismusfinanzierung“ geriet ebenfalls ins Visier der Überwacher. „Aus dem einheitlichen Finanzraum Europa soll damit nicht nur durch Straftaten erworbenes Geld ferngehalten werden, die Kontrolle erstreckt sich vielmehr auch auf rechtmäßig erworbenes Vermögen, solange es sich nur denkmöglich dem Verdacht aussetzt, dem Terrorismus zu dienen“.[25]

---

[20] Näheres siehe unter http://de.wikipedia.org/wiki/Financial_Action_Task_Force_on_Money_Laundering.

[21] Siehe oben FN 3.

[22] 2015/0281 (COD) Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI zur Terrorismusbekämpfung, S. 7.

[23] Mit einer Beschlussfassung der Richtlinie durch das Europäische Parlament ist im Herbst 2016 zu rechnen.

[24] Richtlinie 2005/60/EG des europäischen Parlaments und des Rates vom 26.10.2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, ABl. L 309/15 vom 25.11.2005.

[25] *Sommer*, Geldwäschemeldungen und Strafprozess, in. StraFo 2005, S. 327 – 334.

Der Kontrollor der Zukunft soll nach dem „blueprint“ der Geldwäsche-Richtlinien der Bürger selbst sein, der im (gesetzlich normierten) Auftrag des Staates seine Mitmenschen kontrolliert – und sie im Verdachtsfall meldet.

Seit der Umsetzung der 3. Geldwäsche-RL in Österreich (auch durch Novellierung der Rechtsanwaltsordnung (RAO)[26]) können österreichische Rechtsanwältinnen und Rechtsanwälte in die absurde Situation geraten, in Entsprechung des § 8c öRAO hinter dem Rücken ihrer Mandanten Informationen über einen „Verdacht“ auf „Terrorismusfinanzierung“ oder Geldwäschehandlungen an das Bundesministerium für Inneres (sohin den Polizeibehörden!) melden zu müssen.[27]

Für den Moment sollen nur zwei besonders problematische „überwachungsstaatliche“ Aspekte der 3. Geldwäsche-Richtlinie (bzw. ihrer innerstaatlichen Umsetzung in Österreich) angesprochen werden. Erstens unterliegen Untersuchungshandlungen und Ermittlungen unterhalb der Schwelle eines „Anfangsverdachts“ nicht den Regelungen und damit den Schutzmechanismen der Strafprozessordnung. Zweitens erfolgen die in der 3. Geldwäsche-Richtlinie vorgesehenen „Überwachungen“ nicht durch (mit hoheitlichen Befugnissen ausgestattete) Behörden, sondern eben durch „Private“, durch Banken, Unternehmen, Notare und Rechtsanwälte.

Gibt es einen „Verdacht“ auf Geldwäsche und/oder Terrorismusfinanzierung, werden Privatpersonen automatisch zu Spitzeldiensten verpflichtet, aus der Sicht des Staates werden Spitzeldienste zur „Bürgerpflicht“.

1.3 Die Überwachungs-Gesamtrechnung

1.3.1 Blick nach Deutschland

Im Urteil 1 BvR 256/08 (u.a.) hat das deutsche Bundesverfassungsgericht (BVerfG) ausgesprochen, dass eine Normierung der Vorratsdatenspeicherung (Speicherung von Telekommunikationsverkehrsdaten) nicht als Schritt zu einer Gesetzgebung hin verstanden werden darf, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten

[26] Rechtsanwaltsordnung (RAO), RGBl. Nr. 96/1868 idF BGBl. I Nr. 164/2005.

[27] § 8c. (1) In den Fällen des § 8a Abs. 1 hat der Rechtsanwalt unverzüglich den Bundesminister für Inneres (Bundeskriminalamt, Geldwäschemeldestelle gemäß § 4 Abs. 2 Bundeskriminalamt-Gesetz) zu informieren, wenn er weiß, den Verdacht oder berechtigten Grund zu der Annahme hat, dass das Geschäft der Geldwäscherei (§ 165 StGB) oder der Terrorismusfinanzierung (§ 278d StGB) dient (Verdachtsmeldung). Der Rechtsanwalt ist aber nicht zur Verdachtsmeldung hinsichtlich solcher Tatsachen verpflichtet, die er von einer oder über eine Partei im Rahmen der Rechtsberatung oder im Zusammenhang mit ihrer Vertretung vor einem Gericht oder einer diesem vorgeschalteten Behörde oder Staatsanwaltschaft erfahren hat, es sei denn, dass die Partei für den Rechtsanwalt erkennbar die Rechtsberatung offenkundig zum Zweck der Geldwäscherei (§ 165 StGB) oder der Terrorismusfinanzierung (§ 278d StGB) in Anspruch nimmt.

abzielt. Der Gerichtshof ist der Ansicht, dass die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung von Vorratsdaten voraussetzt, dass diese eine Ausnahme bleibt. Zudem darf sie auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen. Die Einführung der Vorratsdatenspeicherung kann demnach nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen mit Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung. Insgesamt ist das BVerfG der Ansicht, dass durch die Vorratsdatenspeicherung der Spielraum für weitere Datensammlungen erheblich geringer wird. Damit wird die Maxime ausgesprochen, dass eine staatliche Überwachungsmaßnahme bzw. deren Verhältnismäßigkeit also nur beurteilt werden kann, wenn man diese in Zusammenschau mit anderen, bereits bestehenden (Überwachungs-)Befugnissen betrachtet. In besagtem Urteil wird erstmals von einem europäischen Höchstgericht die Idee und die Notwendigkeit einer Überwachungs-Gesamtrechnung ausgedrückt.

Für die Beurteilung der Zulässigkeit der gesetzlich normierten Grundrechtseingriffe ist also 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 verschiedenen Gesetzen (StPO, SPG, PStSG) zu sehen.[28] Andererseits sind auch die verfügbaren Technologien, deren mehr oder weniger präzise gesetzliche Erfassung, sowie deren Eignung für Grundrechtseingriffe, zu berücksichtigen. Wie schon das deutsche BVerfG festgehalten hat, kann eine staatliche Überwachungsmaßnahme bzw. deren Verhältnismäßigkeit nur beurteilt werden, wenn man diese in Zusammenschau mit anderen, bereits bestehenden Befugnissen betrachtet. Durch die Summe aller Eingriffe kann sich ergeben, dass der Spielraum des Gesetzgebers zur Normierung neuer Befugnisse enger wird.[29] Damit ist im Prinzip die Notwendigkeit der „Überwachungs-Gesamtrechnung“ formuliert.[30]

1.3.2 Überwachungsprojekte in der Sicherheitsforschung

Die Projekte Indect, IObserve und IObserveNG dienen als Beispiele für eine potentiell zukünftige Überwachungssituation in europäischen Großstädten. Im Folgenden werden diese Projekte beschrieben und ihre Problematik aufgezeigt. Die Projekte DIANGO und

[28] Siehe dazu unten ausführlich Kapitel 5.2.1.
[29] BVerfG, 1 BvR 256/08 u.a. vom 2.3.2010 (FN 64), RZ 218.
[30] Vgl. für Deutschland die Linksammlung zur „Überwachungs-Gesamtrechnung“ unter https://digitalcourage.de/themen/ueberwachungsgesamtrechnung (11.8.2016).

DIANA geben Aufschluss darüber, welche (mächtigen) Instrumente den Sicherheitsbehörden in absehbarer Zeit zur Verfügung stehen werden.

1.3.2.1 Projekt INDECT [31]

Das Projekt INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment) ist ein EU-Forschungsprojekt im Rahmen des FP7. Start des Forschungsprojekts war 2009. Das Ziel ist es, eine zentrale Schnittstelle zu entwickeln, in der Überwachungsdaten aus vielen unterschiedlichen Quellen miteinander verknüpft und durch Software automatisiert auf mögliche „Gefahren" und „abnormes Verhalten" untersucht werden können. Durch öffentliche Überwachungskameras und Drohnen sollen Computer die Bilddaten abgleichen und so automatisiert Gefahren und abnormes Verhalten erkennen können. Dies soll der vorbeugenden Kriminalitätsbekämpfung dienen. Abgeglichen werden diese Daten unter anderem mit Daten aus sozialen Netzwerken (z.B.: Facebook) und Chats. Dadurch sollen auf automatische Weise strafrechtlich relevante Bedrohungen und Taten erkannt werden. Problematisch erscheint, dass bereits zu langes Sitzen an öffentlichen Plätzen oder plötzliches schnelles Bewegen, sei es um einen Bus zu erwischen oder weil man in Eile ist, zu den abnormalen Verhaltensweisen gehören, welche identifiziert werden und von ferngesteuerten Drohnen mit Überwachungskameras verfolgt werden.

Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird wahrscheinlich versuchen, nicht durch solche Verhaltensweisen aufzufallen und seine völlig normalen und ungefährlichen Verhaltensweisen ändern oder anpassen. Der persönliche Freiraum des Individuums wird eingeschränkt, weil dieses befürchten muss, durch an sich unproblematisches Verhalten Nachteile zu erleiden (bspw. besondere Personenkontrollen oder Sicherheitsüberprüfungen an Flughäfen).

[31] http://www.indect-project.eu/ (11.8.2016).

1.3.2.2 Projekt CLEAN IT[32]

Clean IT ist ein Projekt der EU zur Bekämpfung illegaler Inhalte im Internet. Es hat eine Partnerschaft zwischen den Sicherheitsbehörden und IT-Unternehmen zum Ziel und dient der Sperrung des Zugriffs auf terroristische Inhalte im Internet. Dabei werden diese Seiten von Nutzern, oder IT-Unternehmen gemeldet und anschließend gesperrt und nachverfolgt, wer der Betreiber dieser Seite ist. Somit dient es nicht nur der Absicherung des Internets vor terroristischen Inhalten, sondern auch zur Verbrechensaufklärung. Start des Projekts war im April 2011 und das erklärte Ziel soll eine flächendeckende Kontrolle der Netzinhalte auf globaler Ebene sein. Problematisch erscheint, dass die IT-Unternehmen selbst entscheiden welcher Inhalt gesperrt werden soll und somit in ein freies Internet deutlich eingegriffen wird.

1.3.2.3 Projekt IObserve

IObserve (Intelligente Videoüberwachung der nächsten Generation mit semantischen Templates) ist ein Forschungsprojekt mit dem Ziel videobasierte Überwachungssysteme der nächsten Generation zu schaffen.

Im Unterschied zu normalen Videoüberwachungssystemen, die Handlungen aufzeichnen oder Live an einen Monitor weiterleiten, bei der ein Mensch die Beobachtung vornimmt ist hierbei das Ziel, dass das System selbst erkennt, welche Handlungen von Personen vorgenommen werden. Hierzu werden Detektionsalgorithmen verwendet, welche Personen, Objekte, Fahrzeuge oder Gegenstände erkennen und benennen können, sowie interpretieren können. Mithilfe statistischer Funktionen soll dieses System dazulernen um im Laufe der Zeit genauer zu werden. Ein weiterer Fokus bei der Entwicklung dieses Systems liegt darin, dass es von Laien einfach zu bedienen sein soll, sowie Ereignisse in natürliche Sprache übersetzen soll. [33]

1.3.2.4 Projekt IObserve NG

IObserve NG (Verteilte Videoüberwachung in einer hochskalierbaren service-orientierten Architektur) ist ein sich derzeit in Entwicklung befindendes System, welches die automatische Auswertung von Ereignissen durch Videokameras von iObserve in großem Maßstab (d.h. einer ständig erweiterbaren Infrastruktur) ermöglichen soll um ausgedehnte intelligente Überwachungssysteme zu erreichen. [34]

---

[32] http://www.cleanitproject.eu/ (11.8.2016).
https://netzpolitik.org/2012/clean-it-die-eu-kommission-will-das-internet-uberwachen-und-filtern-ganz-ohne-gesetze/ (11.8.2016).
33 https://web.archive.org/web/20150503101326/ und
http://www.kiras.at/fileadmin/dateien/allgemein/KIRAS Projekte-2009-06-NEU_1.pdf (30.07.2015).
34 https://web.archive.org/web/20150503101326/ und
http://www.kiras.at/fileadmin/dateien/allgemein/KIRAS Projekte-2009-06-NEU_1.pdf(30.07.2015).

1.3.2.5 Projekt DIANA

Das Projekt DIANA (**DI**gitale **A**utomatisierte **N**achrichten**A**nalyse) war ein Forschungsprojekt im österreichischen Sicherheitsforschungsförderprogramm KIRAS. Gegenstand des Projekts war die Entwicklung des Prototypen eines Systems zur (teil-)automatisierten Sammlung und Analyse von Informationen aus öffentlichen Quellen, auch als Open Source Intelligence (OSINT) bezeichnet.[35] Das System soll die Inhalte öffentlich zugänglicher Websites, insbesondere großer nationaler und internationaler Nachrichtenseiten, selbständig abgreifen, speichern, klassifizieren, analysieren und aufbereiten, sodass am Ende nach vorher definierten Kriterien als relevant eingestufte Informationen zur weiteren Analyse an Experten übergeben werden. Der bisher manuell durchgeführte Schritt des Suchens nach aktuellen relevanten Meldungen, z.B. über internationale Krisen und Kriege, soll dadurch automatisiert werden, sodass sich die eingesetzten Personen auf die Analysearbeit konzentrieren können.

Von welchen Websites das System die Inhalte abgreift, wird durch Angabe von URLs durch die Benutzer festgelegt.[36] Dadurch kann das entwickelte System sehr leicht auch zu anderen als den im Projekt angegebenen Zwecken verwendet werden, und somit nicht nur zur Analyse von Nachrichtenmeldungen in den Medien, sondern auch zur Analyse von Websites verschiedenster Art, insbesondere auch von persönlichen Blogs und sozialen Medien.

1.3.2.6 Projekt DIANGO

DIANGO (Digitale Informationsvisualisierung aus automatisierter Analyse von Nachrichten, Geoinformation und multimedialen Objekten) war das Nachfolgeprojekt von DIANA und wurde ebenfalls durch das österreichische Sicherheitsforschungsförderprogramm KIRAS gefördert.[37] DIANGO baute auf den Ergebnissen von DIANA auf und sah deren Erweiterung um die automatisierte Auswertung von Bildern, die automatisierte geografische Verortung von Meldungen und die Anbindung mobiler Endgeräte vor.

Bedarfsträger von DIANA und DIANGO waren das Bundesministerium für Landesverteidigung und Sport und das Bundesministerium für Inneres. Inwieweit Ergebnisse der beiden Projekte nun in der Praxis eingesetzt werden, konnte nicht in Erfahrung gebracht werden.

---

35 http://www.kiras.at/gefoerderte-projekte/detail/?tx_ttnews%5Btt_news%5D=282&cHash=59128cf4bf40c13c6d49806072b5ac9d.
36 http://derstandard.at/2000004325700/Projekt-Diana-Bundesheer-testet-Internet-Beobachtungssystem (11.08.2015).
37 http://www.kiras.at/gefoerderte-projekte/detail/?tx_ttnews%5Btt_news%5D=325&cHash=bf752b02238ba0209a343753cdb2a5f6 (11.08.2015).

1.4 Projektgegenstand: Der Handlungskatalog und die Evaluation

1.4.1 Was leistet HEAT?

HEAT liefert mit dem Handbuch einerseits die Methodik und das Gerüst für eine „Überwachungs-Gesamtrechnung“ in Österreich. Zusammenhänge werden aufbereitet und es wird gezeigt, warum eine isolierte Betrachtung einzelner Maßnahmen kein vollständiges Bild liefert.

Zugleich wird mit HEAT bereits mit einer Gesamtevaluation begonnen und vor allem ein Gesamtbild erzeugt, mit dem sich der Gegenstand künftiger Evaluationen besser eingrenzen lässt.

HEAT liefert also gewissermaßen den Einstieg und leistet einen guten Teil der Arbeit vorweg, die im Sinne staatlicher Schutz- und Gewährleistungspflichten seitens der Bundesregierung und durchaus auch seitens des Parlaments zu leisten wäre. Dabei ist natürlich einzuschränken, dass mit HEAT die Arbeit soweit begonnen wurde, als es die Kapazitäten im Rahmen eines privaten Projekts mit verhältnismäßig bescheidenen Fördermitteln und sehr viel ehrenamtlicher Arbeit zuließen. Außerdem können die Autoren von HEAT in Bezug auf den praktischen Einsatz der verschiedenen Instrumente nicht den Wissensstand haben, den die Bundesregierung hat – oder zumindest haben sollte, denn wie die parlamentarischen Anfragebeantwortungen zeigen, dürften hier erhebliche Informationsdefizite bestehen.

Als Conclusio zu dieser ersten Evaluationsarbeit werden Kriterien präsentiert, die für eine Evaluation sowohl im Sinne der Gesamtrechnung als auch für Bereichsevaluationen (z.B.: bei neuen Gesetzesvorhaben wie der StPO-Novelle, mit der der sog. „Bundestrojaner“ eingeführt werden soll) herangezogen werden sollen.

Hierzu werden Beispiele geboten, wie mit relativ einfachen Methoden durch tabellarische Darstellungen und den Einsatz von Mindmaps verschiedene Dimensionen und Zusammenhänge sichtbar gemacht werden können.

Den Abschluss bilden Anregungen – wiederum auch in Form von Mindmaps – wie durch eine prozess- und zielorientierte Vorgehensweise entsprechende Evaluationsarbeit optimiert werden könnte.

1.4.2 Was ist der Anspruch von HEAT?

Die Anregungen in der Conclusio von HEAT richten sich primär an die Bundesregierung und betonen die Dringlichkeit einer umfassenden Gesamtevaluation im Sinne der Überwachungs-Gesamtrechnung. Dazu dient eine Art Handlungsanleitung, die sich auf das bezieht, was HEAT bereits leistet und anführt, wie der Staat weiter verfahren sollte und vor allem welche Bereiche dringend einer Evaluation bedürfen.

Weiters möchte HEAT dazu anregen, bei einzelnen Gesetzesvorhaben die Wirkungsorientierte Folgenabschätzung (WFA) ernst zu nehmen und (neben den üblichen Budgetauswirkungen) auch die grundrechtlichen und gesellschaftspolitischen Folgen von Gesetzesvorhaben abzuschätzen. Der in HEAT entwickelte Kriterienkatalog sowie die Checklisten sollen hierfür eine Hilfestellung bieten.

Das Handbuch soll zudem zeigen, dass in vielen Bereichen überhaupt erst die Voraussetzungen für eine spätere (ernstzunehmende) Evaluation geschaffen werden müssen, weil entweder gar kein Datenmaterial vorhanden ist oder dieses keine hinreichende Differenzierung aufweist, um den wesentlichen Fragestellungen zu begegnen.

Schließlich ist hervorzuheben, dass dieses Handbuch ganz bewusst nicht nur politische bzw. staatliche Akteure adressiert, sondern vor allem auch der interessierten Zivilgesellschaft ein Instrument in die Hand geben will, mit dem ihre Mündigkeit in einem öffentlichen politischen Diskurs zu diesen höchst komplexen Themen gestärkt wird. Juristische und technische Zusammenhänge, die typischerweise nur für relativ wenige Experten erschließbar sind, sollen in einer möglichst leicht verständlichen Weise transportiert und durch moderne Methoden in ihrer Komplexität etwas reduziert werden. Im besten Fall wird damit gefördert, dass es zu den hier gegenständlichen Fragen – die uns alle betreffen – mehr und breiteren öffentlichen Diskurs gibt.

2 Methoden und Disziplinen

2.1 Methode des Handbuchs

HEAT orientiert sich sowohl inhaltlich als auch im Aufbau, insbesondere im Rahmen der Handlungsempfehlungen und des Kriterienkatalogs, an folgenden Referenzen:

- Europäische Kommission, Leitlinien zur Folgenabschätzung 2009
- Bundeskanzleramt, Österreichisches Handbuch „Bessere Rechtsetzung" 2008
- Policy Brief aus dem EU FP7 Forschungs-Projekt RESPECT unter der Leitung des UN-Sonderberichterstatters zu Privatsphäre und Überwachung, Professor Joseph Cannataci

Die beiden erstgenannten Dokumente sind bereits bestehende Leitlinien zur Folgenabschätzung im Rahmen legistischer Vorhaben. Mit HEAT soll zum Thema Evaluation nicht „das Rad neu erfunden" werden. Es erscheint vielmehr sinnvoll, am bestehenden Rahmen anzusetzen und diesen auf die spezifischen Themenfelder der Anti-Terror Maßnahmen und der staatlichen Überwachung anzuwenden. Das dritte Dokument ist ein Teil der Conclusio des Forschungsprojekts RESPECT[38] im 7. Forschungs-Rahmenprogramm der EU, das zum Thema Überwachungssysteme und Verbrechensbekämpfung eine pan-europäische Bestandsaufnahme mit umfassenden interdisziplinären Analysen bietet. Das hier referenzierte Dokument enthält die konkreten Handlungsempfehlungen an die EU Kommission und wurde vom RESPECT-Projektteam an der Universität Groningen für HEAT zur Verfügung gestellt, die Veröffentlichung wird zu einem späteren Zeitpunkt erfolgen.

Zu den juristischen Fragestellungen kommen zunächst überwiegend die klassischen Methoden der Rechtswissenschaften in Form von Gesetzes-, Judikatur- und Literaturanalysen zum Einsatz. Allerdings arbeitet auch die juristische Analyse mit einem „empirischen Teil", nämlich in Form der parlamentarischen Anfragen an die Bundesregierung, die im Rahmen des Projekts ausgearbeitet und von ausgewählten Abgeordneten zum Nationalrat in Ausübung ihrer parlamentarischen Rechte den jeweiligen Ministern gestellt wurden.

Der sozialwissenschaftliche Teil ist – soweit die Forschungsarbeit speziell für HEAT geleistet wurde – zunächst eine reine Literaturarbeit. Allerdings wird dort eine solide Aufstellung zum gegenwärtigen Stand der Forschung geboten und auf Forschungsprojekte referenziert, die ihrerseits auch sehr ausgiebige empirische Forschungsmethoden aufzubieten haben. Dazu sei ergänzt, dass der für den sozialwissenschaftlichen Teil primär verantwortliche Forscher, Dr. Reinhard Kreissl, an

[38] http://www.rug.nl/research/groningen-centre-for-law-and-governance/eu-projecten/respect?lang=en (9.9.2016).

vielen dieser Projekte vor allem auf EU Ebene in leitender Funktion und unmittelbar an der Forschung beteiligt war.

In methodischer Hinsicht soll der Mehrwert von HEAT aber darin bestehen, dass speziell im Hinblick auf den interdisziplinären Charakter methodische Wege eingeschlagen werden, die vor allem für die rechtswissenschaftliche Disziplin zumindest ungewöhnlich anmuten. Beispielsweise werden Tabellen verwendet, um die Verschränkung zwischen dem materiellen Strafrecht und den prozessualen Regeln auf mehreren Ebenen darzustellen und so z.B.: Gewichtungen und Diskrepanzen im Rechtsschutz auf einen Blick zu erkennen.

Besonders hervorzuheben ist diesbezüglich aber vor allem die Methode der „Mindmap“, die das Herzstück der Conclusio darstellt und vor allem danach trachtet, trotz aller Aufmerksamkeit für das Detail den Überblick zu wahren und die Komplexität in der Darstellung zu reduzieren.

2.1.1 Der Interdisziplinäre Ansatz: Recht – Technik – Soziologie

Die Interdisziplinarität ist ein roter Faden in diesem Handbuch, der sowohl in der Methodik als auch bei den Inhalten seine Spuren zeigt. Im Wesentlichen werden dabei folgende Arbeitsschritte gesetzt:

- **Gesetzliche Grundlagen**
  - Judikatur-Analyse und spezifischer Problemaufriss
    - Fall- und Anwendungsbeispiele aus der Praxis
    - Identifikation von gesetzlich basierten Risiken / Rechtsschutz

- **Verfügbare Technologien**
  - Liste faktisch verfügbarer Technologien mit Erläuterungen
    - Unterscheidung: Überwachung? Analyse (Data-Mining)?
  - Bezug zwischen Technologien und Rechtsgrundlagen
    - Ausdrückliche gesetzliche Regelung? Grenzen? Verfahren?
    - „Überwachungs-Treuhandschaft“: Instrument kann mehr als erlaubt?
    - Technische Absicherung rechtlicher Grenzen und Verfahren?

- **Gesellschaftliche Auswirkungen**
  - Technikfolgenabschätzung und -Evaluation
    - Insb. „chilling-Effekte“ (Meinungs- und Informationsfreiheit, Versammlungsfreiheit, Demonstrationsfreiheit, sog. „politische Grundrechte“)
  - Gesetzesfolgenabschätzung
    - Nach dem Modell der „Wirkungsorientierten Folgenabschätzung“
    - Frageschema und Rechtfertigungslast
  - Ableitung der methodischen Grundlagen zur Evaluation
    - Darstellung relevanter Projekte und Forschung
    - Empfehlungen für die Methodik zur Evaluation im Sinne einer „Überwachungs-Gesamtrechnung“

- **Kriterien und Handlungsstrategie**
  - Unterscheidung: materielle und formelle Kriterien
    - Mögliche Hilfestellung durch Anwendungen der Rechtsinformatik
  - Empfehlung konkreter überschaubarer Maßnahmen (Aktionsplan)
    - Dynamisches Verständnis (Plan-Do-Check-Act, PDCA-Zyklus)
    - Beschreibung notwendiger Grundlagen für künftige Evaluationen (z.B.: Statistiken)
    - Empfehlung für erste Bereichsevaluationen (z.B.: „Geheimnisträger“)

2.2 Wirkungsorientierte Folgenabschätzung (WFA) und Legistik

“Die **Wirkungsorientierung** als **Analyse- und Steuerungsinstrument** für die **Planung** von Maßnahmen, zur Beseitigung oder zur Verminderung **gesellschaftlicher Problemlagen** liefert systematisch Informationen über Herausforderungen, über **Handlungsmöglichkeiten sowie - alternativen** 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.“[39]

Der breite gesellschaftspolitische Ansatz der wirkungsorientierten Folgenabschätzung bei Gesetzesvorhaben, so wie er von Dr. Josef Ostermayer im Vorwort des Berichts über die WFA 2014 formuliert wurde, ist grundsätzlich richtig. In der Praxis zeigt sich jedoch, dass dieser wohlgemeinte Ansatz meist ins Leere läuft. Insbesondere bei eingriffsintensiven Gesetzesvorhaben[40] der jüngeren Vergangenheit, bspw. beim Polizeilichen Staatsschutzgesetz oder dem Begutachtungsentwurf zur StPO-Novelle, mit der die Ermittlungsmaßnahme „Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden“ (sog. „Bundestrojaner“) in Österreich 2016 eingeführt werden sollte, zeigt sich, dass die grundrechtlichen Auswirkungen dieser Gesetzesvorhaben in der WFA überhaupt nicht berücksichtigt wurden. In den genannten Fällen beziehen sich die WFAs ausschließlich auf finanzielle bzw. budgetäre Auswirkungen auf die Gesellschaft und lassen die demokratiepolitischen Auswirkungen von Beschränkungen der Freiheitsrechte für das Individuum und die Gesellschaft als Ganzes außen vor.

[39] Vorwort von Dr. Josef Ostermayer, Bundesminister für Kunst und Kultur, Verfassung und öffentlichen Dienst, Bundeskanzleramt, Bericht über die wirkungsorientierte Folgenabschätzung 2014.

[40] Unter einem sog. „eingriffsintensiven“ bzw. „eingriffsnahen“ besser „verletzungsnahen“ Gesetz versteht man ein Gesetz, das Maßnahmen vorsieht, die nicht bloß zufällig und ausnahmsweise, sondern geradezu in der Regel in (durch die Grundrechte geschützte) Rechtsgüter eingreifen, wenn also der Effekt des Gesetzes in besonderer Nähe zum Eingriff in das Grundrecht steht.

Das Handbuch zur Evaluation der Anti-Terror Gesetze in Österreich bietet im Gegensatz dazu eine eigenständige Systematik, um den gesellschaftspolitischen Herausforderungen solcher Gesetzesvorhaben gerecht zu werden. Dabei wird vor allem in der Conclusio, dem Kriterienkatalog und dem Handlungskatalog zur Evaluation, auf eine eher intuitiv zugängliche Methode gesetzt, die sich vor allem in der Verwendung von Mindmaps widerspiegelt. Diese Art der Darstellung erlaubt einen deutlich besseren Überblick als die typisch juristischen, vollkommen textbasierten Ansätze und erleichtert zudem die Darstellung von Zusammenhängen verschiedener Ebenen. Dabei ist hervorzuheben, dass die Verwendung der Mindmaps insbesondere in der online-Nutzung ihr volles Potential entfalten, weil dort möglich ist, Ebenen ein- und auszublenden und Sub-Ebenen heraus zu zoomen. Dennoch werden die Inhalte der Mindmaps am Ende in strukturierter Textform präsentiert, für alle Leserinnen und Leser, die diese Form der Darstellung präferieren, aus welchen Gründen auch immer.

Das Anliegen von HEAT ist vor allem, den wichtigen und grundsätzlich richtigen Ansatz der WFA aufzugreifen und vor allem durch moderne Präsentationsformen in der Praxis einer eher vollständigen und weniger selektiven, umfassenden Folgenabschätzung zuzuführen.

3 Überwachung aus sozialwissenschaftlicher Perspektive

3.1 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 Feinden 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 und Überwachten, um die sozialen Folgen

und Funktionen von Überwachung. Methodisch analysiert die Sozialwissenschaft empirisch nachweisbare 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.

3.2 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.[41] Eindeutige Konzeptualisierungsversuche scheitern auch daran , dass dem Konzept „Überwachung" – wie David Lyon (2007) feststellt – eine gewisse Ambiguität inhärent ist.[42] 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, Nachbarn „überwachen" einander 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[43], 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 lokaler sozialer 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 Akteure von Angesicht zu Angesicht gegenübertreten. In solchen Lebenswelten, im Dorf, der Familie, der Gemeinde, stellen 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 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 möglicherweise gefährdete Ordnung wiederherzustellen.

---

[41] Vgl. Kreissl, R. et al. (2015): Surveillance. Preventing and detecting crime and terrorism. in: Wright, D.; Kreissl, R. (ed.): Surveillance in Europe., Routledge: London, New York, S. 155.
[42] Vgl. Lyon, D. (2007): Surveillance Studies: An overview., Polity Press: Cambridge, S. 14.
[43] Vgl. Kreissl, R. et al. 2015, S. 155.

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 Stadtbewohners und Staatsbürgers stellt sich anders her, als die des Dorfbewohners. Der eine wird durch seine Nachbarn identifiziert, der andere durch Dokumente und Merkmale, die ihm 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 jeden Bürger über personenbezogene und die Person definierende Informationen verfügt.

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 ein jeder mehr oder weniger leben kann, wie er oder sie will und dass es genügt sich mit den entsprechenden Artefakten auszuweisen, wenn man es mit staatlichen Behörden zu tun hat. Darüber hinaus ist die Privatsphäre der Bürger 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.

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 hier 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, vermeintliche Notwendigkeiten entdeckt werden und die Bürger in ein immer dichteres und engeres Netz der Kontrolle eingebunden werden und sich, wie David Lyon es einmal formuliert hat, in leckgeschlagene Datencontainer verwandeln, die mit jedem Schritt den sie tun, eine Datenspur hinterlassen, die gierig aufgesaugt wird – von staatlichen, wie privaten Datensammlern gleichermaßen.

Die Idee, als Bürger 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.[44] 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. 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.

3.3 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 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

[44] Arendt, H. (2003). *Was ist Politik?* Piper.

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 – 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.[45] 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.[46] 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[47] und dem Verfall dessen, was Richard Sennett als öffentliche Umgangsformen analysiert hat,[48] werden die Bürger sich sozusagen selbst zur Quelle der Unsicherheit und Gefahr. Die Zunahme entsprechender Verunsicherungen, Störungen und Verstörungen lässt sich in modernen Gesellschaften diagnostizieren.[49] 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.

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 ihre 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[50], ob die in ihrem Angesicht vorgeschlagenen Maßnahmen der erweiterten Überwachung und die Forderung nach Aufgabe wohl erworbener und rechtlich

[45] SSiehe bspw. 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), 5.
[46] Klassisch hierzu: Simmel, G. (1987). Der Fremde. Das individuelle Gesetz–Philosophische Exkurse, Suhrkamp Taschenbuch Wissenschaft, Frankfurt am Main (originally published in 1908).
[47] Siehe hierzu: Giddens, A. (2013). *The consequences of modernity*. John Wiley & Sons.
[48] Sennett, R. (1992). *The fall of public man*. WW Norton & Company.
[49] Lasch, C. (1995). Das Zeitalter des Narzißmus.
[50] Siehe etwa kritisch zum politischen Tenor der global zunehmenden Gewalt: Pinker, S. (2011). *The better angels of our nature: The decline of violence in history and its causes*. Penguin UK.

garantierter Freiheitsrechte gerechtfertigt sind. Fraglich ist zudem, ob die in der politischen Diskussion immer wieder vorgebrachte Behauptung, dass Maßnahmen zur Erhöhung der Sicherheit auf Sorgen und Ängste der Bürger reagieren. Es lässt sich anhand von empirischen Untersuchungen zeigen, dass dieses Modell der Politik als „Reaktion" nicht haltbar ist.[51] Die viel zitierten Ängste der Bürger konzentrieren sich, wenn man die Befunde entsprechender Untersuchungen heranzieht eben nicht auf die Themen Kriminalität und Terrorismus. Sicherheit wird im Alltag in Begriffen traditioneller sozialstaatlicher Sicherung verstanden. Sorgen entwickeln sich im Hinblick auf ökonomische Fragen der Sicherung des Lebens und nicht auf Angst vor Kriminalität.[52]

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 vermittelter 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.

3.4 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 westlicher Gesellschaften Opfer einer terroristisch motivierten Straftat wird, so ist die Bedrohung sehr gering[53]. 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, auf die politische Diskussion und die letztlich hervorgerufene Reaktion der staatlichen Behörden. Terrorismus zielt also auf symbolische Wirkungen.

---

[51] Beckett, K. (1999). Making crime pay: Law and order in contemporary American politics. Oxford University Press.

[52] Hier bieten die regelmäßigen Befragungen im Rahmen der European Social Survey und des Eurobarometers ausreichend Belege und Daten.

[53] Siehe dazu auch ein Interview vom 16.07.2016 mit dem Risikoforscher Ortwin Renn in der Aargauer Zeitung, abrufbar unter "Terrorangst können wir überwinden wie Flugangst".

Attacken wie die von 9/11 in New York oder die Anschläge in Paris, Brüssel oder Istanbul seit 2015 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 Terroristen förderlich war. Die einfache Formel lautet hier: je stärker die Reaktion des Staates auf terroristische Aktionen, desto erfolgreicher die Strategie der Terroristen.

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 Akteure.

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 vermehrter 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.“[54] Damit ist gleichzeitig auch auf eine paradigmatische Trendwende moderner Sicherheits- beziehungsweise Überwachungspraktiken hingewiesen, die in der Literatur oftmals als „preventive turn“[55] bezeichnet wird. Demnach verfolgen moderne Überwachungspraktiken zunehmend den Anspruch, Gefahrenquellen frühzeitig zu identifizieren und somit präventiv (oder gar präemptiv) einzugreifen, womit weitgehend soziale Folgekosten verbunden sind. Wie Gandy in diesem Zusammenhang feststellt, zielt Überwachung nicht mehr auf die „production of an accurate impression or representation of the present or the recent past“ ab, sondern begreift sich vielmehr als „strategic representation of the future.“

[54] Hegemann, H.; Kahl, M. (2016): Konstruktionen und Vorstellungen von Wirklichkeit in der Antiterror-Politik: Eine kritische Betrachtung In: Fischer, S.; Masala, C. (Hg.): Innere Sicherheit nach 9/11. Sicherheitsbedrohungen und (immer) neue Sicherheitsmaßnahmen? Springer: Wiesbaden: S. 110.

[55] Gandy, O. H. (2012). a. Statistical surveillance. Remote sensing in the digital age. In: Ball, K. et al. (eds.): Routledge Handbook of Surveillance Studies. Routledge: London, New York, p. 128.

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 Sprengstoff, den er in seiner Schuhsohle an Bord geschmuggelt hatte, ein Flugzeug zum Absturz zu bringen, wurden die Schuhe der Flugpassagiere in die Kontrolle beim Check-In einbezogen.

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. Parallel dazu werden für alle diese Maßnahmen kontinuierlich die entsprechenden neuen rechtlichen Grundlagen angepasst oder neu geschaffen.

Eine rationale Strategie im Bereich der Politik der Inneren Sicherheit hätte eine Reihe von Mindeststandards zu erfüllen. So wären entsprechende Maßnahmen auf ihre Wirksamkeit im Rahmen unabhängiger Evaluationen zu überprüfen. Im Hinblick auf die rechtlichen Grundlagen wären dementsprechend verbindliche zeitliche Begrenzungen vorzusehen und sog. „sunset clauses" einzuführen. Stellt sich nach einer begrenzten Zeit heraus, dass für eine Maßnahme die gewünschten Erfolge nicht nachweisbar sind (bzw. dass problematische Nebenwirkungen überwiegen) so ist die Maßnahme auszusetzen oder aufzuheben.

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 – kurz gesagt: eine an erkennbaren Kriterien der Rationalität orientierte Politik könnte sich bei der Reaktion auf den Terrorismus eines anderen Ansatzes bedienen.[56] Gleichzeitig lässt sich zeigen, dass die im Namen der Terrorismusbekämpfung zunehmend

[56] Aktuelle Befunde zur mangelnden Wirksamkeit des Kampfs gegen den Terrorismus finden sich bei Mueller, J. E., & Stewart, M. G. (2015). *Chasing ghosts: The policing of terrorism*. Oxford University Press.

ausgebaute Überwachung das Wachstum eines sicherheitspolitisch-industriellen Komplexes befördert.[57]

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, bzw. ist in diese eingebettet, die den konstitutiven Grundideen moderner rechtstaatlich verfasster Demokratien entgegenstehen.

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.

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.

Eine andere Interpretation sieht als wesentlichen Treiber dieser Politik die interne Dynamik des politischen Prozesses. Politisch verantwortliche Akteure 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[58], die sich der Loyalität der Bürger nur mehr über das Versprechen, Böses abzuwenden, versichern kann. In Zeiten der seit langem schwelenden fiskalischen Krise und enger werdender staatlicher Handlungsspielräume[59] greift dieses Politikmodell immer weiter um sich und fördert damit den Ausbau des staatlichen Überwachungsregimes.

[57] Hayes, B., Rowlands, M., & Buxton, N. (2009). *Neoconopticon: The EU security-industrial complex* (p. 5). Transnational institute.
[58] Furedi, F. (2005). *Politics of fear*. A&C Black.
[59] O'connor, J. (1979). *The fiscal crisis of the state*. Transaction Publishers.

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.[60] 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 leistet einer Entwicklung Vorschub, die in der Literatur als „chilling effect" analysiert worden ist.[61] Die Unbekümmertheit, die es den Bürgern 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.

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 Bürgern, 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, wiewohl das reale und das gefühlte Risiko hier – noch – immer so weit auseinanderliegen wie bei den Anschlägen, die zu verhindern diese Politik der Überwachung vorgibt.

[60] Albrecht, P. A. (2007). Das nach-präventive Strafrecht: Abschied vom Recht. Institut für Kriminalwissenschaften Frankfurt aM (ed.) Jenseits des rechtsstaatlichen Strafrechts. Frankfurt aM: Lang, 3-26.

[61] Siehe als Fallbeispiel die Arbeit von 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*, *7*, 375.

4 Überwachungsmaßnahmen und Technologien

4.1 Online Überwachung

4.1.1 Internet-Backbone Überwachung

Als Internet Backbone kann man große verkehrsintensive Datenrouten bezeichnen, mit denen Computernetzwerke und Hochgeschwindigkeits-Router im Internet verbunden sind. [62]

Parlamentarische Anfragen 4085J/4088J/4089J *) Haben die österreichischen Behörden Zugriff auf die Internet Backbones und Datencenter wie den Vienna Internet Exchange (VIX) und Interxion (VIE1)? Wenn ja, von welcher Art ist dieser Zugriff? *) Haben österreichischen Behörden direkten Zugriff auf den Verkehr durch die Rechenzentren von Telekommunikationsunternehmen wie A1, UPC, Hutchinson 3, T-Mobile oder Tele2? Wenn ja, von welcher Art ist dieser Zugriff? Gibt es Equipment der Behörden in den Netzen oder Datencentern dieser Firmen? *) Gibt es im BMLVS Bestrebungen, Zugriffsermächtigungen für die Dienste des Bundesheers auf die Glasfaser-Backbones von österreichischen Kommunikationsnetzen zu erhalten beziehungsweise auszuweiten?

Parlamentarische Beantwortung – IST-Stand Österreich
Antwort 4085J: Nein
Antwort 4088J: Stützte sich auf die Amtsverschwiegenheit
Antwort 4089J: Das Bundesministerium für Verkehr, Innovation und Technologie verfügt über keine Kompetenzen, die einen Zugriff oder eine Überwachung rechtfertigen würden. Es verfügt daher auch über keine Informationen zu diesen Fragen.

4.1.2 Foren und Social-Media Überwachung

Parlamentarische Anfragen 4085J/4088J *) Gibt es im BMI neue Überlegungen, von den Internetprovidern wie schon 2008 eine "österreichische Branchenlösung" zur Internetüberwachung zu verlangen? *) Gibt es im BMI Pläne, eigene Geräte in den Räumlichkeiten von Internetprovidern zu installieren, um den Aufbau einer verschlüsselten Verbdingung mit einem sozialen Netz brechen bzw. verhindern zu können? *) Welche Software kommt für den Zweck Open Source Intelligence (OSINT) zum Einsatz? *) Welche Software kommt für den Zweck von Profiling zum Einsatz? *) Welche Software wird zur Beobachtung von Nutzern und/oder nutzergenerierten Inhalten im Internet eingesetzt?

[62] https://en.wikipedia.org/wiki/Internet_backbone (23.07.2015)

*) Welche Software wird zur Identifikation speziell von Gefahrenpotentialen in social-media Plattformen eingesetzt?
*) Welche Software kommt zur Beobachtung von online Foren und sozialen Medien zum Einsatz?
*) Mit welchen social-media-, PR- oder Beratungsagenturen bestehen Geschäftsbeziehungen und welche Aufgabengebiete umfassen diese Geschäftsbeziehungen?
*) Mit welchen Sicherheitsfirmen, Beratungsagenturen und Dienstleistern im Bereich Netzwerk- und Kommunikationsüberwachung bestehen Geschäftsbeziehungen und welche Aufgabengebiete umfassen diese Geschäftsbeziehungen?
*) Mit welchen Mitteln in welcher Höhe wurden die Projekte DIANA/DIANGO bereits gefördert und welche weiteren Ausgaben sind geplant? Inwiefern werden die Systeme von den Behörden eingesetzt?

Parlamentarische Beantwortung – IST-Stand Österreich
Antwort 4085J: Diesbezüglich wird keine spezielle Software eingesetzt (OSINT). Die Systeme DIANA/DIANGO werden noch nicht eingesetzt. Das Bundesministerium für Inneres wirkt an den Projekten DIANA/DIANGO im Sinne einer Einbindung als öffentlicher Bedarfsträger mit. Es bestehen keine Finanzierungspflichten im Hinblick auf die Kosten des Projektes. Im Bereich der Landespolizeidirektionen wurden im Zusammenhang mit der berufsbegleitenden Fortbildung, insbesondere der Problematik der Sozialen Netzwerke (z.B. Cybermobbing, etc.), durch die Agentur „CO-MEDIA“ besondere Schulungen durchgeführt. Es bestehen keine solchen Geschäftsbeziehungen (Social Media, PR, Beratungsagenturen).

Antwort 4088J: Stützte sich auf die Amtsverschwiegenheit

4.1.3 Besucherauswertung von Behördenwebseiten

Parlamentarische Anfragen 4085J/4088J
*) Welche Daten über Besuche von Behördenwebseiten werden erfasst, und in welcher Form werden sie ausgewertet?
*) In welcher Form und für wie lange werden solche Daten und Auswertungen gespeichert; unter welchen Umständen werden sie mit Dritten geteilt?
*) Werden die Auswertungen über die Besucher von Behördenwebseiten für Zwecke der Strafverfolgung verwendet?

Parlamentarische Beantwortung – IST-Stand Österreich
Antwort 4085J: Auf dem Webserver werden Daten im üblichen Ausmaß zur statistischen Auswertung und Verbesserung des Webangebots erfasst. Diese Daten werden maximal zwei Monate gespeichert und anschließend automatisiert gelöscht. Auswertungen bleiben erhalten. Protokolldaten werden nur im Falle einer gerichtlich

strafbaren Handlung gegen das Bundesministerium für Inneres bei Vorliegen eines gerichtlichen Auftrages den Ermittlungsbehörden übergeben.
Antwort 4088J: Stützte sich auf die Amtsverschwiegenheit

4.1.4 Bundestrojaner („Quellen-TKÜ“)

Im März 2016 hat das Bundesministerium für Justiz einen Gesetzesentwurf zur „Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden“ (sog. Quellen-Telekommunikationsüberwachung) vorgelegt, der aufgrund der massiven Kritik im parlamentarischen Begutachtungsverfahren seitens der Zivilgesellschaft, der Wissenschaft aber auch staatlicher Stellen (z.B. der österreichischen Datenschutzbehörde, des österreichischen Datenschutzrats oder des Verfassungsdienstes des Bundeskanzleramts) nun einer Überarbeitung unterzogen wird. Mit einem neuen Entwurf ist nach Ansicht der Verfasser dieses Papiers frühestens im Herbst 2016 zu rechnen.

Im Zusammenhang mit geheimer Überwachung und elektronischer (Kommunikations-) Datenverarbeitung hat der Verfassungsgerichtshof im Erkenntnis zur Vorratsdatenspeicherung[63] auf den Punkt gebracht, worum es geht: ***„Der Einzelne und seine freie Persönlichkeitsentfaltung sind nicht nur auf die öffentliche, sondern auch auf die vertrauliche Kommunikation in der Gemeinschaft angewiesen; die Freiheit als Anspruch des Individuums und als Zustand einer Gesellschaft wird bestimmt von der Qualität der Informationsbeziehungen (vgl. Berka, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT, 2012, Band I/1, 22).“***

In den Materialien[64] zum Ministerialentwurf wird auf den Schlussbericht[65] der Arbeitsgruppe "Online-Durchsuchung" vom März 2008 Bezug genommen, in dem die Verfasser zum Ergebnis kommen, dass der Einsatz von Programmen, die unbemerkt auf einem Computer installiert werden und es ermöglichen, den Inhalt gespeicherter Daten auszulesen, den E-Mail-Verkehr zu überwachen oder das Aufsuchen bestimmter Internetseiten zu ermitteln, ohne dass es der Inhaber bemerkt, nach geltendem Recht nicht zulässig ist. Die nun geplante Einführung einer neuen Ermittlungsmaßnahme, nämlich die "Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden" (sog **“Quellen-Telekommunikationsüberwachung“**) durch eine spezielle Überwachungssoftware stellt nach Ansicht des BMJ keine heimliche Durchsuchung des elektronischen Geräts des Betroffenen dar, da die Ermittlung von sonst auf dem Computersystem gespeicherten Daten nicht Gegenstand dieses Gesetzesvorschlages ist. Dem ist entgegenzuhalten, dass die Installation, der Betrieb und das Verstecken einer Überwachungssoftware solche Zugriffsrechte auf dem Zielsystem

[63] VfGH 27.06.2014, G47/2012.
[64] 192/ME XXV. GP Erläuterungen S 1.
[65] BMJ/BMI Interministerielle Arbeitsgruppe „Online-Durchsuchung“ Bericht, Endfassung vom 09.04.2008.

benötigt, welche dem Trojaner jede beliebige Funktionalität erlauben inklusive des Durchsuchens, Manipulierens und Erstellens von Dateien. Im vorliegenden Entwurf ausdrücklich genannt und erlaubt wird der Zugriff auf gespeicherte Inhalte wie Adressbücher und Kontaktverzeichnisse (z.B.: Outlook, Skype, WhatsApp). Auch wenn das BMJ unter einer solchen Durchsuchung eines Computersystems nach Spuren zur Identifizierung einer Person oder sonstiger Dateien keine "Online-Durchsuchung" verstehen will, ist aus technischer Sicht eine Trennung von "Online-Überwachung" und "Online-Durchsuchung" nicht möglich.

An dieser Stelle wird ein weiteres schwerwiegendes Problem der vereinfachten Herangehensweise des Gesetzgebers deutlich: Technisch kann eine Überwachungssoftware niemals nur Kommunikationsinhalte überwachen, sondern muss, um dem Ziel des Gesetzgebers gerecht zu werden, nämlich den gedanklichen Inhalt übermittelter Kommunikation zu erfassen, immer in der Lage sein, auch sonstige Vorgänge auf dem Zielsystem zu beobachten. Dies ist der einfachen Tatsache geschuldet, dass eine Verschlüsselung dieser Inhalte zu einem beliebigen Zeitpunkt vor der eigentlichen Übermittlung stattfinden kann, der Vorgang der Übermittlung selbst also keinen zweckgemäßen Anknüpfungspunkt für die Datenermittlung darstellt. Auch ohne die entsprechende Absicht des Gesetzgebers kann daher aufgrund der technischen Gegebenheiten die staatliche Überwachung auch bereits formulierte aber noch nicht kommunizierte bzw. übermittelte Gedanken erfassen.

Zahlreiche Missbrauchsfälle in Deutschland[66] und ein Urteil[67] des deutschen Bundesverfassungsgerichts machen deutlich, dass es sich bei der Online-Durchsuchung bzw. -Überwachung um eine höchst riskante und mit schwerwiegenden Eingriffen verbundene Ermittlungsmaßnahme handelt. Mit Hilfe der Installation einer Software auf dem elektronischen Gerät des Betroffenen kann dieser überwacht werden, ohne davon Kenntnis zu erlangen. Dies erscheint im Lichte der im Regelfall offenen Ermittlungen der StPO bedenklich. Der ursprüngliche Geist der StPO von 1873 war vom Grundgedanken einer "offenen" Strafverfolgung geprägt, da man damals gerade den in den Metternichschen Polizeistaat eingebetteten und dem Betroffenen und der Öffentlichkeit gegenüber geheimen Inquisitionsprozess überwunden hatte.[68] Weitere Kritikpunkte sind die diversen Möglichkeiten der betroffenen Zielgruppen, sich vor diesen Maßnahmen zu schützen und die Tatsache, dass die Überwachungssoftware eine Schadsoftware ist, welche von einem Anti-Virus-Programm bei (der sehr wahrscheinlichen) Erkennung

[66] Siehe http://www.berliner-zeitung.de/archiv/bka-reform---das-bundeskriminalamt-soll-per-gesetz-mehr-befugnisse-bei-der-terrorabwehr-bekommen--neue-fahndungsmethoden-sollen-die-jagd-auf-staatsfeinde-erleichtern--beamter-unter-verdacht,10810590,10501420.html (07.05.2016)
und
http://www.spiegel.de/netzwelt/netzpolitik/0,1518,807820,00.html.(21.05.2016)

[67] BVerfG 27.02.2008, 1BvR 370/07.

[68] *Schmoller*, Geändertes Erscheinungsbild staatlicher Verbrechensbekämpfung?, ÖJZ 1996, 21.

blockiert wird. Zudem kann der Betroffene die Software bei Erkennen manipulieren oder z.B.: bewusst falsche Beweise platzieren, um die Ermittler auf eine falsche Fährte zu locken und das tatsächliche Vorhaben parallel in Ruhe ausführen zu können. In so einem Fall wäre der Einsatz der Überwachungssoftware selbst ein erhebliches Risiko für die öffentliche Sicherheit.

Im Ergebnis handelt es sich sowohl bei der Online-Durchsuchung als auch bei der Online-Überwachung um einen intensiven Eingriff in die Grundrechte der Betroffenen. Solche Eingriffe sind nur zulässig, wenn sie dem Grundsatz der Verhältnismäßigkeit entsprechen. Der Verhältnismäßigkeitsgrundsatz verlangt, dass Ermittlungsmaßnahmen und deren gesetzliche Grundlangen durch öffentliche Interessen legitimiert sind. „*Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.*“[69]

In den Erläuternden Bemerkungen zum Ministerialentwurf wird die stetige Gefahr des Terrors hervorgehoben. Die neuartige Ermittlungsmaßnahme soll vor allem dem Zweck dienen, Menschen, welche in den Nahen Osten reisen wollen, zu überwachen, da sich diese möglicherweise in Terrorcamps zu potentiellen Terroristen ausbilden lassen könnten.[70] Es stellt sich somit die Frage, ob eine geplante Reise in bestimmte Gebiete bereits als konkreter Verdacht für die Ausbildung für terroristische Zwecke (§ 278e Abs 2 StGB) oder die Beteiligung an einer terroristischen Vereinigung (§ 278b Abs 2 StGB) gewertet wird und somit die Grundlage für den Einsatz der Überwachungssoftware darstellt. Das Problem einer solchen "Stöberfahndung" ist, dass der Anwendungsbereich für die Ermittlungsmaßnahme sehr weit wird und der Einsatz überhaupt erst zur Schaffung von Verdachtslagen führen kann (dies würde jedoch dem Wortlaut des Gesetzestextes widersprechen). Die jüngere Vergangenheit in Österreich hat gezeigt, dass die bestehenden Anti-Terrorbestimmungen sehr oft angewendet wurden[71], um die Voraussetzungen für Ermittlungsmethoden zu schaffen, die sonst nicht angewendet werden dürften, weil die Strafdrohung der möglichen Grunddelikte ohne

[69] BVerfG 27.02.2008, 1BvR 370/07.
[70] 192/ME XXV. GP Erläuterungen S. 3.
[71] z.B.: Tierschützerprozess in Wr. Neustadt; Uni Brennt AktivistInnen; Anti-Akademikerball-DemonstrantInnen.

Terrorismuszusammenhang oft nicht die notwendigen Schwellen überschreitet. Der Verhältnismäßigkeitsgrundsatz wird dadurch zusehends in Frage gestellt.
Insgesamt bestehen aufgrund des Entwurfs erhebliche Bedenken hinsichtlich der Geeignetheit, der Erforderlichkeit und der Verhältnismäßigkeit im engeren Sinn der geplanten Ermittlungsmaßnahme, die diese zusammengenommen als unverhältnismäßig erscheinen lassen.

4.2 Automatisierter Datenabgleich („Rasterfahndung“)

Logisch definieren lässt sich die Rasterfahndung als Schnittmengenbildung nach Merkmalen von Daten aus verschiedenen Quellen. Typischerweise besteht dabei Vollzugriff auf die jeweiligen Datenbanken und daraus wird dann – vereinfacht gesagt – die Schnittmenge gebildet. Technisch gesehen wäre es möglich, diese „Schnittmengenbildung“ über mehrere Datenbanken hinweg mit einer eigenen Software zu bewerkstelligen, die selbst gar kein Teil der jeweiligen Datenanwendung ist, sondern nur über Schnittstellen auf diese zugreift. Die Ermittler könnten die daraus gewonnenen Informationen sehen, ohne dass dafür ein neuer Eintrag in den jeweils verglichenen Datenbanken entsteht. Auch die Zugriffsprotokollierung würde in diesem Fall nur einen Zugriff auf die einzelnen Werte, die aus der jeweiligen Datenbank verwendet wurden, offenlegen; der Umstand der Informationsgewinnung durch „Data-Mining“[72] wäre jedoch nicht erkennbar.

Die Ermittlung und Weiterverarbeitung „*durch Zugriff etwa auf im Internet öffentlich zugängliche Daten*“ kann nun durch Menschen erfolgen, die systematisch „das Internet“ nach bestimmten Schlagworten durchsuchen. Vorstellbar ist etwa, dass Beamte mit frei verfügbaren Diensten wie Google und Facebook ihre online-Recherchen ausführen. An dieser Stelle sei angemerkt, dass die öffentliche Debatte in den 1990er-Jahren zur Einführung der „Rasterfahndung“ schon große Kritik seitens der Zivilgesellschaft hervorbrachte – weshalb die Maßnahme zunächst auch nur befristet eingeführt wurde – obwohl die Möglichkeiten einer heutigen einfachen „Google-Suche“ damals kaum vorstellbar waren. Die ersten Suchmaschinen damals[73] waren außerdem nicht nur viel weniger komplex, auch die Größenordnung der verfügbaren Datenmenge war um Dimensionen kleiner. Aus damaliger Sicht wurden die – vereinzelt schon damals antizipierten – heutigen Möglichkeiten für eine „elektronische Rasterfahndung“ gewissermaßen als „Science Fiction“-Argumente gar nicht ernsthaft in die Debatte einbezogen. Eingedenk der Tatsache, dass man heute ohne technische Kenntnisse auch z.B.: über Facebook Gesichtserkennungsdienste zur Verfügung hat, um mit einem

[72] Data-Mining hat die Aufbereitung von Daten in Verfahren, die selbständig Annahmen generieren (maschinelles Lernen), diese prüfen und dem Anwender relevante Ergebnisse in verständlicher Form präsentieren, zum Ziel. Berücksichtigt werden auch Lösungsansätze aus dem Bereich der Künstlichen Intelligenz sowie herkömmliche statistische Verfahren.
[73] ZB auch der damals verbreitetste Dienst, gewissermaßen als Pionier, die Suchmaschine „Altavista“.

Referenzbild zu einer Person diese im Netz wiederzufinden, käme das aus damaliger Sicht für sich bereits der Eingriffsintensität einer „Rasterfahndung“ gleich.
Nun ist aber anzunehmen, dass moderne Ermittlungstechnologien auch den österreichischen Verfassungsschützern zur Verfügung stehen. Hierzu gibt es einen großen Markt privater Anbieter für Software zum Zweck der sogenannten „Open Source Intelligence“ (OSINT). Im Prinzip handelt es sich um hochspezialisierte Suchmaschinen-tools, die speziell auf nachrichtendienstliche und/oder polizeiliche Ermittlungsfragen maßgeschneidert sind und systematisch auf der Basis bestimmter Algorithmen alle im Internet zugänglichen Daten durchsuchen, um daraus Informationen zu gewinnen. Die Funktionen der öffentlich verfügbaren Suchmaschinen und sozialen Netzwerke werden dabei regelmäßig automatisiert mitgenutzt.

Nach § 10 PStSG dürfen einerseits mit weitgehenden Befugnissen alle möglichen (auch sensible) Daten aus nicht öffentlichen Quellen ermittelt werden, selbst wenn sie dem Kommunikationsgeheimnis oder einem sonstigen Berufsgeheimnis unterliegen (vgl. § 12 PStSG), außer der Geheimnisschutz liegt innerhalb jener Grenzen, wo § 157 StPO ein Recht zur Zeugnisverweigerung garantiert. All diese Daten dürfen dann – wohl auch in Verbindung mit den „im Internet“ ermittelten Daten – gemeinsam weiterverarbeitet werden.

Es stellt sich daher die Frage, worin eigentlich die Abgrenzung zur „kleinen Rasterfahndung“ gemäß § 141 Abs. 2 StPO besteht. Dort heißt es:
„(2) Datenabgleich ist zulässig, wenn die Aufklärung eines Verbrechens (§ 17 Abs. 1 StGB) ansonsten wesentlich erschwert wäre und nur solche Daten einbezogen werden, die Gerichte, Staatsanwaltschaften und Sicherheitsbehörden für Zwecke eines bereits anhängigen Strafverfahrens oder sonst auf Grund bestehender Bundes- oder Landesgesetze ermittelt oder verarbeitet haben.“

Das Problem besteht schon dem Grunde nach darin, dass nicht exakt definiert ist, was unter einem „Datenabgleich“ zu verstehen ist. Nach der Legaldefinition des § 141 Abs. 1 StPO ist „Datenabgleich“ „der automationsunterstützte Vergleich von Daten (§ 4 Z 1 DSG 2000) einer Datenanwendung, die bestimmte, den mutmaßlichen Täter kennzeichnende oder ausschließende Merkmale enthalten, mit Daten einer anderen Datenanwendung, die solche Merkmale enthalten, um Personen festzustellen, die auf Grund dieser Merkmale als Verdächtige in Betracht kommen“.

Nach Auffassung der Autoren dieses Handbuchs ist auch eine systematische Sammlung von Daten, welche die Behörde aus allen im Internet (und sonst) verfügbaren Quellen anlegt, eine Datenanwendung im Sinne dieser Bestimmung. Es handelt sich dann zumindest um interne Datenanwendungen der Sicherheits- und/oder Strafverfolgungsbehörden, auf die sich § 141 Abs. 2 StPO bezieht.

Festzuhalten ist, dass dieses Problem nicht durch das PStSG neu entsteht, sondern schon bisher aufgrund der unpräzisen Formulierungen – sowohl in § 141 StPO als auch im bestehenden § 53 Abs. 2 SPG – latent ist. Durch die ausdrückliche Erweiterung der gesetzlichen Grundlagen auf die Verarbeitung von ***insbesondere durch Zugriff etwa auf im Internet öffentlich zugängliche Daten***, die großzügige Erweiterung sonstiger Ermittlungsbefugnisse der „Staatsschutzorgane" sowie den reduzierten Rechtsschutz werden die Abgrenzungsschwierigkeiten zur „Rasterfahndung" durch das PStSG aber deutlich potenziert.

4.3 Videoüberwachung

ANFRAGE 4090J/XXV. GP BMI
1) Auf wie vielen Demonstrationen wurden jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 Videoaufnahmen durch die Polizei oder andere Behörden erstellt?
2) Zu welchem Zweck wurden diese Videoaufnahmen verwendet?
3) Nach welcher Zeit werden die Videoaufzeichnungen gelöscht?
4) Im Rahmen wie vieler Demonstrationen wurden jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 Videoaufnahmen von privaten Unternehmen oder Personen für Ermittlungszwecke angefordert?
5) Im Rahmen welcher Demonstrationen wurden jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 Videoaufzeichnungen erstellt oder angefordert?
6) Zu wie vielen Identitätsfeststellungen kam es aufgrund der Auswertung von Videoaufzeichnungen im Rahmen von Demonstrationen jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014?
7) Findet ein Abgleich von bei Demonstrationen angefertigten Videodaten mit Video-, Telekommunikations- oder sonstigen Standortdaten vorangehender Demonstrationen statt?
8) An welchen Überwachungsstandorten kommt es zu einem automatisierten Bildabgleich von Überwachungsvideos?
9) Gibt es eine Möglichkeit zum automatisieren Bildabgleich von mobiler Videoüberwachung?
10) Welche Systeme werden für automatisierten Bildabgleich von Überwachungsvideos verwendet?
11) Sofern automatisierte Gefahrenerkennung Teil des Funktionsumfangs solcher Systeme ist, nach welchen Kriterien wird eine angenommene Gefahr bestimmt?
12) An welchen Standorten und Veranstaltungen wurde bzw. wird das System „SECRET – Search of Critical Events in Videoarchives" 1, „SECRET Search for Critical Events in Videoarchives – interactive"2 oder ein darauf aufbauendes System eingesetzt oder getestet?

BEANTWORTUNG 4090/J XXV. GP, BMI, MIKL-LEITNER
Zu den Fragen 1 und 2 sowie 4 bis 6:

Derartige Statistiken werden nicht geführt. Von einer anfragebezogenen retrospektiven manuellen Auswertung aller relevanten Einzelakte aus den Jahren von 2009 bis 2014 wird auf Grund des exorbitanten Verwaltungsaufwandes und der damit verbundenen enormen Ressourcenbindung im Hinblick auf die Grundsätze der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit des Verwaltungshandelns Abstand genommen.
Darüber hinaus dürfen die Sicherheitsbehörden auf Grundlage und im Rahmen der bestehenden Materiengesetze Videoaufnahmen herstellen sowie personenbezogene Bilddaten verwenden, die von Privaten rechtmäßig ermittelt wurden.
Zu Frage 3:
Die Löschung erfolgt nach den gesetzlichen Vorgaben.
Zu Frage 7:
Nein, ein systematischer Datenabgleich findet nicht statt.
Zu den Fragen 8 bis 12:
Im Zuständigkeitsbereich der Sicherheitsbehörden steht keine Software bzw. kein System für einen automatisierten Bildabgleich von Überwachungsvideos oder von mobiler Videoüberwachung in Verwendung.

ANFRAGE 4085J/XXV. GP BMI, MIKL-LEITNER
27) An welchen Standorten und Veranstaltungen wurde bzw. wird das System „iObserve“, „iObserve NG” oder ein darauf aufbauendes System eingesetzt oder getestet?

BEANTWORTUNG 4085J/XXV. GP BMI, MIKL-LEITNER
Zu Frage 27:
Das System „iObserve“, iObserve NG“ oder ein darauf aufbauendes System wurden bzw. werden weder eingesetzt noch getestet.

Durch die fortschreitende Entwicklung der Videotechnologie in den letzten Jahrzehnten ist die Überwachung von Orten, Gegenständen und Personen beinahe allgegenwärtig geworden. Dies geschieht einerseits im Rahmen der Hoheitsverwaltung im öffentlichen Raum aus sicherheitspolizeilichen Gründen, andererseits im privaten Bereich (einschließlich der Privatwirtschaftsverwaltung öffentlicher Auftraggeber) aus Gründen des Personen- oder Eigentumsschutzes. Durch die DSG-Novelle 2010 wurde im DSG 2000 ein eigener Abschnitt 9a eingeführt, der die Videoüberwachung (Bildaufnahmen- und Übertragungen) regelt. Ob die Legaldefinition der Videoüberwachung im § 50a DSG auch das Element eines Kontroll- oder Überwachungszwecks umfasst, ist in der Lehre umstritten. Unstrittig ist, dass personenbezogene (Bild-)Daten anfallen, wenn am Videomaterial Personen erkennbar sind (gem. § 4 Z 1 DSG genügt dafür bereits Identifizierbarkeit) und somit ein Eingriff in das Recht auf Geheimhaltung gem. § 1 Abs 1 DSG vorliegt. § 50a DSG gilt jedoch nur vorbehaltlich einer spezielleren Regelung in einem Materiengesetz, wie beispielsweise dem SPG oder dem PStSG (in denen die Videoüberwachung im Rahmen der Hoheitsverwaltung geregelt ist).

Mittlerweile gibt es sehr fortgeschrittene Video- und Audiotechnologie am Markt, die es ermöglicht, sehr genaue Audio- und Videoanalysen vorzunehmen und diverse Ereignisse zu detektieren. Bspw. ist die Detektion einfacher Ereignisse, wie Bewegungsdetektion oder Objekttracking bis hin zur Kombination solcher Ereignisse und die skalierbare Verarbeitung, Auswertung und Analyse von Videomassendaten möglich.

4.3.1 Verwendung personenbezogener Bilddaten durch die Sicherheitsbehörden (SPG)

Unter bestimmten Voraussetzungen sind die Sicherheitsbehörden ermächtigt, personenbezogene Bilddaten Dritter (z.B. von Überwachungskameras von Banken) zu verwenden (§ 53 Abs 5 SPG). Die Verwendung ist zulässig, wenn sonst die Abwehr gefährlicher Angriffe oder krimineller Verbindungen gefährdet oder erheblich erschwert ist und zudem bestimmte Tatsachen auf eine schwere Gefahr für die öffentliche Sicherheit schließen lassen (laut den Materialien meint der Gesetzgeber damit „eine besonders gewichtige, aus der Durchschnittskriminalität deutlich herausragende Gefahr“[74]. Der Dritte muss das Bildaufzeichnungsgerät auch rechtmäßig eingesetzt haben und es darf sich nur um Daten über öffentliches Verhalten handeln. Die Befugnis nach dem SPG gewährt nur eine datenschutzrechtliche Ermächtigung, Informationen einzuheben, sie räumt aber keine Rechtsmacht ein, die Bilddaten gegen den Willen des Dritten zu verwenden oder sicherzustellen. Eine Sicherstellung bzw. Beschlagnahme von Videomaterial Dritter ist nur im Rahmen der Strafverfolgung nach den §§ 110 und 115 StPO zulässig.
Datenermittlungen iSd § 53 Abs 5 SPG sind dem Rechtsschutzbeauftragten mitzuteilen (§ 91c Abs 1 SPG).

4.3.2 Ermittlung personenbezogener Daten mit Bildaufzeichnungsgeräten durch die Sicherheitsbehörden und Demonstrationsüberwachung (SPG)

Die Ermittlung personenbezogener Daten mit Bildaufzeichnungsgeräten im Dienste der allgemeinen Sicherheitspolizei ist in § 54 Abs 4 und 4a SPG geregelt. Zusammen mit den Abs 5, 6 und 7 leg cit ist diese Regelung abschließend, der Einsatz von Bildaufzeichnungsgeräten ist also nur in den in den genannten Normen geregelten Fällen zulässig. Der Einsatz dieser Geräte kann offen oder verdeckt erfolgen, wobei der verdeckte Einsatz an besondere Voraussetzungen (Abs 3 leg cit) geknüpft ist. Die heimliche Verwendung hat zur Voraussetzung, dass die Abwehr gefährlicher Angriffe oder krimineller Verbindungen ohne den heimlichen Einsatz gefährdet oder wesentlich erschwert wäre. Aufgrund des Verhältnismäßigkeitsgrundsatzes (§ 29 SPG) hat die verdeckte Aufzeichnung zu unterbleiben, solange das Ziel (öffentliches Interesse an der Verhinderung von Straftaten) auch mit offenem Einsatz erreicht werden kann. Für einen

[74] RV zu BGBl. I 158/2005.

offenen Einsatz genügt die Erkennbarkeit der Überwachung, die Maßnahme muss also nicht explizit öffentlich angekündigt werden. Eine bloße Bildübertragung ohne Aufzeichnung wird in § 54 Abs 8 SPG geregelt. Die Ermittlung personenbezogener Videodaten im Rahmen der erweiterten Gefahrenerforschung (Beobachtung einer Gruppierung bzw. Schutz vor verfassungsgefährdenden Angriffen) ist seit 01.07.2016 in § 11 Abs 1 Z 3 PStSG geregelt.
Ermittlungen personenbezogener Daten mit Bildaufzeichnungsgeräten sind dem Rechtsschutzbeauftragten mitzuteilen (§ 91c Abs 1 SPG).

Gem. § 54 Abs 5 SPG ist die öffentlich angekündigte Ermittlung personenbezogener Daten mit Bild- und Tonaufzeichnungsgeräten 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 iSd Versammlungsgesetzes 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.

Gem. § 54 Abs 6 SPG dürfen nach öffentlicher Ankündigung personenbezogene Daten mit Bild- und Tonaufzeichnungsgeräten im Dienste der 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 Rechtsschutzbeauftragten mitzuteilen und darf erst nach Ablauf der Drei-Tages-Frist (Meldung ans BMI) bzw. bei Vorliegen einer entsprechenden Äußerung des Rechtsschutzbeauftragten vorgenommen werden.

4.3.3 Body Worn Cameras (§ 13a Abs 3 SPG)

Durch die Novellierung des SPG im Zuge der Einführung des Polizeilichen Staatsschutzgesetzes wurde auch eine Rechtsgrundlage für den Einsatz von sog. „Body-Worn-Cameras“ bzw. „Körperkameras geschaffen, wobei die Regelung vorerst nur bis Ende 2019 in Kraft sein soll. Zu Zwecken der Dokumentation von Amtshandlungen, bei denen Befehls- oder Zwangsgewalt ausgeübt wird, ist der offene Einsatz von Bild- und Tonaufzeichnungsgeräten erlaubt. Vor Beginn der Aufzeichnung muss der Einsatz aber dem Betroffenen derart angekündigt werden, dass er ihm auch bekannt wird. Die solcherweise ermittelten personenbezogenen Daten dürfen nur zur Verfolgung von strafbaren Handlungen, die sich während der Amtshandlung ereignen oder zur Kontrolle der Rechtmäßigkeit letzterer verwendet bzw. ausgewertet werden. Bis zur Auswertung oder Löschung (Löschungsfrist von sechs Monaten) der Daten sind diese gem. § 14 DSG 2000 vor unberechtigter Verwendung (insb. durch Protokollierung aller Zugriffe und Verschlüsselung) zu sichern. Beim Einsatz ist besonders darauf zu achten, dass bei Eingriffen in die Privatsphäre von Betroffenen der Verhältnismäßigkeitsgrundsatz gewahrt wird.

Seit März 2016 wird der Einsatz von Body-Worn-Cameras von der Polizei in Wien, Salzburg und der Steiermark getestet, wobei der Probebetrieb vom KIRAS-Studienprojekt[75] "Evaluation & Begleitung der Einführung von Body-Worn Cameras" (EBeCa) begleitet wird[76].

4.3.4 Automatisierter Bildabgleich / Rasterfahndung (§§ 141 ff StPO)

Laut der Beantwortung auf die parlamentarische Anfrage 4085J/XXV. GP findet in Österreich ein Abgleich von Videodaten mit Video-, Telekommunikations- oder Standortdaten vorangehender Demonstrationen nicht statt. Bei der Verarbeitung von rechtmäßig ermittelten Daten ist den Sicherheitsbehörden jedenfalls gem. § 53 Abs 2 SPG ein automationsunterstützter Datenabgleich iSd § 141 StPO (sog. „Rasterfahndung“) untersagt.
Die Forschungsprojekte „iObserve“ und „iObserve NG“, die in den Kapiteln 4.1.1.3 und 1.1.4 kurz beschrieben werden, beschäftigen sich mit Videoüberwachungssystemen, die selbst erkennen können, ob Handlungen von Personen vorgenommen werden, die uU als gefährliche Angriffe qualifiziert werden, um das Einschreiten der Sicherheitsbehörden zu ermöglichen.

[75] http://www.kiras.at/gefoerderte-projekte/detail/?tx_ttnews%5Btt_news%5D=521&cHash=9d3cbe24a1938d7814bbae4ec4f3fc77.

[76] http://www.bmi.gv.at/cms/bmi/_news/bmi.aspx?id=34597234544743706D7A303D&page=0&view=1.

4.3.5 Großer Spähangriff / Bloßer Spähangriff (§§ 136 Abs 1 Z 3, 136 Abs 3 StPO)

Der große Späh- und Lauschangriff gem. § 136 Abs 1 Z 3 StPO ist an besondere Zulässigkeitsvoraussetzungen geknüpft, da keiner der Überwachten Kenntnis von der Überwachung hat. Er darf nur eingesetzt werden, wenn es um die Aufklärung oder die Verhinderung besonders schwerer Straftaten geht, ein dringender Tatverdacht besteht und die Überwachung zudem notwendig ist. Dieses Element der Notwendigkeit wurde allerdings vom Gesetzgeber gelockert, nachdem die Überwachung nicht nur zulässig ist, wenn die Aufklärung oder Verhinderung der genannten Taten ohne Überwachung aussichtslos wäre, sondern auch ansonsten wesentlich erschwert wäre. Die Überwachung ist also auch dann zulässig, wenn auch noch andere Ermittlungsmaßnahmen zur Verfügung stünden und ist somit nicht Ultima Ratio.

Die optische Überwachung (ohne Tonübertragung) außerhalb von Wohnungen ist in § 136 Abs 3 Z 1 StPO geregelt und ist für die Aufklärung jeglicher strafbaren Handlung gestattet. Voraussetzung ist jedoch, dass ein Verdacht besteht, dass jemand eine bestimmte strafbare Handlung begangen hat. Die Überwachung muss zu dem Zweck erfolgen, Gegenstände oder Örtlichkeiten zu überwachen, um das Verhalten von verdächtigen Personen zu erfassen die mit dem Gegenstand oder der Örtlichkeit in Kontakt treten. Es geht also um die Möglichkeit der Objektüberwachung in der Öffentlichkeit. Im Gegensatz dazu fehlt es zur (vorsorglichen) Überwachung irgendeines öffentlichen Verhaltens unter Verwendung von Bild- oder Tonaufzeichnungsgeräten zur Aufklärung und Ermittlung von allfälligen Straftaten (ohne Tatverdacht) an einer gesetzlichen Grundlage in der StPO.

Strengere Überwachungsvoraussetzungen sieht § 136 Abs 3 Z 2 StPO für eine optische Überwachung von vom Hausrecht geschützten Räumlichkeiten vor. Diese Form der Überwachung ist nur zur Aufklärung von strafbaren Handlungen zulässig, die vorsätzlich begangen werden und mit mehr als einjähriger Freiheitsstrafe bedroht sind. Außerdem muss die Aufklärung der Straftat ohne die optische Überwachung wesentlich erschwert sein (d.h. die Überwachung ist auch dann zulässig, wenn zwar andere Ermittlungsmaßnahmen zur Verfügung stünden, aber langwieriger oder weniger zuverlässig sein würden). Neben diesen Voraussetzungen bedarf es noch der Zustimmung des Inhabers der Räumlichkeiten (ausdrückliche Zustimmung von Beginn der Überwachungsmaßnahme an).

4.3.6 Rechtsgrundlagen Überblick

Grundsätzlich gelten für die oben beschriebenen Technologien folgende gesetzlichen Bestimmungen:

- Sicherheitspolizeigesetz (SPG)
  - Im Besonderen:
    - § 13a Abs 3 SPG – Body Worn Cameras
    - § 53 Abs 5 SPG – Verwendung personenbezogener Bilddaten Dritter
    - § 54 Abs 4 SPG – Ermittlung personenbezogener Daten mit Bild- und Tonaufzeichnungsgeräten
    - § 54 Abs 4a SPG – verdeckte Ermittlung personenbezogener Daten mit Bild- und Tonaufzeichnungsgeräten
    - § 54 Abs 5 SPG – Überwachung von Zusammenkünften zahlreicher Menschen
    - § 54 Abs 6 SPG – Überwachung öffentlicher Orte
    - § 91c SPG – Befassung des Rechtsschutzbeauftragten
- Polizeiliches Staatsschutzgesetz (PStSG)
  - Im Besonderen:
    - § 11 Abs 1 Z 3 PStSG – (verdeckte) Ermittlung personenbezogener Daten durch Einsatz von Bild- und Tonaufzeichnungsgeräten im Rahmen der erweiterten Gefahrenerforschung
- Strafprozessordnung (StPO)
  - Im Besonderen:
    - § 141 StPO – automatisierter Datenabgleich („Rasterfahndung“)
    - § 136 Abs 1 Z 3 StPO – optische und akustische Überwachung von Personen („großer Späh- und Lauschangriff“)
    - § 136 Abs 3 Z 1 und 2 StPO – optische Überwachung („bloßer Spähangriff“)
- Datenschutzgesetz 2000 (DSG 2000)
  - Im Besonderen:
    - § 14 DSG 2000 – Datensicherheitsmaßnahmen

4.4 Telekommunikation und Dienste der Informationsgesellschaft

4.4.1 Auskunftspflichten der Betreiber und Diensteanbieter im Überblick

Die Möglichkeiten, die sich anbieten, um im Zuge eines strafrechtlichen Ermittlungsverfahrens Spuren zu sichern bzw. diesen nachzugehen, sind nicht als abschließender Katalog in einem einzigen Gesetzt zusammengefasst. Vielmehr sind die verschiedenen gesetzlichen Ermächtigungen zur Speicherung, Sicherung oder Erlangung von Daten auf verschiedene Gesetze aufgeteilt, die einander ergänzen. Es ist daher unumgänglich, das Zusammenspiel all dieser Gesetze zu betrachten, möchte man die Auswirkungen einer Rechtsnorm abschätzen. Kurzum: Keiner der hier erwähnten Gesetzestexte darf nur isoliert gesehen werden.[77] Eben dieser Umstand macht die genaue Betrachtung zugleich auch sehr komplex und für den interessierten Laien intransparent.

Bisher wurden die verschiedenen prozessualen Normen nach der StPO, dem SPG und dem MBG dargestellt, die es den staatlichen Sicherheitsbehörden ermöglichen, Informationen über eine Person aufgrund einer (strafrechtlich relevanten) Verdachtslage, zu erlangen. In engem Zusammenhang mit den Auskunftspflichten von Betreibern oder Providern (nach TKG, ECG) stehen daher die §§ 76a, 134, 135 StPO oder §§ 137, 138 StPO.

Wie in Kapitel 5.2.2 im Detail beschrieben, ist der Übergang zwischen den Befugnissen nach StPO und SPG (vor allem § 53 Abs 3a und 3b SPG) relevant: Nach einem **gefährlichen Angriff** haben die Sicherheitsbehörden, unbeschadet ihrer Aufgaben nach der Strafprozessordnung die maßgebenden Umstände, einschließlich der Identität des dafür Verantwortlichen, zu klären, soweit dies **zur Vorbeugung weiterer gefährlicher Angriffe erforderlich** ist. Sobald ein bestimmter Mensch einer versuchten oder bereits begangenen strafbaren Handlung verdächtig ist, gelten ausschließlich die Bestimmungen der StPO (§ 22 Abs 3 SPG). Allein der Wortlaut zeigt, dass die Abgrenzung nicht immer leicht festzustellen ist.

Im Folgenden soll auf einen praktisch sehr wichtigen Bereich der Informationsgewinnung eingegangen werden: den Bereich der "Informations- und Kommunikationstechnologie" (IKT bzw. englisch ICT). Man denke dabei an die Vielzahl von Kommunikationswegen, die jedem Menschen mit technischen Geräten (Smartphone, Notebook, Tablet) und Zugang zum Internet zur Verfügung stehen und tagtäglich genützt werden: SMS, E-Mail, Social Media, Blogs, Foren, Telefonate, Voice over IP, Text over IP etc.

[77] Auch wenn immer wieder gerne angedeutet wird, dass unterschiedliche Gesetze nichts miteinander zu tun haben, http://derstandard.at/2000013721690/Vorratsdaten-Mikl-Leitner-fuer-Diskussion-ueber-Wiedereinfuehrung. (02.04.2015)

Beispiel: Anna hat ein brandneues Smartphone und verwendet täglich ihren Laptop. Neben SMS/MMS und Sprachtelefonie ist sie Mitglied in verschiedenen WhatsApp-Gruppen, über die sie Texte und Fotos verschickt. Auf dem Laptop ruft sie über ihr E-Mail-Programm regelmäßig Nachrichten ab und versendet welche. Zudem nützt sie mehrmals monatlich Skype, um mit ehemaligen StudienkollegInnen und FreundInnen im Ausland zu telefonieren.

4.4.1.1 Datenkategorien

Um die folgenden Zusammenhänge besser verständlich zu machen, werden zu Beginn die verschiedenen Typen von Daten definiert, deren Terminologie den (EU-)Gesetzen und Verordnungen entstammt. Wie sogleich erkennbar sein wird, sind diese Definitionen (die nach unterschiedlichen Gesichtspunkten erfolgen, z.B.: nach Art des Datums, Speicherdauer, Verwendungszweck) ebenfalls nicht streng abgrenzbar, sondern können einander überschneiden, je nachdem aus welchem Blickwinkel man sie betrachtet.

So sind z.B.: Zugangsdaten eine Unterkategorie der Verkehrsdaten und können überdies auch Betriebsdaten sein, sofern sie zu Zwecken der Verrechnung benötigt werden. Bis 30.6.2014 fielen sie zudem auch in die Kategorie der Vorratsdaten.

- **Stammdaten: Name** (Familienname und Vorname bei natürlichen Personen, Name bzw. Bezeichnung bei juristischen Personen), akademischer Grad bei natürlichen Personen, **Anschrift** (Wohnadresse bei natürlichen Personen, Sitz bzw. Rechnungsadresse bei juristischen Personen), **Teilnehmernummer** und sonstige Kontaktinformation für die Nachricht, Information über Art und Inhalt des Vertragsverhältnisses, Bonität.
- **Inhaltsdaten:** Alle Inhalte von übertragenen Nachrichten (z.B.: **Texte** einschließlich der „Betreff"-Zeile in einer E-Mail, Text einer SMS, **Bilder** in Attachments). Inhaltsdaten unterliegen dem Fernmelde- und Kommunikationsgeheimnis.
- **Verkehrsdaten:** Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden (z.B.: **dynamische IP-Adressen**, aktive und passive **Teilnehmernummer**, die Leitwege, das verwendete Protokoll und das Netz, vom dem die Nachricht ausgeht oder an das sie gesendet wird[78]).
- **IP-Adressen sind ein Sonderfall**, da deren Einordnung als Stamm- oder Verkehrsdaten nicht einheitlich von den Gerichten beantwortet wurde. Die überwiegende Ansicht ist mittlerweile in der EU, dass dynamische IP-Adressen

[78] ErwGr 15 der DatenschutzRL für elektr. Kommunikation, RL 2002/58/EG.

Verkehrsdaten, statische IP-Adressen jedoch (zugleich) Stammdaten sind. In Österreich ist dies seit 1.4.2012 ausdrücklich im TKG definiert.[79]

- **Zugangsdaten:** Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind (z.B.: **IMSI – International Mobile Subscriber Identity**, durch die die SIM-Karte – Subscriber Identity Module, eindeutig identifiziert ist, **Logfiles**, **IP-Adressen** sind nach der Legaldefinition Zugangsdaten und als solche eine Sub-Kategorie der Verkehrsdaten)
- **Standortdaten: Verkehrsdaten**, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung des jeweiligen Nutzers eines öffentlichen Kommunikationsdienstes angeben. Im Fall von festen Telekommunikationsendeinrichtungen sind Standortdaten die Adresse der Einrichtung.
- **Vorratsdaten**[80]: Verkehrs- und Standortdaten, die vom Betreiber erzeugt und verarbeitet werden und (in Österreich lediglich von 1.4.2012 bis 30.6.2014) ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach dem Ende der jeweiligen Kommunikation verdachtsunabhängig gespeichert wurden. Diese Daten waren nicht ident mit jenen, die für Verrechnungszwecke (idR drei Monate) ohnehin gespeichert wurden. Hinzu kamen weitere Daten wie z.B.: Verkehrsdaten von Festnetz- und Mobil-Anschlüssen mit Flatrates oder Prepaid-Tarifen, Telefonnummer des Anrufers bei eingehenden Anrufen, erfolglose Anrufversuche, IP-Adressen, Cell-IDs (also den Aufenthaltsort von Mobiltelefonen) und E-Mail Daten[81].
- **Betriebsdaten:** Betriebsdaten können sowohl **Verkehrs-, Zugangs-, Standort-** als auch **Stammdaten** sein, sofern diese zu Zwecken etwa der Verrechnung an Endkunden oder Vorleistungsentgelten benötigt werden. Diese sind demnach regelmäßig innerhalb der dreimonatigen Frist für Rechnungseinsprüche[82] vorhanden, unter Umständen aber auch darüber hinaus.

---

[79] Siehe dazu detailliert Tschohl, Die Anonymität im Internet – Umsetzung der Vorratsdaten-RL im österreichischen Telekom-, Strafprozess- und Sicherheitspolizeirecht, in: Jaksch-Ratajczak/Stadler, Aktuelle Rechtsfragen der Internetnutzung, Band 2, 341 ff.

[80] http://derstandard.at/1297818694702/Vorratsdaten-Beispiele-fuer-Datensammlung. (17.01.2016)).

[81] https://netzpolitik.org/2013/vorratsdatenspeicherung-eu-kommission-legt-beweise-fuer-notwendigkeit-vor-beweist-aber-die-notwendigkeit-nicht/. (30.05.2016)).

[82] Die Frist für den Rechnungseinspruch selbst beträgt 6 Wochen, von der Entstehung der Kommunikation bis zur Abwicklung der Löschung kann die Gesamtdauer aber 3 Monate betragen.

Mit der Aufhebung der Vorratsdatenspeicherung durch den VfGH[83] im Jahr 2014 wurden die Regeln über das Speichern und die Auskunft über Vorratsdaten aufgehoben. Nichtsdestotrotz ist es für Behörden aber nach wie vor möglich, innerhalb der ihnen gesetzlich zustehenden Befugnisse auf sogenannte Betriebsdaten zurückzugreifen.[84] Es ist unklar, was vom Begriff umfasst ist und wie lange diese Daten gespeichert werden. Ebenso ist öffentlich nicht bekannt, ob Kommunikationsbetreiber interne Policies im Hinblick auf die Speicherung dieser Daten haben und wenn ja, wie diese ausgestaltet sind (z.B.: was die Dauer der Speicherung betrifft).

4.4.1.2 Begrifflichkeiten aus dem TKG

§ 92 Abs 3 Z 3 TKG: **Stammdaten** = alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:

- Name (Familienname und Vorname bei natürlichen Personen, Name bzw. Bezeichnung bei juristischen Personen),
- akademischer Grad bei natürlichen Personen,
- Anschrift (Wohnadresse bei natürlichen Personen, Sitz bzw. Rechnungsadresse bei juristischen Personen),
- Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,
- Information über Art und Inhalt des Vertragsverhältnisses,
- Bonität;

§ 92 Abs 3 Z 4 TKG: **Verkehrsdaten** = Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

§ 92 Abs 3 Z 4a TKG: **Zugangsdaten** = jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind;

§ 92 Abs 3 Z 5 TKG: **Inhaltsdaten** = die Inhalte übertragener Nachrichten (Z 7);

§ 92 Abs 3 Z 6 TKG: **Standortdaten** = Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung des jeweiligen Nutzers eines öffentlichen Kommunikationsdienstes angeben, im Fall von festen Telekommunikationsendeinrichtungen sind Standortdaten die Adresse der Einrichtung;

[83] VfGH-Erkenntnis vom 27.6.2014, kundgemacht in BGBl I 44/2014/44.
[84] Siehe auch http://blog.lehofer.at/2014/06/vfghvds.html. (13.03.2016)).

Betriebsdaten

Obwohl die Vorratsdatenspeicherung aufgehoben wurde ist es für Behörden aber nach wie vor möglich, auf sogenannte Betriebsdaten zurückzugreifen.[85] Aus diesem Grund stellen sich einige wichtige Fragen:

- Was sind **Betriebsdaten** und wie lange werden sie gespeichert?
- Haben Kommunikationsbetreiber interne Policies zur Speicherung dieser Daten?
- Wenn ja, wie sind diese Policies ausgestaltet (z.B.: was die Dauer der Speicherung betrifft)?

Betriebsdaten existieren terminologisch in der **TKG-Datensicherheitsverordnung (TKG-DSVO)**:
In dieser Verordnung werden die näheren Bestimmungen des Formats, der Datenfelder und der Syntax der CSV-Datei bei der Übermittlung von Auskünften über Verkehrsdaten (§ 99 Abs. 5 TKG 2003) und Vorratsdaten (§ 102b TKG2003[86]), zur Datensicherheit und zur Protokollierung bei der Übermittlung der in Z 1 genannten Auskünfte sowie zur Datensicherheit bei der Speicherung und der Zugriffsprotokollierung von Vorratsdaten getroffen. Der Anwendungsbereich dieser Verordnung erstreckt sich auf die Verwendung von Verkehrsdaten, Zugangsdaten und Standortdaten sowie Stammdaten, soweit diese in Verbindung mit den eben genannten Datenkategorien verarbeitet werden.[87]

Demnach können Betriebsdaten sowohl Verkehrs-, Zugangs-, Standort- als auch Stammdaten sein, sofern diese zu Zwecken etwa der Verrechnung an Endkunden oder Vorleistungsentgelten benötigt werden (§ 99 Abs 2 und 3 TKG, siehe unten bei **Verkehrsdaten**). Diese sind demnach regelmäßig innerhalb der dreimonatigen Frist für Rechnungseinsprüche vorhanden, unter Umständen aber auch darüber hinaus (§ 99 Abs 2 Z 1 bis 3 TKG).

4.4.1.3 Auskunftspflichten im Telekommunikationsbereich

Die relevanten Normen zur Mitwirkungs- und Auskunftspflicht von IKT Anbietern gegenüber Sicherheits- und Strafverfolgungsbehörden finden sich in den §§ 90, 94, 99 TKG. Die Systematik des TKG sieht jedoch vor, dass jedem Auskunftsanspruch, der in der

[85] Siehe auch http://blog.lehofer.at/2014/06/vfghvds.html. (01.07.2016)).
[86] Diese Bestimmung wurde mit BGBl. I 44/2014 aufgehoben (Aufhebung der Vorratsdatenspeicherung.
[87] Vgl. http://www.bmvit.gv.at/telekommunikation/recht/aut/verordnungen/dsvo.html. (01.07.2016)).

in der Rechtsordnung an irgendeiner Stelle normiert ist (z.B.: in der StPO, im SPG), eine korrespondierende Bestimmung im TKG gegenüber stehen muss.

Genau deshalb enthält § 99 Abs. 1 TKG die Formulierung, dass Verkehrsdaten „außer in den **in diesem Gesetz** geregelten Fällen nicht gespeichert oder übermittelt werden" dürfen. Dem entsprechend enthält § 99 Abs. 5 TKG in der Folge eine abschließende Aufzählung der korrespondierenden Rechtsnormen in der StPO und im SPG sowie neuerdings auch im PStSG, die dem Anbieter eine Auskunftspflicht auferlegen. Dieser **abschließende Katalog zulässiger Fälle der Datenverwendung** wurde – im Zuge der nationalen VDS-Umsetzung – mit der TKG Novelle 2011[88] eingeführt, begleitet durch die Einführung TKG-DSVO und die Einrichtung der DLS als exklusivem Kanal zur Abwicklung der Auskünfte. Die Erläuterungen zu § 99 Abs. 1 TKG weisen ausdrücklich darauf hin, dass hier dem datenschutzrechtlichen Transparenzgebot Rechnung getragen wird. „Eine Nachschau im TKG muss dem Anbieter Rechtsklarheit bieten, welche Datenverwendungen zulässig sind."[89] Der Oberste Gerichtshof[90] hat schon 2012 unter Berufung auf diese Rechtslage solche Auskunftsansprüche abgelehnt, die in § 99 Abs. 5 nicht ausdrücklich aufgezählt sind, selbst wenn ein anderes Gesetz einen Auskunftsanspruch normiert wie z.B.: in § 87b Urheberrechtsgesetz.[91]

Nun hat der Gesetzgeber allein in den Jahren 2015 und 2016 zwei neue Rechtsgrundlagen zur Auskunftserteilung über Verkehrsdaten außerhalb der StPO oder des SPG geschaffen, dabei aber die Systematik des § 99 TKG ignoriert und dort keine entsprechende Ergänzung normiert. Der mit dem Steuerreformgesetz 2015/2016[92] neu eingeführte § 99 Abs. 3a FinStrG enthält einen Auskunftsanspruch zu Verkehrsdaten und einen Verweis auf § 99 Abs. 5 TKG, im TKG selbst wurde aber keine korrespondierende Norm geschaffen.

Weiters ist am 1.8.2016 § 48b BörseG neu in Kraft getreten[93]. Die Bestimmung gewährt der Finanzmarktaufsicht (FMA) eine Auskunft über Daten einer Nachrichtenübermittlung (§ 134 Z2 StPO einschließlich der in § 76a StPO genannten Daten, also Verkehrs-, Zugangs-, Standort- und Stammdaten), wenn der begründete Verdacht einer Zuwiderhandlung gegen § 48c BörseG (Missbrauchs von Insiderinformationen und Marktmanipulation) oder § 48d Abs. 1 Z2 BörseG (Verstoß gegen die Verpflichtungen zur Veröffentlichung von

[88] Kundgemacht am 18. Mai 2011 durch BGBl. I Nr. 27/2011.
[89] Erläuterungen zu § 99 Abs. 1 TKG, 1074 der Beilagen, XXIV. GP.
[90] OGH 6 Ob 119/11k auch mit Verweis auf die Materialien zur TKG Novelle.
[91] Vgl. dazu OGH 4 Ob 41/09x, wo der OGH schon vor der Novellierung mit guten Gründen den zivilrechtlichen Auskunftsanspruch wegen Urheberrechtsverletzungen ablehnt. Die Entscheidung 6 Ob 119/11k schließt sich dieser Entscheidung ausdrücklich an und argumentiert die neue Rechtslage.
[92] Steuerreformgesetz 2015/2016, BGBl. I Nr. 118/2015.
[93] Bundesgesetz über die Wertpapier- und allgemeinen Warenbörsen und über die Abänderung des Börsesensale-Gesetzes 1949 und der Börsegesetz-Novelle 1903 (Börsegesetz 1989 - BörseG) BGBl. I. Nr. 555/1989 idF BGBl. I Nr. 76/2016.

Insiderinformationen und daran anknüpfende Verpflichtungen) besteht. Das Landesgericht für Strafsachen Wien entscheidet als Einzelrichter mit Beschluss über einen entsprechenden Antrag der FMA. **Das Börsegesetz enthält weder einen Verweis auf das TKG noch wurde eine Anpassung im TKG selbst vorgenommen**. Anders als § 99 Abs. 3b FinStrG ist im Börsegesetz auch **keine Regelung enthalten, wonach die DLS als Kommunikationskanal für Auskünfte exklusiv vorzusehen ist**.

Problematisch im Rahmen der Auskunftspflichten der IKT-Anbieter erscheint im Hinblick auf die Rechtssicherheit, dass der konkrete Umfang der **Betriebsdaten** nicht definiert ist. Welche Daten die Betreiber zu diesen Zwecken speicherten und insbesondere wie lange sie dies taten, konnte jedenfalls bis ins Jahr 2012 - so die einhellige Antwort - verlässlich nicht einmal für einen einzelnen Betreiber einheitlich beantwortet werden. Als Begründung dafür wurden die Vielfalt an Gebührenmodellen sowie spezielle Vereinbarungen mit Vertragspartnern angeführt. Auch wenn diese Tatsache zur Folge hatte, dass die um Auskunft ersuchende Stelle im Zeitpunkt der Anfrage nicht mit Sicherheit wusste, ob die gewünschten Daten überhaupt (noch) vorhanden waren oder nicht, so ist an dieser Stelle festzuhalten, dass in der Praxis - schon alleine aufgrund der Möglichkeit von Rechnungseinsprüchen - die von den Strafverfolgungsbehörden benötigten Daten bei den Betreibern regelmäßig vorhanden waren.[94] Einen klaren normativen Anhaltspunkt, dass jeder Anbieter verpflichtend eine Policy zur Speicherung von Betriebsdaten zu führen hat, enthält die TKG-Datensicherheitsverordnung in § 5 Abs 4 TKG-DSVO. Die Datenschutzbehörde kann demnach jederzeit verlangen, dass ein Anbieter diese Policy vorlegt, das heißt umgekehrt, der Anbieter muss diese jederzeit aktuell und bereit halten. Allerdings erwächst daraus kein unmittelbarer Anspruch, eine solche „Betriebsdatenrichtlinie“ auch öffentlich zu machen. Ob und mit welchem Ergebnis die Datenschutzbehörde bislang von den Anbietern solche internen Speicherrichtlinien eingefordert und überprüft hat, ist den Autoren dieses Handbuchs nicht bekannt.

Begriffsbestimmungen nach der TKG-DSVO

§ 2. (1) **Verkehrsdaten, Zugangsdaten und Standortdaten** sowie – soweit sie in Verbindung mit den zuvor genannten Datenkategorien verarbeitet werden - **Stammdaten** werden bezeichnet als

1. „**Betriebsdaten**“, soweit diese für den Anbieter für die in § 99 Abs. 2 und 3 TKG 2003 erfassten Zwecke notwendig sind;
2. „Vorratsdaten“, soweit diese vom Anbieter ausschließlich aufgrund der Verpflichtung gemäß § 102a TKG 2003 für die in § 102b TKG 2003 genannten Zwecke vorrätig gespeichert werden (§ 92 Abs. 3 Z 6b TKG 2003).

(...)

94 *Pühringer*, Vorratsdatenspeicherung, JAP 2012/2013/10 (80).

- § 99 Abs 5 Z 1 betrifft die im Rahmen des Abs 2 gespeicherten "Billingdaten" (bzw. Betriebsdaten, vgl. § 2 Abs 1 Z 1 TKG-DSVO) und stellt sicher, dass diese im Rahmen der *Auskunft über Daten einer Nachrichtenübermittlung* gemäß § 134 Z 2 StPO an die nach der StPO zuständigen Organe bei Vorliegen der entsprechenden formellen Voraussetzungen übermittelt werden.[95]

- § 99 Abs 5 Z 2 regelt die Auskunft über Zugangsdaten, nämlich insbesondere IP-Adressen und E-Mail-Adressen (siehe § 76a Abs 2 Z 1 bis 4 StPO). Auskünfte über Name und Anschrift eines Teilnehmers, dem eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, werden aus Sicht der Ermittlungen überhaupt nur dann begehrt, wenn das Ermittlungsinteresse darin besteht, einen bereits bekannten Kommunikationsvorgang einem bestimmten Teilnehmer zuzuordnen.[96]

- § 99 Abs 5 Z 3 normiert das ausnahmsweise Abgehen vom (vor dem Außerkrafttreten der VDS in § 102b Abs 1 TKG) normierten) Grundsatz, dass Verkehrsdaten nur bei Vorliegen einer richterlichen Bewilligung beauskunftet werden dürfen.[97]

Funkzellenabfrage: VfGH sagt zulässig – Beispiel Deutschland, SMS vom Provider, wenn Individuum Teil einer Abfrage wird. → Vergleich **Rasterfahndung** (§ 141 StPO "automatisationsunterstützter Datenabgleich", wann liegt eine solche vor?)

Informationspflichten des Betreibers gegenüber den staatlichen Behörden

§ 90 TKG
(...)
(6) Anbieter von Kommunikationsdiensten sind verpflichtet, Verwaltungsbehörden auf deren schriftliches und begründetes Verlangen Auskunft über **Stammdaten** im Sinne von § 92 Abs. 3 Z 3 litte. a bis e von Teilnehmern zu geben, die in Verdacht stehen, durch eine über ein öffentliches Telekommunikationsnetz gesetzte Handlung eine Verwaltungsübertretung begangen zu haben, soweit dies ohne Verarbeitung von Verkehrsdaten möglich ist.

(7) Anbieter von Kommunikationsdiensten sind auf schriftliches Verlangen der zuständigen Gerichte, Staatsanwaltschaften oder der Kriminalpolizei (§ 76a Abs. 1 StPO)

95 Stratil (Hrsg), TKG 20034 (2013) 423 f.
96 Stratil (Hrsg), TKG 20034 (2013) 424.
97 Stratil (Hrsg), TKG 20034 (2013) 425; 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 (350).

verpflichtet, diesen zur Aufklärung und Verfolgung des konkreten Verdachts einer Straftat Auskunft über **Stammdaten** (§ 92 Abs. 3 Z 3) von Teilnehmern zu geben. Dies gilt sinngemäß für Verlangen der Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a Z 1 SPG. In dringenden Fällen können aber solche Ersuchen vorläufig mündlich übermittelt werden.

(8) Anbieter von Mobilfunknetzen haben **Aufzeichnungen über den geografischen Standort** der zum Betrieb ihres Dienstes eingesetzten Funkzellen zu führen, sodass jederzeit die richtige Zuordnung einer Standortkennung (Cell-ID) zum tatsächlichen geografischen Standort unter Angabe von Geo-Koordinaten für jeden Zeitpunkt innerhalb eines sechs Monate zurückliegenden Zeitraums gewährleistet ist.

KOMMENTAR

- Es handelt sich um eine **bloß deklarative Liste** an Informationspflichten für die TK-Unternehmer. Davon bleiben all jene Informationsverpflichtungen unberührt, die in anderen Bestimmungen des TKG oder in anderen Bundesgesetzen festgelegt sind. *Die Informationsnachfragen der Behörden müssen jedenfalls **angemessen und objektiv gerechtfertigt** sein und auf das **absolut Notwendige** beschränkt werden.*[98] Zur Einholung dieser Auskünfte ist jeweils die Behörde berechtigt, die die verlangten Informationen zur verantwortlichen Ausführung ihres Aufgabenbereiches benötigt.[99]

- Informationsersuchen müssen **angemessen** sein und **keine unzumutbare Belastung für Unternehmen** darstellen. Die eingeholten Informationen sollen öffentlich zugänglich sein, sofern es sich nicht um vertrauliche Informationen handelt und Rechtsvorschriften über das Geschäftsgeheimnis eingehalten werden. Das Zurverfügungstellung von Informationen stellt keine Bedingung für die Aufnahme der Tätigkeit als Betreiber dar.[100]

[98] So in den ErlRV 128 der Beilagen XXII. GP 17.
[99] *Stratil* (Hrsg), TKG 2003[4] (2013) 376.
[100] ErlRV 128 der Beilagen XXII. GP 17.

4.4.1.4 Auskünfte im Bereich der Informationsgesellschaft (ECG)

E-Commerce-Gesetz:

§ 18 ECG
(1) Die in den §§ 13 bis 17 genannten Diensteanbieter sind nicht verpflichtet, die von ihnen gespeicherten, übermittelten oder zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen.

(2) Die in den §§ 13 und 16 genannten Diensteanbieter haben auf Grund der Anordnung eines dazu gesetzlich befugten inländischen Gerichtes diesem **alle Informationen zu übermitteln, an Hand derer die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Übermittlung oder Speicherung von Informationen abgeschlossen haben, zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen ermittelt werden können**.

(3) Die in § 16 genannten Diensteanbieter haben **auf Grund der Anordnung einer Verwaltungsbehörde dieser den Namen und die Adressen der Nutzer** ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, zu übermitteln, sofern die Kenntnis dieser Informationen eine wesentliche Voraussetzung der Wahrnehmung der der Behörde übertragenen Aufgaben bildet.

(4) Die in § 16 genannten Diensteanbieter haben den **Namen und die Adresse eines Nutzers ihres Dienstes**, mit dem sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, **auf Verlangen dritten Personen zu übermitteln, sofern** diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts sowie überdies glaubhaft machen, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.

(5) Sonstige Auskunfts- und Mitwirkungspflichten der Diensteanbieter gegenüber Behörden oder Gerichten bleiben unberührt.

KOMMENTAR
Aus den Erläuterungen zum ECG (817 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXI. GP)

Zu § 18 ECG:
Die Richtlinie hindert die Mitgliedstaaten in Art. 15 Abs. 1 daran, eine **allgemeine Überwachungspflicht der Access oder Host Provider** für die von ihnen übermittelten oder gespeicherten Informationen vorzusehen. Auch können die Mitgliedstaaten diese Provider nicht dazu verpflichten, von sich aus Umstände über eine allenfalls rechtswidrige

Tätigkeit zu ermitteln. Die in den Art. 12 bis 14 der Richtlinie (§§ 13, 15 und 16 ECG) genannten Anbieter sind nicht verpflichtet, die von ihnen gespeicherten oder übermittelten Informationen und Inhalte vorweg einer Kontrolle auf deren Rechtskonformität zu unterziehen. Damit sollen sie aber nicht davon abgehalten werden, mit ihren Nutzern Verträge über die von diesen einzuhaltenden Standards zu schließen. In solchen Verträgen können die Provider die Nutzer insbesondere dazu verpflichten, rechtswidrige Tätigkeiten oder Informationen zu unterlassen und sich für den Fall eines Zuwiderhandelns die Entfernung der von ihnen gespeicherten Informationen oder die Sperre des Zugangs vorbehalten. Auch will die Richtlinie – wie schon erwähnt – den Bestrebungen der Anbieter, illegale Inhalte aus dem Internet und anderen Kommunikationsnetzen durch entsprechende technische Vorrichtungen möglichst herauszuhalten, nicht entgegenstehen. Es ist wichtig, dass sich die Provider dieser Fragen annehmen, zumal das Internet und die anderen modernen Kommunikationstechnologien vielfach unter Hinweis auf dort auffindbare Inhalte diskreditiert werden. Effiziente und funktionierende Mechanismen der "Selbstreinigung" können dazu beitragen, das Vertrauen in die modernen Kommunikationstechnologien zu stärken.

Art. 15 Abs. 2 der Richtlinie stellt es den Mitgliedstaaten aber frei, die Diensteanbieter zu verpflichten, Behörden oder Gerichte über mutmaßliche rechtswidrige Tätigkeiten oder Informationen zu unterrichten. Auch können die Mitgliedstaaten die Anbieter dazu verhalten, den zuständigen Behörden auf Verlangen Informationen über die Nutzer ihrer Dienste herauszugeben. Letztlich lässt die Richtlinie die Befugnis der Behörden oder Gerichte unberührt, von den Anbietern zu verlangen, dass eine Rechtsverletzung abgestellt oder verhindert wird (siehe Art. 12 Abs. 3, Art. 13 Abs. 2 und Art. 14 Abs. 3 der Richtlinie).

§ 18 ECG führt die in Art. 15 Abs. 1 der Richtlinie festgelegten Grundsätze aus. Nach Abs. 1 sollen die in den §§ 13 bis 17 genannten Anbieter (also Access Provider, Betreiber von Suchdiensten, Betreiber, die ein Caching vornehmen, Host Provider und Linksetzer) nicht verpflichtet sein, vorweg die von ihnen gespeicherten, übermittelten oder zugänglich gemachten Informationen zu überwachen. Ferner trifft sie keine Verpflichtung, von sich aus einer allenfalls rechtswidrigen Tätigkeit von Nutzern, die ihre Dienste in Anspruch nehmen, nachzugehen. Es bleibt den Providern aber unbenommen, bestimmte mutmaßlich rechtswidrige Inhalte und Informationen durch entsprechende automationsunterstützt ablaufende Verfahren zu identifizieren, zu sperren oder zu entfernen. Entsprechend dem Vorschlag, die Regelungen der Richtlinie über den Ausschluss der straf- und schadenersatzrechtlichen Verantwortlichkeit auch auf die Betreiber von Suchmaschinen und auf Online-Anbieter, die auf fremde Inhalte verweisen, auszudehnen (§§ 14 und 17 ECG), sollen auch solche Provider von einer allgemeinen Überwachungspflicht freigestellt werden.

Die Bestimmungen der Abs. 2 und 3 entsprechen der in Art. 15 Abs. 2 zweiter Teil der Richtlinie erwähnten Ermächtigung der Mitgliedstaaten. Access und Host Provider sollen nach Abs. 2 auf Grund einer gerichtlichen Anordnung (in der Regel ein im Vorverfahren ergangener gerichtlicher Beschluss) verpflichtet sein, einem zu dieser Anordnung gesetzlich befugten inländischen Gericht auf Verlangen alle Informationen zu übermitteln, an Hand derer die Nutzer, mit denen sie Vereinbarungen über die Übermittlung oder Speicherung von Informationen abgeschlossen haben, ermittelt werden können. Die Verpflichtung zur Herausgabe der Daten setzt voraus, dass der Anbieter darüber verfügt. Bei der gerichtlichen Anordnung nach § 18 Abs. 2 ECG wird es sich in der Regel um eine nur unter besonderen Voraussetzungen zulässige Überwachung des Fernmeldeverkehrs im Sinn der §§ 134 ff StPO handeln. Weitergehende Mitwirkungspflichten des Betreibers (etwa nach § 89 TKG) bleiben – siehe § 18 Abs. 5 ECG – unberührt. Die Verpflichtung zur Herausgabe der Daten setzt voraus, dass das Gericht zu einer solchen Anordnung gesetzlich befugt ist. Ferner wird vorausgesetzt, dass das Gericht die Informationen zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen benötigt. Das soll auf Grund der Bemerkungen der Kommission im Notifikationsverfahren ausdrücklich klargestellt werden.

§ 18 Abs. 3 ECG soll auch einer dazu gesetzlich befugten Behörde Auskunftsrechte einräumen. Die Auskunftspflicht trifft in einem solchen Fall aber nur Host Provider, auch erstreckt sie sich nur auf den Namen und die Adresse der Nutzer ihrer Dienste. Sie greift ebenfalls nur dann, wenn der Provider über diese Daten verfügt. Das Begutachtungsverfahren hat gezeigt, dass gerade die Gewerbebehörden den Namen und die Anschrift bestimmter Nutzer benötigen, um dem Verdacht einer Gewerbeübertretung oder einer Übertretung sonstiger gewerberechtlicher Vorschriften nachzugehen. Eine entsprechende Auskunftsverpflichtung der Host Provider ist daher geboten. Die Auskunftspflicht setzt voraus, dass die Kenntnis des Namens und der Adresse eines bestimmten Nutzers eine wesentliche Voraussetzung zur Wahrnehmung der der Behörde übertragenen Aufgaben bildet. Diese Voraussetzungen wird die Behörde in ihrem Auskunftsersuchen oder -bescheid darzulegen haben. Letztlich ist eine Behörde nur dann auskunftsberechtigt, wenn sie dazu gesetzlich befugt ist. § 18 Abs. 3 ECG räumt der Behörde für sich allein noch kein Aufsichtsrecht ein. Dazu bedarf es vielmehr noch einer in dem jeweiligen "Materiengesetz" (etwa in der Gewerbeordnung 1994 oder im Wertpapieraufsichtsgesetz) angesiedelten Regelung.

Nach § 18 Abs. 4 ECG sollen Host Provider bestimmte Informationen über ihre Vertragspartner auch an dritte Personen, die daran ein überwiegendes rechtliches Interesse bescheinigen, übermitteln. Mit dieser Regelung soll Personen, die durch rechtswidrige Tätigkeiten oder Informationen eines ihnen nicht bekannten Nutzers in ihren Rechten verletzt werden, und Verbänden oder Gesellschaften, die sich der Wahrung der Rechte bestimmter anderer Personen widmen (etwa Verbraucherverbänden oder Verwertungsgesellschaften), die Rechtsverfolgung erleichtert werden. Diese Verpflichtung

der Provider ist in der Richtlinie nicht unmittelbar vorgezeichnet. Sie verstößt aber als Überwachungspflicht für den besonderen Fall des Eingriffs in die Rechte dritter Personen nicht gegen den Wortlaut oder den Geist der Richtlinie (vgl. wiederum den Erwägungsgrund 47). Die Bekanntgabe des Namens und der Adresse des Nutzers eines Dienstes, mit dem der Anbieter Vereinbarungen über die Speicherung von Informationen abgeschlossen hat, liegt im Interesse des in seinen Rechten Verletzten. Aber auch dem Provider kann eine solche Regelung entgegenkommen, weil sie dem Betroffenen die unmittelbare Rechtsverfolgung gegen den Urheber einer rechtswidrigen Tätigkeit oder Information erleichtert und damit Verfahren gegen den Provider selbst vermieden werden können.

Voraussetzung für die Bekanntgabe des Namens und der Adresse des Nutzers eines Host Providers an einen Dritten ist die Glaubhaftmachung eines überwiegenden rechtlichen Interesses des Dritten an der Feststellung der Identität des Nutzers, mit dem der Host Provider Vereinbarungen über die Speicherung abgeschlossen hat. Zudem muss der Auskunftswerber einen bestimmten rechtswidrigen Sachverhalt bescheinigen. Der Auskunftswerber muss letztlich glaubhaft machen, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die von ihm wahrgenommene oder betriebene Rechtsverfolgung bildet. Unter diesen Voraussetzungen werden der Bekanntgabe der Daten des Nutzers auch keine datenschutzrechtlichen Gründe entgegenstehen (vgl. auch § 8 Abs. 1 Z 4 DSG 2000).

Die Frage, unter welchen Voraussetzungen der Provider einen Auskunftsanspruch anerkennen und die verlangten Daten dem Interessenten herausgeben kann, kann in der Praxis Schwierigkeiten bereiten. Ähnlich wie bei der Beurteilung der "tatsächlichen Kenntnis" im Sinn des § 16 ECG wird dabei auf die Fähigkeiten und das Wissen eines juristischen Laien abzustellen sein (siehe die Erläuterungen zu § 16). Ist es auch für den Nichtfachmann offenkundig, dass eine bestimmte Information gegen die Rechte Dritter verstößt, so steht der Herausgabe der verlangten Daten nichts entgegen. Gleiches gilt, wenn der Auskunftswerber nachvollziehbar und einleuchtend darlegt, dass er die von ihm erwünschten Daten zur Rechtsverfolgung vor den Gerichten benötigt.
Die Auskunftsverpflichtung des Providers erstreckt sich auch im Fall des Abs. 4 nur auf den Namen und die Adresse eines Nutzers, mit dem er Vereinbarungen über die Speicherung von Daten abgeschlossen hat. Weitergehende Informationen, etwa ein Userprofil oder andere Umstände, die zur Rechtsverletzung führen, können dem Auskunftswerber nicht mitgeteilt werden. Der Host Provider wird durch diese Regelung auch nicht verpflichtet, diese Daten zu speichern oder aufzubewahren, er hat auch nur die ihm verfügbaren Daten herauszugeben.

§ 18 Abs. 5 ECG stellt klar, dass Auskunfts- und Mitwirkungspflichten von Online-Anbietern (vor allem nach den §§ 134 ff. StPO 1975 in Verbindung mit § 89 TKG sowie nach § 53 SPG) unberührt bleiben.

4.4.1.5 Sonderfall IP-Adressen[101]

Das Interesse der Sicherheitsbehörden an einer Auskunft über einen – hinter einer IP-Adresse stehenden – Teilnehmer besteht überhaupt nur 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 Verkehrsdatenauskunft, die erst den Personenbezug herstellt, anonym. Die Information darüber, welchem Teilnehmer 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 wie gesagt nicht aufzeichnen, welche Internetseiten vom Teilnehmer aufgerufen wurden. Allerdings sind viele Internetseiten bzw. -dienste technisch derart konzipiert, dass bei Zugriffen auf diese Seiten oder Dienste die IP-Adresse des Teilnehmers sowie der Zeitpunkt des Zugriffs durch den Host-Provider[102] 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, Suchanfragen bei Google,...). Gleichzeitig lässt sich daraus noch nicht ableiten, ob der Anschlussinhaber auch mit dem Urheber 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-Lenkererhebung" erforderlich sein, um Aussagekraft und Zuverlässigkeit der ermittelten Daten beurteilen zu können; denn eine reine Gefährdungshaftung für Inhaber von Internet- oder Telefonanschlüssen ist der österreichischen Rechtsordnung bislang nicht bekannt. Der Aussagekraft und mit ihr verbunden dem tatsächlich Nutzen der Daten für den angestrebten Zweck kommen für die Verhältnismäßigkeit der behördlichen

[101] *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; Hasberger, Die providerinterne Auswertung von Verkehrsdaten und Datenschutz, MR 2010, 23.

[102] Host-Provider ist jener Dienstanbieter, der den Speicherplatz für Web-Seiten zur Verfügung stellt. Zu den verschiedenen Arten von Providern siehe die Web-Seite des Datenschutzexperten und Richter des OLG Salzburg, Franz Schmidbauer: http://www.internet4jurists.at/provider/provider1a.htm (9.9.2016).

Befugnisse entscheidende Bedeutung zu, die bereits abstrakt in jeden Abwägungsvorgang mit einzubeziehen sind.

Die Judikatur des OGH in Strafsachen behandelte Auskünfte über Name und Anschrift zu einer bestimmten (bereits bekannten) IP-Adresse bisher als Stammdatenabfrage nach § 103 (4) TKG. Dass der Anbieter 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 (GZ 11 Os 57/05z). Damit bestanden schon bisher in Bezug auf IP-Adressen keine materiellen Einschränkungen auf bestimmte schwerere Delikte.
Richtervorbehalt oder sonstige Formerfordernisse mit Rechtsschutzcharakter gibt es bei Stammdatenauskünften ebenso keine, vielmehr ist sogar die Kriminalpolizei ohne Anordnung der Staatsanwaltschaft auskunftsberechtigt. Diese Auslegung verkennt völlig, dass diese Ermittlungsbefugnisse eigentlich eher in der Nähe einer Inhaltsüberwachung anzusiedeln sind. Allerdings sind eben zumindest zwei Ermittlungsschritte notwendig. Zunächst muss nämlich beim Dienstanbieter die IP-Adresse zum Ermittlungsrelevanten Inhalt erheben, die Rechtsgrundlage dafür bietet § 18 (4) E-Commerce Gesetz (ECG). Oder diese Information ist auf anderem Weg bekannt geworden, etwa durch Beschlagnahme oder Auswertung eines Servers. Aus dieser Perspektive liegen zunächst noch gar keine personenbezogenen Daten vor, weil der Dienstanbieter nach ECG den Bezug zu einem bestimmten Teilnehmer selbst gar nicht herstellen kann. Dieser Bezug ergibt sich erst aus dem zweiten Ermittlungsschritt durch die Auswertung beim Internet-Zugangsanbieter. Weil sich das Ausmaß dieses Eingriffs in das Datenschutzgrundrecht aber erst „über 2 Ecken" erschließt, scheint der eher sorglose Umgang mit dieser Eingriffsermächtigung weiter zu bestehen.

Im Zivilrecht hat der OGH zu GZ 4 Ob 41/09x (Rechtssache LSG gg Tele 2) diese Problematik unter ausdrücklichem Bezug auf die strafrechtliche Judikatur erkannt, demnach sind dynamische IP-Adressen jedenfalls als Verkehrsdaten zu behandeln[103]. Mit der Legaldefinition der öffentlichen IP-Adresse in § 92 (3) Z 16 TKG in Verbindung mit der ausdrücklichen neuen Rechtsgrundlage für Stammdatenauskünfte an Justizbehörden in § 90 (7) TKG löst der Gesetzgeber diese Judikaturdivergenz nun auf.[104] Sachlich besteht das Problem auf Grund der weiten Ausnahmen über § 99 (5) TKG in Verbindung mit § 76a (2) StPO aber fast unverändert weiter.

[103] So im Ergebnis auch das VfGH Erkenntnis G 31/08 vom 1. Juli 2009, wenngleich diese Frage dort nicht mit derselben Tiefe behandelt wird, sondern lediglich die Speicherverpflichtung thematisiert wird.
[104] Vgl. dazu die EB zur RV § 90 (7) sowie zu 92 (3) Z 16, Nr. 1074, XXIV. GP, http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/fname_206854.pdf (18.4.2011).

Eine Auskunftserteilung zu Name und Anschrift einer IP-Adresse ist im Rahmen eines zivilgerichtlichen Verfahrens (etwa in Zusammenhang mit Urheberrechtsverletzungen) nicht möglich. [105]

4.4.2 Überwachung der Inhalte

Standortdaten und „Funkzellenabfrage“ Parlamentarische Anfragen 4084J/4087J
*) In wie vielen Fällen wurden jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 das Instrument einer Funkzellenabfrage ("Funkzellenabfrage" heißt eine Auswertung aller im Bereich einer Sendestation zu einem bestimmten Zeitpunkt gespeicherten Daten, siehe OLG Wien vom 26.4.2013, 9Bs108/13s)
durch österreichische Behörden zum Einsatz gebracht?
*) Aufgrund welcher Rechtsgrundlage werden Funkzellenabfragen von den österreichischen Behörden vorgenommen?
*) Aufgrund welcher Deliktsarten wurden Funkzellenabfragen jeweils
in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 zum Einsatz gebracht?
*) Von wie vielen Personen wurden Daten im Rahmen des Einsatzes von Funkzellenabfragen erhoben?
*) Welche Datenarten bzw. Kategorien von Datenarten werden bei einem Einsatz einer Funkzellenabfrage erhoben?
*) Welche Vorkehrungen werden getroffen um die Daten von unbeteiligten Dritten im Abfragegebiet einer Funkzellenabfrage zu schützen?
*) Wurden in der Vergangenheit oder werden aktuell Funkzellenabfragen im Rahmen von Großveranstaltungen eingesetzt?
*) Falls ja, bei wie vielen Großveranstaltungen wurden Funkzellenabfragen
jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 zum Einsatz gebracht?
*) In wie vielen Fällen konnten durch die Nutzung Funkzellenabfrage geplante Straftaten verhindert oder Straftaten aufgeklärt werden? Welche Deliktarten sind hier betroffen?
*) Wie lange werden die Daten von Funkzellenabfragen aufbewahrt?
Gibt es hier eine unterschiedliche Behandlung der Daten von unbeteiligten Dritten?
*) Vorausgesetzt eine erfolgreiche Funkzellenabfrage liefert eine Liste an Telefonnummern und Anschlussinhabern,
unter denen sich der oder die Verdächtige(n) befinden sollen. Wie funktioniert der weitere Abgleich, um die Verdächtigen von den nicht Verdächtigen zu filtern?
*) Wenn ein solcher Abgleich automationsunterstützt abläuft,
wird dieser auf Basis des §141 ff. StPO („Rasterfahndung“) durchgeführt?

[105] 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 (355 f).

Parlamentarische Beantwortung – IST-Stand Österreich

Antwort 4084J: Funkzellenabfragen erfolgen ausschließlich nach gerichtlicher Genehmigung über Anordnung einer Staatsanwaltschaft gemäß § 135 Abs. 2 Strafprozessordnung. Daher wird auf die Beantwortung der gleichlautenden Anfrage 4087/J vom 6. März 2015 an das Bundesministerium für Justiz verwiesen.

Antwort 4087J: Bei der sogenannten Funkzellenauswertung handelt es sich um eine Anordnung der Auskunft über Daten einer Nachrichtenüberwachung nach §§ 134 Z 2, 135 Abs. 2 StPO. Als solche werden diese Anordnungen auch in der Verfahrensautomation Justiz statistisch erfasst.

Bei der statistischen Erfassung wird keine Unterscheidung getroffen, ob die Anordnung einen Telefonanschluss, einen Internetanschluss oder eine Funkzelle betrifft. Aufgrund dessen liegen mir als Bundesminister für Justiz keine Daten vor, um diese Fragen beantworten zu können.

> Im Hinblick auf die Anordnungsvoraussetzungen bzw. zur Frage nach den Deliktsarten kann im Allgemeinen zunächst auf § 135 Abs. 2 StPO verwiesen werden. Demnach ist eine Auskunft über Daten einer Nachrichtenübermittlung zulässig,
>
> „1. wenn und solange der dringende Verdacht besteht, dass eine von der Auskunft betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird, […]
> 3. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.
> 4. wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.
>
> Eine Zustimmung des Inhabers der technischen Einrichtung (§ 135 Abs. 2 Z 2 StPO) kommt im Fall der Funkzellenauswertung, aber auch beim Einsatz des IMSI-Catchers nicht in Betracht.
>
> Aufgrund der Eingriffsintensität der Maßnahmen ist nach der geltenden Rechtsprechung besonders auf die Verhältnismäßigkeit zu achten. Derartige Maßnahmen werden daher nur bei schwerer Kriminalität zum Einsatz gelangen können, wenn keine weiteren Ermittlungsansätze bestehen bzw. andere (weniger in die Grundrechte Dritter eingreifende) Maßnahmen nicht zum selben Ergebnis führen. Dies wurde vom Obersten Gerichtshof in seiner erst am 5. März 2015 ergangenen Entscheidung bestätigt, in der er hervorhebt, „dass dem Verhältnismäßigkeitsgebot in jedem Einzelfall – etwa durch die Begrenzung der Maßnahme auf eine kurze Zeitspanne – zu entsprechen ist, um zu gewährleisten, dass in das Kommunikationsgeheimnis Unbeteiligter nur soweit eingegriffen wird, als dies für einen erfolgversprechenden Ermittlungsschritt unvermeidlich und im Hinblick auf die zu erwartende

Zahl von Betroffenen und das Gewicht der aufzuklärenden Straftat vertretbar ist“.

Eine Entscheidung des Oberlandesgerichtes Wien zur Aktenzahl 9 Bs 108/13s gibt es hingegen nicht.

Zunächst ist der gesetzliche Rahmen zu beachten. § 134 Z 2 StPO definiert die Daten einer Nachrichtenüberwachung als „die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG), die nicht einer Anordnung gemäß § 76a Abs. 2 unterliegen, und Standortdaten (§ 92 Abs. 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes)“.

Der kriminaltaktische Sinn der sogenannten Funkzellenauswertung besteht jedoch in der Ermittlung, welche Anschlüsse sich zu einem bestimmten Zeitpunkt im Sendebereich der Funkzelle befunden haben. Es geht also um die Zugangsdaten, d.h. „jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind“ (§ 92 Abs. 3 Z 4a TKG).

Ich kann diese Frage nur aus Sicht des Justizressorts beantworten, denn die Aufsicht über die Telekommunikationsbetreiber fällt nicht in meine Zuständigkeit. Der Schutz von personenbezogenen Daten wird allgemein dadurch gewährleistet, dass das Ermittlungsverfahren nicht öffentlich ist. Akteneinsicht steht in erster Linie nur den Parteien des Verfahrens zu, d.h. Beschuldigten gemäß §§ 51 bis 53 StPO, dem Opfer und dem Privatbeteiligten gemäß § 68 StPO. Im Fall eines (nachgewiesenen) begründeten rechtlichen Interesses kann auch dritten Personen ein Recht auf Akteneinsicht zustehen (§ 77 StPO). Darüber hinaus gilt § 145 StPO. Nach § 145 Abs. 2 StPO sind Anordnungen und Genehmigungen dieser Ermittlungsmaßnahme, ihre gerichtlichen Bewilligungen sowie in Bild oder Schriftform übertragene Ergebnisse (§ 134 Z 5) zunächst getrennt aufzubewahren und erst dann zum Akt zu nehmen, wenn die betreffende Anordnung dem Beschuldigten gegenüber rechtskräftig geworden ist, spätestens jedoch beim Einbringen der Anklage. Bis zur Zustellung der Anordnung an den Beschuldigten können sie von der Einsicht durch diesen sowie durch Privatbeteiligte und Opfer ausgenommen werden, wenn zu befürchten ist, dass andernfalls der Zweck der Ermittlungen oder die Persönlichkeitsrechte von Personen, die von diesen Ermittlungsmaßnahmen betroffen sind, gefährdet wären; im Übrigen gilt § 51 Abs. 2 StPO.

§ 145 Abs. 3 StPO bestimmt weiters: „Solange in Bild- oder Schriftform übertragene Ergebnisse einer Ermittlungsmaßnahme in den Fällen des §§ 135 Abs. 2 bis 3 sowie 136 Abs. 1 Z 2 und 3 nicht zum Akt genommen werden, sind sie samt den zugehörigen Anordnungen, gerichtlichen Bewilligungen und sonstigen Aktenstücken unter Verschluss aufzubewahren. Näheres hat der Bundesminister für Justiz durch Verordnung zu bestimmen.“

Bei der Bezug habenden Verordnung handelt es sich um die Verschlusssachenverordnung (BGBl. II Nr. 351/2014). Darüber hinaus ist auch § 139 StPO zu beachten:

„(1) Dem Beschuldigten ist zu ermöglichen, die gesamten Ergebnisse (§ 134 Z 5) einzusehen

und anzuhören. Soweit berechtigte Interessen Dritter dies erfordern, hat die Staatsanwaltschaft jedoch Teile der Ergebnisse, die nicht für das Verfahren von Bedeutung sind, von der Kenntnisnahme durch den Beschuldigten auszunehmen. Dies gilt nicht, soweit während der Hauptverhandlung von den Ergebnissen Gebrauch gemacht wird.

(2) Die von der Durchführung der Ermittlungsmaßnahme betroffenen Personen haben das Recht, die Ergebnisse insoweit einzusehen, als ihre Daten einer Nachrichtenübermittlung, für sie bestimmte oder von ihnen ausgehende Nachrichten oder von ihnen geführte Gespräche oder Bilder, auf denen sie dargestellt sind, betroffen sind. Über dieses und das ihnen nach Abs. 4 zustehende Recht sind diese Personen, sofern ihre Identität bekannt oder ohne besonderen Verfahrensaufwand feststellbar ist, von der Staatsanwaltschaft zu informieren. […]

(4) Auf Antrag des Beschuldigten oder von Amts wegen sind Ergebnisse der Ermittlungsmaßnahme zu vernichten, wenn diese für ein Strafverfahren nicht von Bedeutung sein können oder als Beweismittel nicht verwendet werden dürfen. Dieses Antragsrecht steht auch den von der Ermittlungsmaßnahme Betroffenen zu, insoweit für sie bestimmte oder von ihnen ausgehende Nachrichten oder Bilder, auf denen sie dargestellt sind, oder von ihnen geführte Gespräche betroffen sind."

Im Rahmen eines Strafverfahrens finden die Bestimmungen über die Anordnung der Auskunft über Daten einer Nachrichtenüberwachung nach §§ 134 Z 2, 135 Abs. 2 StPO Anwendung. Zu den Anwendungsvoraussetzungen möchte ich auf die Beantwortung der Fragen 1 bis 3 verweisen. Darüber hinaus bin ich zur Beantwortung nicht zuständig; für Fragen der Gefahrenabwehr nach dem Sicherheitspolizeigesetz ist die Frau Bundesministerin für Inneres zuständig.

Sollte neben einer Funkzellenauswertung noch eine „Rasterfahndung", d.h. ein automationsunterstützter Datenabgleich gemäß § 141 StPO, erforderlich sein, müsste diese Anordnung, wie bereits in der Frage angedeutet, nach den strengen Voraussetzungen des § 141 StPO angeordnet und gerichtlich bewilligt werden. In diesem Fall wäre zusätzlich nicht nur der Rechtsschutzbeauftragte der Justiz nach § 147 StPO zur Prüfung und Kontrolle der Anordnung, Genehmigung und Durchführung des automationsunterstützten Datenabgleichs berufen, auch die Datenschutzbehörde hätte eine Rechtsmittelmöglichkeit (§ 142 Abs. 4 StPO). Aus den dem Parlament übermittelten Gesamtberichten über besondere Ermittlungsmaßnahmen der Jahre 2009 bis 2013 ergibt sich jedoch, dass die Maßnahme des automationsunterstützten Datenabgleichs nicht zur Anwendung gelangte. Üblicherweise werden Auswertungen mehrerer Funkzellen (z.B. bei schweren Serieneinbruchsdiebstählen Funkzellenauswertungen unterschiedlicher Tatorte) verglichen, um den Kreis der in Frage kommenden Täter zumindest einzugrenzen. In vielen Fällen sind die im Zusammenhang mit Einbruchsdiebstählen verwendeten Anschlüsse bereits durch diese Ermittlungsmaßnahmen eindeutig identifizierbar.

4.4.2.1 IMSI Catcher

Parlamentarische Anfragen 4084J/4087J/4088J/4089J *) Wie viele IMSI Catcher welchen Gerätetyps und Modells wurden im Verantwortungsbereich des Ministeriums angeschafft?

*) Wie viele IMSI Catcher im Verantwortungsbereich des Ministeriums besitzen ausschließlich Funktionalität zur Identifikation von TeilnehmerInnen und wie viele sind darüber hinaus auch im Stande Inhalte zu überwachen?
*) Für welche Behörde und welche Abteilung dieser wurde jeweils
in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 IMSI-Catcher-Ausrüstung angeschafft?
*) Wie viel hat diese gekostet?
*) Von wie vielen Personen wurden Daten im Rahmen des Einsatzes von
IMSI Catchern jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 erhoben?
*) Von wie vielen dieser Einsätze von IMSI Catchern in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014
wurde jeweils lediglich die Funktionalität zur Identifizierung einzelner TeilnehmerInnen genutzt und in wie vielen Fällen wurden darüber hinaus auch Kommunikationsinhalte überwacht?
*) Worin besteht die jeweilige Einsatznotwendigkeit dieser Ausrüstung für die jeweilige Abteilung der jeweiligen Behörde?
*) Aufgrund welcher Rechtsgrundlage werden IMSI-Catcher von den österreichischen Behörden zum Einsatz gebracht?
*) Welche Vorkehrungen werden getroffen, um die Daten von unbeteiligten Dritten im Einsatzgebiet eines IMSI-Catchers zu schützen?
*) Welche gelinderen Mittel müssen ausgeschöpft bzw. ausgeschlossen werden, bevor ein IMSI-Catcher zum Einsatz kommt?
*) Welche Geräte vom Typ IMSI-Catcher sind in Österreich bewilligt?
*) In welcher Form und auf welcher Rechtsgrundlage ist diese Bewilligung erfolgt (Bescheid, Typengenehmigung, generelle Genehmigung)?
*) Welche Stellen sind die Bewilligungsinhaber?
*) Auf welcher Rechtsgrundlage werden in Österreich IMSI-Catcher auf lizenzierten Frequenzbändern betrieben?
*) Werden von den Fernmeldebüros oder Vertragsfirmen Messungen vorgenommen, um illegale IMSI-Catcher zu identifizieren?

Parlamentarische Beantwortung – IST-Stand Österreich

Antwort 4084J: Dem Bundesministerium für Inneres steht aktuell ein IMSI-Catcher zur Verfügung. (Kommunikations-)Inhalte können mit diesem Gerät nicht überwacht werden. Im Vollzugsbereich des Bundesministeriums für Inneres wird der IMSI-Catcher ausschließlich unter den Voraussetzungen des § 53 Abs. 3b Sicherheitspolizeigesetz als technisches Mittel zur Lokalisierung der Endeinrichtung von gefährdeten oder diesen begleitenden Menschen zum Zwecke der Hilfeleistung oder Abwehr einer Gefahr in allen Bundesländern zum Einsatz gebracht. Wenn auf Grund des bei der Behörde vorliegenden Sachverhalts (bestimmte Tatsachen) von einer gegenwärtigen Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen ausgegangen werden muss und die Lokalisierung der Endeinrichtung mittels IMSI-Catcher das zielführendste Mittel zur

Aufgabenerfüllung darstellt, ist sein Einsatz verhältnismäßig. Durch spezielle Software sind technische Vorkehrungen zum Schutz der Daten unbeteiligter Dritter getroffen worden. Statistiken über die Art der Hilfeleistung werden nicht geführt. Von einer anfragebezogenen bundesweiten retrospektiven manuellen Auswertung unter Einsicht in die Akten bei jeder einzelnen fallführenden Dienststelle wird angesichts des dafür erforderlichen hohen Verwaltungsaufwandes unter Beachtung der Grundsätze der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit des Verwaltungshandelns Abstand genommen. Im Zusammenhang mit der Zahl der Fälle, in denen eine Lokalisierung unter Einsatz technischer Mittel stattgefunden hat, wird auf § 91c iVm § 91d Abs. 4 SPG verwiesen, wonach die Bundesministerin für Inneres den Jahresbericht des Rechtsschutzbeauftragten mit den diesbezüglichen Informationen über Verlangen dem ständigen Unterausschuss des Ausschusses für innere Angelegenheiten gemäß Art 52a B-VG zugänglich macht. Soweit nach dem Einsatz des IMSI-Catchers im Dienste der Strafrechtspflege gefragt wird, wird zuständigkeitshalber auf die Beantwortung der gleichlautenden Anfrage 4087/J vom 6. März 2015 an das Bundesministerium für Justiz verwiesen.

Antwort 4087J: Der Einsatz des sogenannten IMSI-Catchers ist nicht gesondert in der StPO geregelt, sondern fällt allgemein in den Anwendungsbereich der Anordnung der Auskunft über Daten einer Nachrichtenüberwachung[106] nach §§ 134 Z 2, 135 Abs. 2 StPO und ist daher nicht gesondert erfassbar oder auswertbar.

Antwort 4088J: Beruft sich auf die Amtsverschwiegenheit

Antwort 4089J: Es besteht eine telekommunikationsrechtliche Bewilligung zur Einfuhr, zum Besitz und zum Betrieb für eine Anlage, die im Frequenzbereich der Mobilkommunikationsnetze 900 und 1800 MHz arbeitet. Die genaue Typenbezeichnung und der Hersteller der Anlage werden aus Gründen der Amtsverschwiegenheit nicht beauskunftet. Die telekommunikationsrechtliche Bewilligung erfolgt mit Bescheid auf der Grundlage des Telekommunikationsgesetzes. Inhaber der telekommunikationsrechtlichen Bewilligung ist das Bundesministerium für Inneres. Die Fernmeldebehörden messen routinemäßig das Funkfrequenzspektrum. Da IMSI-Catcher Mobilfunk-Basisstationen imitieren, sind deren Funksignale kaum als solche von IMSI-Catchern zu identifizieren. Allenfalls könnten auch Störungen bei Mobilfunkbetreibern auf die Existenz eines IMSI-Catchers hinweisen. Bisher konnten messtechnisch auch keine IMSI-Catcher im Betrieb aufgefunden werden und es gab bisher auch keine einschlägigen Störmeldungen.

Das Problem beim IMSI Catcher besteht vor allem darin, dass er faktisch deutlich mehr kann, als die Rechtsgrundlage zulässt. Während § 53 Abs. 3b SPG nur erlaubt, den aktuellen Standort einer gefährdeten Person zu erheben, eignet sich der IMSI Catcher

[106] Sic! – hier geht es um Daten einer Nachrichtenübermittlung, nicht -überwachung.

insbesondere zum Abhören von Inhalten, ohne dass dafür die Mitwirkung des Anbieters erforderlich ist. Hier wäre dringend geboten, dass entsprechende rechtliche, technische und organisatorische Sicherungen geschaffen werden, die eine gesetzeskonforme Anwendung effektiv sichern.

4.4.2.2 Stille SMS

Parlamentarische Anfragen
*) In wie vielen Fällen wurden jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 wie viele stille SMS auf Veranlassung von Österreichischen Behörden im Einflussbereich des Ministeriums versendet?
*) Aufgrund welcher Deliktsarten wurden jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 stille SMS versandt?
*) Aufgrund welcher Rechtsgrundlage werden von den österreichischen Behörden stille SMS versandt?
*) Welche technischen Möglichkeiten verwenden österreichische Sicherheitsbehörden für den Versand stiller SMS?

4.4.2.3 Überwachungs- und Auskunftsbefugnisse im Überblick

Die nachfolgende Tabelle zeigt einen Überblick, nach welchen Rechtsgrundlagen ein Anbieter welchen Behörden welche Daten bekannt geben darf. Der Überblick wurde von der ISPA (Internet Service Providers Austria) für deren Mitglieder erstellt und wird seit 2010 kontinuierlich weiterentwickelt. Da die ISPA einen sehr großen Teil der österreichischen Telekom-Industrie repräsentiert, hat die Darstellung auch in der Praxis eine entsprechende Bedeutung. Deshalb und weil die Übersicht einen echten Mehrwert bietet, wird sie auch hier wiedergegeben.

Beauskunftung - Übersicht

Rechtsgrundlage	Grundnorm (TKG)	Auskunft über	Anfrage- Art	DLS-Pflicht (Anfrage)	DLS-Pflicht (Antwort)	Anfrageber. Stelle	Anfragegrund	"Begründung" (gegenüber NB)
Sicherheitspolizeigesetz (SPG)								
§ 53 Abs 3a Z 1 SPG	§ 90 Abs 7	Stammdaten[1]	schriftlich	(vorzugsweise) wenn optiert	ja, wenn optiert	Polizei[1]	SPG	nein
		Stammdaten[1]	schriftlich	nein	nein	Polizei[1]	SPG	nein
		Stammdaten[1]	(vorläufig) mündl. (Verw. § 90/7 TKG)	nein	nein	Polizei[1]	SPG - dringender Fall	nein - Nachreichung
§ 53 Abs 3a Z 2 SPG	§ 99 Abs 5 Z 4	IP-Adressen-Bekanntgabe	schriftlich	ja	ja	Polizei	Gefahrenabwehr / EAH / krimin. Vbg	nicht ausdrücklich vorgesehen
		IP-Adressen-Bekanntgabe	schriftlich	nein (bei GiV)	nein	Polizei	Gefahrenabwehr / EAH / krimin. Vbg	nicht ausdrücklich vorgesehen
§ 53 Abs 3a Z 3 SPG	§ 99 Abs 5 Z 4	Stammdaten zu IP-Adresse	schriftlich	ja	ja	Polizei	Gefahrenabwehr / EAH / krimin. Vbg	nicht ausdrücklich vorgesehen
		Stammdaten zu IP-Adresse	schriftlich	nein (bei GiV)	nein	Polizei	Gefahrenabwehr / EAH / krimin. Vbg	nicht ausdrücklich vorgesehen
§ 53 Abs 3a Z 4 SPG	§ 99 Abs 5 Z 3	passive Rufdaten	schriftlich	ja	ja	Polizei	Gefahrenabwehr / EAH	nicht ausdrücklich vorgesehen
		passive Rufdaten	schriftlich	nein (bei GiV)	nein	Polizei	Gefahrenabwehr / EAH	nicht ausdrücklich vorgesehen
§ 53 Abs 3b SPG	§ 99 Abs 5 Z 3	IMSI, Standort	schriftlich	nein (da immer GiV - "gegenwärtig"!)	nein	Polizei	Gefahrenabwehr / EAH	ja
		IMSI, Standort	mündlich	nein (da immer GiV - "gegenwärtig"!)	nein	Polizei	Gefahrenabwehr / EAH	ja - Nachreichung!
Strafprozessordnung (StPO)								
§ 76a Abs 1 StPO	§ 90 Abs 7	Stammdaten	schriftlich	(vorzugsweise) wenn optiert	ja, wenn optiert	Gerichte, StA, Polizei	Straftat	nein
		Stammdaten	schriftlich	nein	nein	Gerichte, StA, Polizei	Straftat	nein
		Stammdaten	(vorläufig) mündl. (Verw. § 90/7 TKG)	nein	nein	Gerichte, StA, Polizei	Straftat - dringender Fall	nein - Nachreichung
§ 76a Abs 2 Z 1, Z 4 2. Fall StPO	§ 99 Abs 5 Z 2	IP-Adresse, E-Mail & IP-Adr. des Abesenders	schriftlich	ja (auch bei GiV)	ja	Gericht, StA	Straftat (Anordnung der StA)	nein (Anordnung)
§ 76a Abs 2 Z 2 - 3 StPO		E-Mail-Adresse	schriftlich	nein (optional)	nein (optinonal)	Gericht, StA	Straftat (Anordnung der StA)	nein (Anordnung)
§§ 134 Z 2 / 135 Abs 2 StPO	§ 99 Abs 5 Z 1	Verkehrsdaten	schriftlich	ja	ja	Gerichte, StA, Polizei	Straftat (gerichtlich bewilligte Anordnung der StA)	nein (Anordnung)
		Zugangsdaten (eingeschränkt auf IMSI, IMEI)[2]	schriftlich	ja	ja	Gerichte, StA, Polizei	Straftat (gerichtlich bewilligte Anordnund der StA)	nein (Anordnung)
		Standortdaten (historisch / fortlaufend)	schriftlich	ja	ja	Gerichte, StA, Polizei	Straftat (gerichtlich bewilligte Anordnung der StA)	nein (Anordnung)
		Standortdaten (aktuelle Peilung)	schriftlich	nein	nein	Gerichte, StA, Polizei	Straftat (gerichtlich bewilligte Anordnung der StA)	nein (Anordnung)
Telekommunikationsgesetz (TKG)								
§ 90 Abs 6 TKG	-	Stammdaten	schriftlich	nein	nein	Verwaltungsbehörden	Verwaltungsübertretung	ja
§ 90 Abs 7 TKG	-	Stammdaten	schriftlich	(vorzugsweise) wenn optiert	ja, wenn optiert	Gerichte, StA, Polizei	Straftat	nein
		Stammdaten	schriftlich	nein	nein	Gerichte, StA, Polizei	Straftat	nein
		Stammdaten	(vorläufig) mündl.	nein	nein	Gerichte, StA, Polizei	Straftat - dringender Fall	nein, aber Nachreichung
§ 98 Abs 1 TKG	-	Stammdaten	schriftlich	nein	nein	Notrufdienst-Betreiber	Notfall	ja (da Anfrage durch 3. Person)
		Stammdaten	mündlich	nein	nein	Notrufdienst-Betreiber	Notfall	ja - Nachreichung!
		Standortdaten (Benachrichtigung des Betroffenen)	schriftlich	nein	nein	Notrufdienst-Betreiber	Notfall	ja (da Anfrage durch 3. Person)
		Standortdaten (Benachrichtigung des Betroffenen)	mündlich	nein	nein	Notrufdienst-Betreiber	Notfall	ja - Nachreichung!
§ 98 Abs 3 TKG (Schnittst.NRT)	-	Stammdaten	schriftlich	nein (Schnittst.NRT)	nein (Schnittst.NRT)	Notrufdienst-Betreiber	Notfall	nein (da Gesuchter direkt)
		Stammdaten	mündlich	nein (Schnittst.NRT)	nein (Schnittst.NRT)	Notrufdienst-Betreiber	Notfall	nein (da Gesuchter direkt)
		Standortdaten (Benachrichtigung des Betroffenen)	schriftlich ("unmittelbar")	nein (Schnittst.NRT)	nein (Schnittst.NRT)	Notrufdienst-Betreiber	Notfall	nein (da Gesuchter direkt)
		Standortdaten (Benachrichtigung des Betroffenen)	mündlich ("unmittelbar")	nein (Schnittst.NRT)	nein (Schnittst.NRT)	Notrufdienst-Betreiber	Notfall	nein (da Gesuchter direkt)
DIVERSES								
Rechtsgrundlage		**Auskunft über**	**Anfrage- Art**	**DLS-Pflicht (Anfrage)**	**DLS-Pflicht (Antwort)**	**Anfrageber. Stelle**	**Anfragegrund**	**"Begründung" (gegenüber NB)**
§ 99 Abs 3 FinStrG	-	Stammdaten (erweitere Pflichten)	schriftlich	nein	nein	Finanzstrafbehörde	Finanzstrafverfahren	nein
§ 99 Abs 3a FinStrG	fehlt!	Verkehrsdaten (IP-Adresse; Name & Anschrift zu IP-Adresse)	schriftlich	ja	ja	Finanzstrafbehörde	Finanzstrafverfahren (Anordnung des Senatsvorsitzenden	ja
§ 11 Abs 1 Z 5 PStSG	§ 90 Abs 7	Stammdaten	schriftlich	(vorzugsweise) wenn optiert	ja, wenn optiert	BVT, LV	PStSG, Ermächtigung des DSB bei BMI	nein
		Stammdaten	schriftlich	nein	nein	BVT, LV	PStSG, Ermächtigung des DSB bei BMI	nein
		Stammdaten	(vorläufig) mündl. (Verw. § 90/7 TKG)	nein	nein	BVT, LV	PStSG, Ermächtigung des DSB bei BMI	nein
§ 11 Abs 1 Z 5 PStSG	§ 99 Abs 5 Z 3	IP-Adressen-Bekanntgabe	schriftlich	ja	ja	BVT, LV	PStSG, Ermächtigung des DSB bei BMI	nein
		IP-Adressen-Bekanntgabe	schriftlich	nein (bei GiV)	nein	BVT, LV	PStSG, Ermächtigung des DSB bei BMI	nein
		IMSI, Standort	schriftlich	nein (da immer GiV - "gegenwärtig"!)	nein	BVT, LV	PStSG, Ermächtigung des DSB bei BMI	nein
		IMSI, Standort	mündlich	nein (da immer GiV - "gegenwärtig"!)	nein	BVT, LV	PStSG, Ermächtigung des DSB bei BMI	nein
§ 11 Abs 1 Z 7 PStSG	§ 99 Abs 5 Z 5	Verkehrsdaten, Standort, Zugangsdaten	schriftlich	ja	ja	BVT, LV	Straftat mit mehr als 1 J. FS; Ermächtigung des	Ermächtigung des Rechts-schutzsenats ist anzuführen
§ 143 BAO	-	gs Stammdaten (erweitere Pflichten)	schriftlich	nein	nein	Abgabenbehörde	Erhebung von Abgaben	nein
§ 48b Abs 3 BörseG	fehlt!	Verkehrsdaten, Standortdaten, Zugangsdaten, Stammdaten	schriftlich	ja	ja	Finanzmarktaufsicht	Verwaltungsübertretung	Gerichtlich bewilligte Anordnung der FMA
§ 14a UWG	-	Name, Anschrift anhand Rufnummer	schriftlich	nein	nein	idR Schutzverband	Verdacht unlauterer Geschäftspraxis	ja
§ 22 Abs 2a MBG	-	Stammdaten zu Rufnummer	schriftlich	nein	nein	militär. Organe/	nachrichtendienstl. Aufklärung/Abwehr	nein

Hinweis: Statische/ vertragliche zugewiesene IP-Adressen werden als Stammdaten behandelt. Dynamische IP-Adressen werden als Zugangsdaten behandelt.

[1] Gerichte, StA und Kriminalpolizei: Auskunft über Stammdaten (§ 90 (7) TKG); Sicherheitsbehörden: nur Name, Anschrift, Teilnehmernummer (§ 53 (3a) Z 1 SPG)

[2] Die Beauskunftung von dynamische IP-Adressen sowie die in § 76a Abs. 2 StPO angeführten Email-Daten darf ab 01.04.12 nur nach Anordnung des StA gem § 102 StPO erfolgen.

Hinweis: Durch Mausklick auf die Rechtsgrundlage der Anfragen (Spalte A) oder die korrespondierende Norm im TKG (Spalten B) gelangen Sie zu der jeweiligen Bestimmung im Rechtsinformationssystem (RIS).

v.0.43., 15.09.2016 ENTWURF

Die Stimme der Internetwirtschaft in Österreich

ispa Internet Service Providers Austria

4.4.3 Netzsperren und Netzfilter

Netzsperren und Internet Service Provider als "Hilfssheriffs":
Der Begriff der Piraterie-Websites hat in den letzten Jahren durchgängige Bekanntheit erlangt. Besonders aufgrund der medialen Berichterstattung wurden Websites wie kino.to oder thepiratebay.org und die Verfolgung von deren Betreibern breit thematisiert. Derartigen Websites ist gemein, dass sie zu einem wesentlichen Anteil urheberrechtlich geschützte Filme und Musik ohne Erlaubnis der Rechteinhaber und daher nicht rechtmäßig zum Download oder Streaming zur Verfügung stellen.

4.4.3.1 Warum Netzsperren?

Neben der strafrechtlichen Ahndung der Betreiber rückte im Laufe der Zeit zunehmend die Frage in den Vordergrund, ob die sog. Internet-Piraterie durch das Sperren jener Seiten, die den Zugriff auf illegale Inhalte ermöglichen, eingedämmt werden kann. Darunter sind technische Vorkehrungen zu verstehen, die es dem Nutzer verunmöglichen, weiterhin auf diese Seiten zuzugreifen. Vielfach diskutiert werden vor allem DNS- und IP-Sperren. Die Antwort auf diese Frage ist neben ihrer rechtspolitischen Bedeutung aber auch für die Urheber von höchster Relevanz, die daran interessiert sind, dass ihre geschützten Werke nicht unautorisiert im Internet zugänglich sind. Neben der möglichen Effizienz solcher Maßnahmen, ging es also darum zu klären, auf welcher rechtlichen Grundlage und durch wen solche Sperren überhaupt durchführbar sind. Ein wesentlicher Rechtsakt der Europäischen Union im Bereich des Urheberrechts ist die sog. Informations-Richtlinie[108], die eine grundlegende Harmonisierung der nationalen Rechtsordnungen schuf und in Österreich im Jahr 2003 umgesetzt wurde. Damit wurde eine Bestimmung im österreichischen Urheberrechtsgesetz[109] eingeführt, nach der es Urhebern im Ergebnis möglich ist, Internet Service Provider (ISP) dazu zu verpflichten, den Zugriff der Nutzer zu solchen Piraterie-Websites[110] zu verhindern. Es reicht dafür aus, wenn der ISP den bloßen Zugang zur illegalen Quelle ermöglicht, ohne eine weitergehende Verbindung zum Betreiber dieser Quelle zu haben. Diese Rechtslage wurde bereits vom Europäischen Gerichtshof[111] und dem Obersten Gerichtshof[112] in Österreich bestätigt. ISP sind also angehalten, nach Aufforderung durch den Rechtsinhaber solche Seiten zu sperren. Unklar bleibt aber nach der derzeitigen Rechtslage, unter welchen (formalen) Voraussetzungen und in welcher Form diese Sperren erfolgen sollen.

[108] RL 2001/29/EG.
[109] § 81 Abs 1a UrhG.
[110] Nämlich Websites, die strukturell rechtsverletzende Inhalte zur Verfügung stellen.
[111] EuGH Rs C-314/12.
[112] OGH 24.06.2014, 4Ob71/14s; OGH 21.10.2014, 4 Ob 140/14p; OGH 19.05.2015, 4Ob22/15m.

4.4.3.2 Worin besteht das Problem?

Netzsperren sind aus vielerlei Gründen heftig umstritten: Zunächst wurde rechtlich bislang nicht geklärt, welche Form von Netzsperre durch die ISP ausreichend ist, um der Verpflichtung nachzukommen. Eine DNS-Sperre kann relativ leicht umgangen werden, während mit einer (weniger leicht umgehbaren) IP-Sperre weitergehende Eingriffe in die Struktur verbunden sind, die auch andere Websites betreffen können, deren Inhalte im Gegensatz zur Piraterie-Seite völlig legal sind. Damit sind aber im selben Atemzug auch wesentliche Grundrechte (Recht auf Meinungsfreiheit der Betreiber, Informationsfreiheit der Nutzer, Berufsfreiheit der ISP) betroffen. Umfassen die Maßnahmen auch die Filterung des Datenverkehrs, verletzen sie das Kommunikationsgeheimnis und sind somit auch datenschutzrechtlich höchst problematisch.[113] Es stellt sich somit die grundsätzliche Frage, ob diese möglichen Grundrechtseingriffe im Verhältnis zu dem damit bezweckten Ergebnis solcher Sperren stehen – nämlich diese Form der Kriminalität im Internet zu verhindern oder wenigstens zu reduzieren.

Ebenso ist fraglich, ob die derzeit diskutierten Sperrmodelle, die wie das gesamte Internet einem stetigen technischen Wandel unterliegen, auch in einigen Jahren noch der Rechtslage entsprechen können.

Neben gut argumentierten Meinungen gelangen auch mehrere Studien[114]zu dem Ergebnis, dass Netzsperren zur effizienten Verhinderung der Verbreitung von illegalen Inhalten im Internet (z.B.: urheberrechtlich geschützten Werke, Kinderpornografie) ungeeignet sind, da sie regelmäßig technisch umgangen werden können und zudem keine Nachhaltigkeit aufweisen: Vielmehr führen sie derzeit zu einem sog Hydra-Effekt, wonach die gesperrte Website in Kürze durch zahlreiche "Klonseiten" mit denselben illegalen Inhalten ersetzt wird. Dies liegt auch darin begründet, dass die relevanten Dateien, die über die Website abrufbar sind, in der Regel auf verschiedenen Servern gespeichert sind und durch die Website nur eine leicht zu ersetzende Verbindung zu diesen Dateien ermöglicht wird. Handelt es sich gar um eine „Piraterie-Software", die direkt am Rechner installiert wird und von dort den Zugriff auf BitTorrent-Verzeichnisse mit illegalen Inhalten ermöglicht, gibt es auch keine Website mehr, die man sperren könnte.[115]

---

[113] Vgl. die Rechtslage in Deutschland, http://www.welt.de/wirtschaft/webwelt/article144652893/Muessen-Internetanbieter-illegale-Seiten-sperren.html (2.11.2015).

[114] ZB die von der EU-Kommission in Auftrag gegebene Studie: Online Copyright Enforcement, Consumer Behavior, and Market Structure (2015), abrufbar unter http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2604197 (02.11.2015)).
Studie: Clickonomics: Determining the Effect of Anti-Piracy Measures for One-Click Hosting (2013), abrufbar unter http://www.internetsociety.org/sites/default/files/07_1_0.pdf (01.07.2015)).

[115] So z.B.: die Software „Popcorn Time", http://derstandard.at/2000021562821/Sinnlose-Netzsperren-gegen-Popcorn-Time (01.07.2015).

4.4.3.3 Was bedeutet die Schaffung einer "Sperrinfrastruktur"?

Die derzeit unklare Rechtslage in Bezug auf die Art der Sperren und deren jedenfalls fragwürdige Effizienz führen zu Unsicherheiten auf Seiten aller (wirtschaftlich) Beteiligten. Während Urheber an einer klaren rechtlichen Handhabe gegen die Verletzung ihrer Rechte interessiert sind, lehnen ISP ihre Rolle als Mitverantwortliche unter anderem mit dem Argument ab, dass sie lediglich eine neutrale Infrastruktur zur Verfügung stellen. Berücksichtigt man die internationalen Entwicklungen der letzten Jahre, zeichnet sich aber eine zunehmende Etablierung von Sperrverfahren ab. Neben gesetzlichen Bestimmungen gibt es auch Kooperationen zwischen ISP und Rechteinhabern, wie etwa im Fall des sog Graduated Response System (GRS) oder "Three Strikes System". Hier erhält der ISP von Urhebern Informationen über die rechtsverletzenden Seiten und mahnt seine Kunden schriftlich in einem 3-Schritte-Verfahren ab, wenn diese auf den genannten Seiten aktiv sind. Im Fall des Zuwiderhandelns sind Sanktionen wie z.B.: die Reduktion der Netzwerkbandbreite, das Sperren der betroffenen Seiten oder die (temporäre) Sperre des Kundenzugangs vorgesehen. Der Irish High Court Commercial hat – weltweit erstmalig – die Implementierung eines solchen Systems im Wege einer einstweiligen Verfügung gegen einen ISP im Frühjahr des Jahres 2015 angeordnet.[116]

Es wird deutlich, dass all diese Möglichkeiten mehr oder weniger intensive Eingriffe in die Struktur des Internets durch die ISP erfordern und in unterschiedlicher Ausprägung auch die Kontrolle und Beobachtung des Nutzerverhaltens durch diese voraussetzen. ISP sind nach Unionsrecht aber nicht dazu verpflichtet, die von ihnen generierten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen.[117]

4.4.3.4 Mehr Daten – mehr Missbrauchspotential

Durch solche Verfahren wird zudem eine neue Infrastruktur geschaffen, die einen zusätzlichen Pool an Daten beinhaltet, die dem ISP – zumindest temporär – zur Verfügung stehen. Dabei kann es sich um Daten handeln, deren Herausgabe der Staat nach den Bestimmungen des Telekommunikationsgesetzes (TKG), der Strafprozessordnung (StPO), des Sicherheitspolizeigesetzes (SPG) oder des Polizeilichen Staatsschutzgesetzes PStSG) vom ISP verlangen kann. Eine de facto Verschärfung von überwachenden Maßnahmen passiert daher nicht immer zwingend im Kernbereich des Staatsschutzes. Vielmehr sind die Verstrickungen vielfältig und im Fall der Netzsperren auf das Urheberrecht, das dem Schutz von geistigen Schöpfungen dient, zurückzuführen. Dennoch: Das Missbrauchspotential ist dabei stets gegeben.

[116] Vgl. http://www.irelandip.com/2015/04/articles/intellectual-property/high-court-orders-upc-to-take-action-against-illegal-downloaders/ (01.07.2015)).
[117] § 18 Abs 1 ECG.

4.5 Verkehrsbewegungen

4.5.1 Straßenverkehrs-Maut und staatliche Überwachung

Das Risiko einer umfassenden staatlichen Überwachung im Straßenverkehr hat zugenommen und verdient in der rechtspolitischen Debatte soweit es um Datenschutz geht, große Aufmerksamkeit. Für Frachtunternehmen bestehen zwar schutzwürdige Geheimhaltungsansprüche im Hinblick auf Geschäftsgeheimnisse sowie die personenbezogenen Daten betroffener Mitarbeiter. Wirkliches Gewicht bekommen die Datenschutzfragen in der Mautdebatte aber erst durch die potentiell drohende Dimension einer flächendeckenden Überwachung des PKW-Verkehrs zum Zwecke (und möglicherweise Vorwand) einer flächendeckenden PKW Maut.

Wenngleich dies ein Szenario ist, gegen welches Vorkehrungen getroffen werden sollten, ist zu bedenken, dass das Thema einer PKW Maut im Hinblick auf Datenschutz im Straßenverkehr angesichts der jüngsten Entwicklungen höchstens ein Nebenschauplatz ist. Hier ist vor allem das Auto-Notruf-Konzept „E-Call" angesprochen, dass ab 31. März 2018 für alle neuen PKW Modelle verpflichtend zu implementieren ist. Die infrastrukturseitige Umsetzung ist in Österreich dazu voll im Gange.[118] Durch das „E-Call" Notrufsystem wird jeder PKW potentiell ständig lokalisierbar, wobei die Nutzer die entsprechende Funktion auch nicht abschalten können, wie dies in der Debatte im EU Parlament vor der Abstimmung noch als Einschränkung gefordert wurde. Das System wurde politisch von einigen Seiten als nicht notwendige anlasslose Überwachung des gesamten Autoverkehrs abgelehnt.[119] In der Umsetzung ist nun besonders darauf Bedacht zu nehmen sein, dass die strenge Zweckbindung und Beschränkung auf Notrufträger in der technischen Umsetzung effektiv abgesichert wird. Dies schützt freilich nicht vor späteren rechtspolitischen Begehrlichkeiten, ein einmal etabliertes System wie den „E-Call" gesetzlich für andere, ursprünglich nicht vorgesehene Zwecke zu erweitern. Insofern ist auch nicht auszuschließen, dass in einer späteren Debatte über ein flächendeckendes PKW Mautsystem die Forderung erhoben werden könnte, auf dem bald ausgerollten „E-Call" System aufzusetzen.

Hinzu kommt die generelle Entwicklung in der Autoindustrie und in der Verkehrsplanung, durch den Einsatz von „e-connected Cars" sowohl die Verkehrsentwicklung als auch die Sicherheitsrisiken im Straßenverkehr positiv zu beeinflussen. Hierzu werden Fahrzeuge in absehbarer Zukunft über Schnittstellen verfügen, die sowohl eine Kommunikation von Fahrzeugen untereinander („Car-to-Car") als auch mit der Infrastruktur („Car-to-X") ermöglichen sollen. Unter Einsatz moderner „Big-Data" Analysemethoden sollen interaktive Verkehrsleitsysteme in Echtzeit an aktuelle Bedingungen angepasst und so die

[118] Siehe die Details unter http://www.e-call.at/ (20.5.2016).
[119] ZB http://derstandard.at/2000014982338/Autonotruf-eCall-verpflichtend-ab-2018-in-alle-neue-Pkw (20.5.2016).

Verkehrsbelastung optimal verteilt werden. Die Datenerfassung im Rahmen solcher Systeme, die längst keine ferne „Science Fiction" mehr sind, geht weit über das hinaus, was im Rahmen eines Mautsystems typischerweise erfasst werden soll. Zusammenfassend lässt sich daher zu diesem Datenschutz-Risiko feststellen, dass die Gefahr einer flächendeckenden Überwachung durch die Entwicklungen zum Notrufsystem „E-Call" sowie die Entwicklung zu „Smart Traffic" und „Smart City" weitaus größer, naheliegender und konkreter ist, als eine Ausdehnung eines flächendeckenden LKW-Mautsystems auf PKW.

Zweckbindung (§ 6 DSG)

Der Grundsatz der Zweckbindung ist eine zentrale Säule des Datenschutzes und spielt auch bei der Verarbeitung von Daten, welche durch die im Folgenden beschriebenen Technologien ermittelt werden, eine große Rolle. Ein potentielles Risiko stellt die Zweckentfremdung dar. Dabei lässt sich eine mögliche Zweckentfremdung in verschiedene Szenarien zu unterscheiden:

- Externer Angriff unter Ausnützung von Datensicherheitslücken
- Interner Missbrauch unter Ausnützung von organisatorischen Schwachstellen
- Gesetzlich legalisierter Zugriff auf Mautdaten außerhalb des Mautsystems

Gegen die ersten beiden Szenarien können und müssen in der Umsetzung eines Mautsystems effektive technische und organisatorische Maßnahmen vorgesehen werden. Hier gibt es in der österreichischen Verwaltung durchaus einen großen Erfahrungsschatz und Konzepte, auf die man zurückgreifen kann. Vor allem ist hier die „**Portalverbund-Vereinbarung**" von Bund und Ländern zu nennen. Dort sind verschiedene Sicherheitsklassen und eine Sicherheitsarchitektur für die Vergabe von Berechtigungen definiert, die sich in der Praxis in vielen Fällen als effektiv erwiesen haben.[120]

Schwieriger ist aber der Umgang mit dem letzten genannten Risiko, einer Zweckentfremdung auf Basis anderer Gesetze, die mit der Mauterhebung selbst nichts zu tun haben. Angesprochen sind damit insbesondere Datenauskunftspflichten nach der Strafprozessordnung, dem Sicherheitspolizeigesetz, dem polizeilichen Staatsschutzgesetz oder auch nach der Zivilprozessordnung im Rahmen eines Zivilverfahrens. Hier müssen von vornherein klare Regeln und Grenzen aufgestellt werden, um einen „gesetzlich legitimierten Missbrauch" von Beginn an zu verhindern. Beim Terminus „Missbrauch" ist in diesem Zusammenhang natürlich Zurückhaltung geboten, weil es vor allem um jene Fälle geht, wo mangels klarer gesetzlicher Regelungen Graubereiche bestehen.

[120] Vgl. z.B.: die Umsetzung der Durchlaufstelle (DLS) unter Nutzung der Portalverbund-Strukturen zur Abwicklung von Auskünften an Strafverfolgungs- und Sicherheitsbehörden durch Telekommunikationsunternehmen.

4.5.2 Section-Control

Parlamentarische Anfrage 4089J
*) An wie vielen Standorten waren wie viele Einrichtungen für Section Control jeweils in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 im Einsatz?
*) Werden Systeme der Section Control für andere Zwecke als zur Geschwindigkeitsüberwachung eingesetzt?
Wenn ja, für welche Zwecke?
*) Wie wird im Verantwortungsbereich des Ministeriums sichergestellt,
dass Unbefugte keinen Zugriff auf Daten der Section Control haben und erlangen können?
*) Wie lange werden die Aufzeichnungen von Verkehrskameras zur Stauerkennung aufbewahrt?
*) Welche Stellen haben Zugriff auf die Aufzeichnungen der Verkehrskameras zur Stauerkennung?

Parlamentarische Beantwortung – IST-Stand Österreich
Antwort 4089J:
Ich darf hierzu auf folgende Aufstellung verweisen:
- BGBl. II Nr. 169/2007 v. 16.07.2007 (Section Control-Messstreckenverordnung Wechselabschnitt), i.d.F. BGBl. II Nr. 429/2008)
- BGBl. II Nr. 168/2007 v. 16.07.2007 (Section Control-Messstreckenverordnung Kaisermühlentunnel)
- BGBl. II Nr. 264/2008 v. 22.07.2008 (Section Control-Messstreckenverordnung Laßnitzhöhe 2008), aufgehoben durch BGBl. II Nr. 75/2009 v. 18.03.2009
- BGBl. II Nr. 179/2009 v. 19.06.2009 (Section Control-Messstreckenverordnung Graz Ost): baustellenbedingte Section Control-Anlage; Verordnung zwar noch nicht formell aufgehoben, aber seit Oktober 2009 abgebaut und daher nicht mehr aktiv
- BGBl. II Nr. 247/2009 v. 29.07.2009 (Section Control-Messstreckenverordnung Ehrentalerbergtunnel), aufgehoben durch BGBl. II Nr. 339/2013
- BGBl. II Nr. 440/2009 v. 15.12.2009 (Section Control-Messstreckenverordnung Pichl): baustellenbedingte Section Control-Anlage; Verordnung zwar noch nicht formell aufgehoben, aber seit September 2010 abgebaut und daher nicht mehr aktiv
- BGBl. II Nr. 421/2010 v. 14.12.2010(Section Control-Messstreckenverordnung Amras): baustellenbedingte Section Control-Anlage; Verordnung zwar noch nicht formell aufgehoben, aber seit Dezember 2011 abgebaut und daher nicht mehr aktiv
- BGBl. II Nr. 229/2011 v. 21.07.2011 (Section Control-Messstreckenverordnung Hanssonkurve): baustellenbedingte Section Control-Anlage; Verordnung zwar noch nicht formell aufgehoben, aber seit September 2012 abgebaut und daher nicht mehr aktiv
- BGBl. II Nr. 321/2011v. 03.10.2011 (Section Control-Messstreckenverordnung Plabutsch Tunnel) • BGBl. II Nr. 168/2012 v. 25.05.2012 (Section Control-Messstreckenverordnung Ybbs): baustellenbedingte Section Control-Anlage; Verordnung zwar noch nicht formell aufgehoben, aber seit Oktober 2012 abgebaut und daher nicht mehr aktiv • BGBl. II Nr. 370/2012 v. 09.11.2012 (Section Control-Messstreckenverordnung Aistersheim-Weibern), aufgehoben durch BGBl. II Nr. 59/2013 v. 22.02.2013
- BGBl. II Nr. 59/2013 v. 22.02.2013 (Section Control-Messstreckenverordnung Aistersheim-

Weibern 2013) • BGBl. II Nr. 208/2013 v. 12.07.2013 (Section Control-Messstreckenverordnung Bosrucktunnel) • BGBl. II Nr. 339/2013 v. 08.11.2013 (Section Control Messstreckenverordnung Ehrentalerbergtunnel 2013)
• BGBl. II Nr. 338/2013 v. 08.11.2013 (Section Control-Messstreckenverordnung Nordumfahrung Klagenfurt)
• BGBl. II Nr. 282/2014 v. 10.11.2014 (Section Control-Messstreckenverordnung Weibern-Haag 2014)
• BGBl. II Nr. 287/2014 v. 13.11.2014 (Section Control-Messstreckenverordnung Hummelhof 2014)

Werden Systeme der Section Control für andere Zwecke als zur Geschwindigkeitsüberwachung eingesetzt? Wenn ja, für welche Zwecke? Nein.

Wie wird im Verantwortungsbereich des Ministeriums sichergestellt, dass Unbefugte keinen Zugriff auf Daten der Section Control haben und erlangen können?

Der Bundesminister für Verkehr, Innovation und Technologie legt per Verordnung lediglich mittels Section Control überwachte Messstrecken auf Autobahnen fest; für darüberhinausgehende Aspekte der Vollziehung der StVO (wie etwa die Anordnung eines Einsatzes von Section Control) sowie für Messstrecken auf anderen Straßen sind gemäß Art. 11 B-VG die Länder zuständig. Im Sinn des Datenschutzgesetzes ist der Bundesminister für Verkehr, Innovation und Technologie daher auch nicht Auftraggeber für die im Rahmen einer Verkehrsüberwachung mittels Section Control stattfindenden Datenverarbeitung, und es besteht auch kein Zugriff auf im Rahmen einer solchen Überwachung verarbeitete Daten. Die ASFINAG errichtet auf dem hochrangigen Straßennetz Section Control Anlagen und stellt die Verfügbarkeit der Anlagen sicher, die datenschutzrechtlichen Auftraggeber dieser betriebenen Anlagen sind jedoch die jeweils zuständigen Verkehrsbehörden. Sämtliche im Rahmen von Section Control Anlagen ermittelten Daten werden unmittelbar nach deren Ermittlung noch innerhalb der jeweiligen Section Control Anlage verschlüsselt („End to End – Verschlüsselung“). Die jeweils zuständigen Verkehrsbehörden verfügen in ihrer Eigenschaft als datenschutzrechtliche Auftraggeber über die notwendigen Schlüssel.

Wie lange werden die Aufzeichnungen von Verkehrskameras zur Stauerkennung aufbewahrt? Übereinstimmend mit § 98f Abs. 3 StVO werden die Daten der zur Verkehrsbeobachtung eingesetzten Kameras gar nicht gespeichert. Ausgenommen davon sind Fälle, in denen gemäß § 98f Abs. 3 letzter Satz StVO für Zwecke der Information der Öffentlichkeit im Wege von Medien im Bedarfsfall auf Anfrage manuell einzelne Bildquellen ausgewählt und daraus kurze Bildfolgen gespeichert und an Medien übermittelt werden. Dabei wird sichergestellt, dass eine Identifizierung von Personen oder Fahrzeugen nicht möglich ist. Die zur Erkennung von Verkehrsstörungen in Tunnelanlagen ermittelten Videodaten werden im Sinn des § 4 Abs. 5 Z 6 Straßentunnel-Sicherheitsgesetz (STSG) grundsätzlich spätestens nach Ablauf von 72 Stunden gelöscht, sofern im Einzelfall nicht die Voraussetzungen einer maximal dreijährigen Speicherung im Sinn des § 4 Abs. 5 Z 7 STSG vorliegen. Auf Rastplätzen erfolgt die Speicherung für 48 Stunden auf Basis einer Meldung an die Datenschutzbehörde. Danach werden die Daten automatisiert überschrieben.

Welche Stellen haben Zugriff auf die Aufzeichnungen der Verkehrskameras zur

> Stauerkennung? Die zur Verkehrsbeobachtung auf dem hochrangigen Straßennetz eingesetzten Videokameras werden nach Maßgabe des § 98f StVO, die in Tunnelanlagen zur Erkennung von Verkehrsstörungen eingesetzten Videokameras nach Maßgabe des § 4 Abs. 5 STSG betrieben. Nach Maßgabe dieser Regelungen zulässigerweise gespeicherte Videodaten werden im Sinn des § 98f Abs. 3 letzter Satz StVO bzw. des § 4 Abs. 5 Z 8 STSG fallweise an anfragende Medien übermittelt. Sonstige Übermittlungen von zulässigerweise gespeicherten Daten an Behörden oder Betroffene finden ausschließlich auf Grundlage der jeweils einschlägigen gesetzlichen Bestimmungen – wie z.B. § 110 Abs.1 oder § 99 Abs. 3 StPO - statt.
>
> Der Begriff Abschnittskontrolle bezeichnet ein System zur Überwachung von Tempolimits im Straßenverkehr, bei dem nicht die Geschwindigkeit an einem bestimmten Punkt gemessen wird, sondern die Durchschnittsgeschwindigkeit über eine längere Strecke. Dies geschieht mit Hilfe von zwei Überkopfkontrollpunkten, die mit Kameras ausgestattet sind. Das Fahrzeug wird sowohl beim ersten wie auch beim zweiten Kontrollpunkt fotografiert. Die Identifizierung der Fahrzeuge erfolgt anhand des Kfz-Kennzeichens mittels automatischer Nummernschilderkennung. Aufgrund der benötigten Zeit zwischen den beiden Kontrollpunkten wird eine Durchschnittsgeschwindigkeit ermittelt. Liegt diese über der erlaubten Höchstgeschwindigkeit, erfolgt eine automatische Weiterleitung der ermittelten Daten an die Exekutive. [121]

Der VfGH behandelte in seiner Entscheidung G 147/06 uA datenschutzrechtliche Fragen iZm der Section Control. Auftraggeber der Section Control ist die für die Verkehrspolizei zuständige Behörde. Im Falle einer Section Control in Wien, wäre dies die Wiener Landesregierung. Diese muss die Datenanwendung auch bei der Datenschutzkommission melden. Da nur das Heck eines Fahrzeuges fotografiert wird, ist die fahrende Person somit nicht erkennbar. Nur mit einem Verzeichnis der Zulassungsbesitzer kann eine Person identifiziert werden. Diese Zusammenführung von Daten kann nicht durch den Auftraggeber der Section Control erfolgen, sondern ausschließlich durch die Verwaltungsstrafbehörde nach Abrufen der Übertretungsdatensätze. Somit handelt es sich bei den Daten um indirekt personenbezogene Daten. *Gemäß §7 Abs1 DSG 2000 dürfen Daten nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.* Die Zuständigkeit ergibt sich aus §94a Abs 1 iVm §94 b Abs 1 lit a StVO. *Die schutzwürdigen Geheimhaltungsinteressen der Betroffenen sind gemäß § 8 Abs 2 DSG 2000 nicht verletzt, da im System 'Section Control' nur indirekt personenbezogene Daten verwendet werden.* Grundsätzlich dürfen die verarbeiteten Daten nur für den Zweck verwendet werden, für den sie ermittelt wurden (§ 6 Abs 1 Z 2 und Z 3 DSG). Sollten die Daten für andere Zwecke verwendet werden, so handelt es sich um eine Übermittlung iSd § 4 Z 12 DSG). Des Weiteren dürfen Daten gem. § 6 Abs 1 Z 5 DSG *nur solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung*

[121] https://de.wikipedia.org/wiki/Abschnittskontrolle.

der Zwecke, für die sie ermittelt wurden, erforderlich ist. Sobald Daten für den Zweck der Datenanwendung nicht mehr benötigt werden, gelten sie gemäß § 27 Abs 1 (vierter Satz) DSG 2000 als unzulässig verarbeitete Daten und sind zu löschen. Ergibt die Geschwindigkeitsmessung also, dass die zulässige Höchstgeschwindigkeit nicht überschritten wurde, so werden die Daten nicht weiter benötigt und sind daher umgehend zu löschen. Dem wird vom System der 'Section Control' entsprochen: Die zwischengespeicherten Daten werden gelöscht, sobald festgestellt wurde, dass keine Überschreitung der zulässigen Höchstgeschwindigkeit vorliegt. Darüber hinaus werden die Daten auch gelöscht, wenn ein Zeitfenster von acht Minuten überschritten ist, ohne dass eine Übertretung erkannt wurde.

Zusammenfassend erfordert eine verfassungskonforme Section-Control folgende Vorrausetzungen im Sinne der Begründung des VfGH:[122]
1) All jene Daten, aus denen kein Vorwurf der Geschwindigkeitsübertretung abgelesen werden kann, sind unverzüglich zu löschen.
2) Die Überwachung einer "bestimmten Wegstrecke" mittels eines automatischen Geschwindigkeitsmesssystems ist nur dann erlaubt, wenn diese Wegstrecke räumlich und möglichst auch zeitlich genau definiert ist. Der überwachte Abschnitt darf nicht beliebig gewählt werden, sondern muss eine besondere Notwendigkeit der Überwachung, also eine besondere Gefahrensituation, aufweisen.
3) Jede "bestimmte Wegstrecke", die per Section Control überwacht werden soll, muss vom Verkehrsminister durch Verordnung, die die oben genannten Kriterien erfüllt, angeordnet werden. Die Datenerhebung muss für die betroffenen Kraftfahrer vorhersehbar sein und allenfalls auch angefochten werden können.

4.5.3 Autobahn-Maut (GoBox)

Die GO-Box ist ein elektronisches Gerät, das zur Entrichtung der fahrleistungsabhängigen Lkw-Maut in Österreich seit 1. Januar 2004 benötigt wird. Ohne GO-Box kann die vorgeschriebene Maut nicht entrichtet werden. Bei nicht ordnungsgemäßer Entrichtung der Lkw-Maut wird eine Ersatzmaut in Höhe von EUR 240,00 fällig. Zur Feststellung von Mautprellern gibt es sowohl Kontrollen durch die Exekutive und durch Mautaufsichtsorgane der ASFINAG-Maut-Service-GesmbH als auch ein automatisches kamerabasiertes Kontrollsystem. Gemäß § 6 Bundesstraßen-Mautgesetz 2002 (BStMG), BGBl I 2002/109, unterliegt die Benützung von Mautstrecken mit mehrspurigen Kraftfahrzeugen, deren höchstzulässiges Gesamtgewicht mehr als 3,5 t beträgt, der fahrleistungsabhängigen Maut. Deren Höhe richtet sich nach der Anzahl der Achsen der Kraftfahrzeuge und der von diesen gezogenen Anhängern (§ 9 Abs 2 BStMG). Die Entrichtung der Maut erfolgt grundsätzlich auf elektronischem Weg (§ 7 Abs 1 BStMG). Zu

[122] Siehe dazu Öhlböck, Section Control rechtswidrig, Online-Beitrag vom 15.7.2007 unter http://www.rechtsfreund.at/news/index.php?/archives/67-Section-Control-rechtswidrig.html (11.8.2016).

diesem Zweck wird den mautpflichtigen Straßenbenützern im Zuge der Anmeldung zum Mautsystem leihweise ein Gerät („GO-Box") zur Verfügung gestellt, das im mautpflichtigen Kraftfahrzeug anzubringen und auf dem die Achsenzahl einzustellen ist.[123] In dem vorher zitierten schadensersatzrechtlichen Zivilprozess wurde aus datenschutzrechtlichen Gründen der Zugang zu Go-Box Daten zwecks Ausforschung des Schädigers verneint. Begründet wurde dies damit, dass *die Möglichkeit, den - im Strafverfahren nicht ausforschbaren - Schädiger mit Hilfe der im Mautsystem gespeicherten Daten ausforschen zu können, bloße Spekulation bleibt, ist doch nicht einmal bekannt, ob der Schädiger tatsächlich mit einem mit einer „GO-Box" ausgestatteten Kraftfahrzeug fuhr.*

Zum Zugriff auf „GO-Box" Daten im Rahmen eines strafrechtlichen Ermittlungsverfahrens gibt es keine ausdrücklichen Rechtsgrundlagen und es findet sich dazu auch keine Judikatur im Rechtsinformationssystem des Bundes (RIS). Entsprechende Auskunftsbegehren an die ASFINAG sind aber grundsätzlich im Rahmen der Amts- und Rechtshilfe gemäß § 76 StPO zulässig. Allerdings ist im Einzelfall die Frage zu klären, ob im bestehenden LKW-Mautsystem eine Datenauskunft durch ein Gericht oder die Staatsanwaltschaft nach der Strafprozessordnung (StPO) als „automationsunterstützter Datenabgleich" im Sinne des § 141 StPO (vulgo **„Rasterfahndung"**) zu sehen ist. Hier ist wohl zu differenzieren: Die Nachfrage nach einem bestimmten, bereits identifizierten Fahrzeug wäre eine konkrete Auskunft, die nicht unter § 141 StPO fällt und nach § 76 StPO zu erteilen ist. Wenn jedoch nur nach einigen Kriterien wie z.B.: Zeit und Fahrtroute ein gesuchtes Fahrzeug erst identifiziert werden soll, indem ein Abgleich mit allen Daten im Mautsystem vorgenommen wird, wäre dies jedenfalls eine „Rasterfahndung", die den Beschränkungen des § 141 StPO unterliegt.

4.5.4 Automatisierte Kennzeichenerkennung

Parlamentarische Anfragen 4089J
*) Welche Datenarten bzw. Kategorien von Datenarten werden bei einem Einsatz einer automatisierten Kennzeichenerkennung erhoben?
*) Wie hoch ist die Fehlerrate bei der automatisierten Kennzeichenerkennung?
*) Welche Vorkehrungen werden getroffen um die Daten von unbeteiligten Dritten im Einsatzgebiet einer automatisierten Kennzeichenerkennung zu schützen?
*) Wie lange werden Kennzeichen von Fahrzeugen, die Übertretungen begangen haben, gespeichert? An welche Stellen wird diese Information weitergegeben?
*) Wie lange werden Kennzeichen von Fahrzeugen, die keine Übertretung begangen haben, gespeichert? An welche Stellen wird diese Information weitergegeben?
*) In wie vielen Fällen haben Polizeibehörden auf Daten automatisierter Kennzeichnungserkennungsgeräte gemäß § 54 Abs. 4b SPG für den Zweck der Fahndung in den Jahren 2009, 2010, 2011, 2012, 2013 und 2014 jeweils zugegriffen?

[123] OGH 14.08.2008, 2Ob178/07a.

Parlamentarische Beantwortung – IST-Stand Österreich
Antwort 4089J:
Section Control-Anlagen haben – wie auch alle anderen Systeme zur Verkehrsüberwachung – keine „automatisierte Kennzeichenerkennung". Sie dienen ausschließlich der automatisierten Feststellung einer Übertretung der Straßenverkehrsordnung. Ich verweise hinsichtlich der Speicherung von Bilddokumenten, die mittels automatisierter Überwachungssysteme wie etwa Section Control generiert wurden, auf die §§ 98a ff. der Straßenverkehrsordnung.

Bei der automatisierten Kennzeichenerkennung handelt es sich um eine Videoüberwachungsmethode, die Schrifterkennung (OCR - *optical character recognition*) nutzt, um Kfz-Kennzeichen an Fahrzeugen zu erkennen. Dazu werden entweder fest installierte Videoüberwachungskameras, Foto- und Videokameras in Geschwindigkeitsmessanlagen oder speziell dafür aufgestellte mobile Geräte genutzt. Derartige Systeme werden von Behörden zur automatischen Beweisführung bei der Erhebung von Mautgebühren und zur Verkehrsüberwachung (etwa Geschwindigkeits- und Abstandsmessungen oder Einhaltung des roten Lichtzeichens an ampelgeregelten Kreuzungen) eingesetzt.

Ein technisch taugliches System kann sowohl die aufgenommenen Bilder speichern als auch den erkannten Text auslesen, teilweise zusätzlich ein Foto des Fahrers speichern.
Üblicherweise wird zur Ausleuchtung infrarotes Licht eingesetzt, um unabhängig von der Tageszeit Aufnahmen machen zu können. Die Systeme verwenden auch Blitzlicht, um einerseits die Bildqualität zu steigern und andererseits dem Fahrer sein Fehlverhalten zu signalisieren. Eingesetzte Systeme unterscheiden sich im Detail, insbesondere aufgrund länderspezifischer Unterschiede in den benutzten Nummernschildern.

Die Systeme werten entweder an Ort und Stelle aus oder es werden Fotos gesammelt und an ein ausgelagertes Rechnersystem gesendet, wo die Erkennung zeitversetzt stattfindet.[124]

Die in Österreich von der ASFINAG verwendeten Geräte können die Anzahl der Achsen eines LKW zählen, die korrekte Anbringung der GO-BOX kontrollieren, sowie ein Foto von der Windschutzscheibe und ein seitliches Foto

124 https://de.wikipedia.org/wiki/Automatische_Nummernschilderkennung (01.07.2016)).

(schwarz/weiß) machen um die korrekte Zahlung der Mautgebühr zu bestimmen.

Die Geräte des Innenministeriums werden entweder mobil oder stationär eingesetzt. Die Kennzeichen der vorbeifahrenden Kraftfahrzeuge werden automatisch erfasst und verschlüsselt mit dem Fahndungsdatenbestand des EKIS abgeglichen. Bei einem "Treffer" werden die Fahndungsdaten an die Polizei übermittelt und auf ihre Richtigkeit überprüft. Ist das Fahrzeug als gestohlen gespeichert, wird die Fahndung veranlasst.
Wenn nicht, wird der Datensatz sofort gelöscht.[125]

4.5.5 Rechtsgrundlagen im Überblick

Grundsätzlich gelten für die oben beschriebenen Technologien die gesamten Rechtsmaterien und im Besonderen:

- **Straßenverkehrsordnung (StVO):** § 98a ff. StVO – Besondere Vorschriften für die Verkehrsüberwachung mittels bildverarbeitender technischer Einrichtungen
- **Straßentunnel-Sicherheitsgesetz (STSG):** § 4 STSG – Aufgaben des Tunnel-Managers
- **Strafprozessordnung (StPO):** § 141 ff. StPO – Automationsunterstützter Datenabgleich
- **Datenschutzgesetz 2000 (DSG 2000):** § 6 DSG 2000 – Grundsätze; § 7 DSG 2000 – Zulässigkeit der Verwendung von Daten

4.6 Reisebewegungen

4.6.1 Passenger Name Record (PNR)

Parlamentarische Anfrage 4014/J (XXV. GP) BMI

1. Wie sehen die genauen Zielvorgaben, auch in zeitlicher Hinsicht, des Projektes im Rahmen des ISEC Programmes aus?
2. Gibt es Partner in diesem Projekt?
    a. Wenn ja, welche?
3. Wie und von wem wird die Datenschutzkonformität überprüft?
4. Wie wird das Grundrecht auf Privatsphäre und der Rechtsschutz Betroffener in diesem Projekt berücksichtigt?

125 http://www.bmi.gv.at/cms/BMI/_news/BMI.aspx?id=49424B594B6E47574C664D3D&page=0&view=1 – 29.07.2015.

5. Welche konkreten Datenbanken sollen an die PNR Datenbank angebunden werden?
6. Existiert eine österreichische PNR Datenbank zum aktuellen Zeitpunkt?
    a. Wenn ja, ist sie mit anderen europäischen Datenbanken verbunden?
    b. Wenn nein, ist eine solche österreichische PNR Datenbank in Planung? Wenn ja, wie ist der genaue Zeitplan?
7. Auf welcher rechtlichen Grundlage erfolgte die Einrichtung einer PNR Datenbank und die Anbindung von anderen Datenbanken, bzw. auf welcher rechtlichen Grundlage sollen diese erfolgen?
8. Von welchen Daten, die in der österreichischen PNR Datenbank gesammelt werden, geht das Projekt aus?

Parlamentarische Beantwortung 4014/J (XXV. GP) BMI – IST-Stand Österreich

Zu den Fragen 1, 2 und 5:
An diesem ISEC-Projekt nehmen neben Österreich noch folgende Mitgliedstaaten teil:
Bulgarien, Estland, Finnland, Frankreich, Lettland, Litauen, Niederlande, Italien, Rumänien, Portugal, Schweden, Slowakei, Slowenien, Spanien, Ungarn und Zypern.
Für jeden der teilnehmenden Mitgliedstaaten sind die Zielvorgaben des Projektes unterschiedlich.
Einige Mitgliedstaten setzen bzw. setzten bereits operative Umsetzungsmaßnahmen (z.B. Bau eines Prototypen, Testbetrieb, etc.). Österreich hat sich im Gegensatz dazu entschieden, lediglich ein theoriebegleitetes Projekt durchzuführen.
Im Fokus dieser Projektarbeit steht die Beantwortung der Frage – sollte es zu einer entsprechenden Richtlinie der Europäischen Kommission kommen – wie eine datenschutzkonforme Anbindung nationaler Datenbanken an eine österreichische Passagier-Informations-Datenbank (Passenger Information Unit - PIU) erfolgen könnte. Das Projektziel ist die Erstellung eines Maßnahmenkatalogs, welcher im Bedarfsfall als Richtschnur für eine spätere Umsetzung herangezogen werden kann. Es werden jedoch keine operativen Maßnahmen gesetzt.
Das Projektende ist mit 30. Juni 2015 festgelegt.

Zu den Fragen 3, 4 und 8:
Eine von der Europäischen Kommission zu erlassende Richtlinie, sowie bei deren Umsetzung auch die einzelnen Mitgliedstaaten, werden sich am Gutachten der Agentur der Europäischen Union für Grundrechte (European Union Agency for Fundamental Rights –FRA) zu orientieren haben.
Die FRA hat für die Mitgliedstaaten eine Leitlinie für die Einführung nationaler Systeme für Fluggastdatensysteme erstellt und veröffentlicht, die zwölf Grundrechtserwägungen enthält.
Es ist eine Liste von Regeln, die zur Wahrung der Grundrechte bei der Einführung nationaler Systeme zur Speicherung von Fluggastdatensätze (Passenger Name Records –

PNR) als Mindestanforderungen zu beachten sind. So sollen die Mitgliedstaaten für klare und strenge Zweckbeschränkungen, verbesserte Mechanismen für den Schutz personenbezogener Daten und eine erhöhte Transparenz des Systems für Passagiere Sorge tragen.
Da die Richtlinie der Europäischen Kommission zur Fluggastdatenspeicherung sich erst im Stadium der Diskussion auf europäischer Ebene befindet, können noch keine Aussagen über deren Inhalte und die notwendige nationale gesetzliche Umsetzung getroffen werden. Eine Fluggastdatenspeicherung kann jedoch nur unter Berücksichtigung der Grundrechtecharta und der Datenschutzrichtlinie sowie unter Bedachtnahme auf die Rechtsprechung der Höchstgerichte erfolgen, womit die Verhältnismäßigkeit und die Achtung der Grundrechte gewahrt bleibt.

Zu den Fragen 6 und 7:
Es gibt mangels entsprechender gesetzlicher Grundlagen keine PNR-Datenbank in Österreich. Damit stellt sich auch die Frage nach der Anbindung anderer Datenbanken nicht.

Parlamentarische Anfrage 4025/J (XXV. GP) BMI

1. Wie viele Anfragen gab es in den Jahren 2009 bis 2014 nach Paragraph §111 FPG? (Bitte um Aufschlüsselung auf Jahre)
2. Bei wie vielen Personen führte diese Abfrage zu einer erweiterten Kontrolle bei der Einreise nach Österreich?
3. Welcher Nationalität gehörten diese jeweils Personen an? (Bitte um Aufschlüsselung auf Jahre)
4. Wie viele dieser Anfragen wurden im Rahmen eines Rechtshilfeersuchens gestellt?
5. Wie lange werden die Daten nach einer Abfrage durch §111 FPG gespeichert?
6. Gibt es einen (teil-)automatisierten Abgleich der Daten, die durch §111 FPG übermittelt wurden mit anderen Datenbanken (z. B. dem Europol Focal Point Travellers oder dem Schengen Informationssystem (SIS, SIS II)?
7. Gibt es für die Abfrage von erweiterten Passagierdaten eine technische Schnittstelle?
    a. Wenn ja, wie ist diese Schnittstelle definiert?
8. Werden PNR-Daten von österreichischen Fluglinien, Reiseveranstaltern oder anderen Anbietern in diesem Bereich an Behörden von Drittstaaten übermittelt?
    a. Wenn ja, erfolgt diese Übermittlung auf Grund einer gesetzlichen Verpflichtung?
    1. Wenn ja, aufgrund welcher gesetzlichen Grundlage erfolgt diese Übermittlung?
    2. Wenn nein, welche andere Rechtsgrundlage besteht für diese Datenübermittlung?

b. Wenn ja, welche Rechtsschutzmechanismen stehen in diesen Fällen den Betroffenen zu Verfügung?

Parlamentarische Beantwortung 4025/J (XXV. GP) BMI – IST-Stand Österreich

Zu den Fragen 1 und 2:
Das Advance Passenger Information System (APIS) stand in den Jahren 2009 bis 2011 noch nicht zur Verfügung.

Jahr	Anfragen gem. § 111 FPG	erweiterte Kontrollen
2012	2663	3
2013	3799	44
2014	109911	164

Zu Frage 3:
Über die Staatszugehörigkeit der angefragten Personen werden keine statistischen Aufzeichnungen geführt.
Zu Frage 4:
Keine.
Zu Frage 5:
Ab Übermittlung der Daten durch die Fluglinie werden sie gemäß Art. 6 der RL 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln, 24 Stunden für Abfragen bereitgehalten und sodann automatisch gelöscht.
Zu Frage 6:
Es findet kein (teil-)automatisierter Abgleich mit anderen Datenbanken statt. Der zuständige Grenzkontrollbeamte führt nach Risikoeinschätzung und auf Grund seiner Erfahrungswerte in Bezug auf einzelne von ihm gesondert auszuwählende Passagiere ausschließlich Abfragen im nationalen „Elektronischen Kriminalpolizeilichen Informationssystem“ (EKIS) sowie im „Schengener Informationssystem der zweiten Generation“ (SIS II) zum Zwecke der Grenzkontrolle durch.
Zu Frage 7:
Die Passdaten werden von den Fluggesellschaften über einen gesicherten Kanal bzw. verschlüsselt dem Bundesministerium für Inneres übermittelt, welches diese Daten den zuständigen Landespolizeidirektionen über eine Intranet-Webanwendung für Zwecke der Grenzkontrolle zur Verfügung stellt. Jede Landespolizeidirektion hat nur auf die Daten Zugriff, die den in ihrem Zuständigkeitsbereich liegenden Flughafen betreffen.
Zu Frage 8:
Vom Bundesministerium für Inneres werden mangels Rechtsgrundlage keine Fluggastdatensätze (Passenger Name Record – PNR) an Behörden von Drittstaaten übermittelt.

Die Vorgangsweise privater Unternehmen fällt nicht in den Vollzugsbereich des Bundesministeriums für Inneres, weshalb darüber keine Aussagen getroffen werden können.

Das Europäische Parlament hat nach einem langen Gesetzgebungsprozess Mitte April 2016 eine neue Richtlinie über die Verwendung von Fluggastdatensätzen (PNR[126]-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität verabschiedet[127], die als Richtlinie EU/2016/681 am 27. April 2016 im Amtsblatt der Europäischen Union veröffentlicht wurde. Die Richtlinie zielt nicht primär auf die Speicherung, sondern auf die Verwendung der entsprechenden Daten ab[128]. Verwendung bedeutet in diesem Zusammenhang die Aufbereitung der (personenbezogenen) Daten für die Strafverfolgung und die Prävention. Das Reiseverhalten von Flugpassagieren soll durch Software (Algorithmen) analysiert werden, indem die bei der Buchung angegebenen Daten mit Daten aus anderen Quellen bzw. Datenbanken betreffend Personen und Gegenstände abgeglichen[129] und möglicherweise Korrelationen gefunden werden. Durch diese Vorgehensweise sollen Entscheidungen der staatlichen Behörden vorbereitet werden, um etwa Personenkontrollen oder längerfristige Überwachungsmaßnahmen an Terrorverdächtigen durchzuführen. Die Mitgliedstaaten sollen die erhaltenen PNR-Daten untereinander und mit Europol[130] austauschen können, wenn dies zur Bekämpfung von Terrorismus und schwerer Kriminalität als erforderlich erachtet wird[131].
Auch wenn es seit nunmehr mehr als einem Jahrzehnt Abkommen der EU mit den USA, Australien und Kanada[132] zur Fluggastdatenverarbeitung gibt, die europäische Fluglinien

[126] Passenger Name Record.
[127] Der Text wurde mit 461 Stimmen angenommen, bei 179 Gegenstimmen und 9 Enthaltungen.
[128] Art 6 der RL EU/2016/681.
[129] Erwägungsgrund (ErwGr) 6 der RL EU/2016/681.
[130] Ein sicherer Datenaustausch mit Europol soll über die Netzanwendung SIENA erfolgen, ErwGr 23 und Art 10 der RL EU/2016/681.
[131] ErwGr 24 der RL EU/2016/681.
[132] Die Rechtsgrundlage (das Abkommen zwischen der EU und Kanada aus dem Jahr 2005) zur Übermittlung von PNR-Daten an kanadische Behörden war nach Ablauf der Geltungsdauer des entsprechenden Beschlusses der Kommission vom 22.09.2009 ab diesem Zeitpunkt nicht mehr gegeben. Nachdem der Rat am 05.12.2013 beschloss, das Europäische Parlament (EP) um seine Zustimmung zum Abschluss eines neuen Abkommens (welches von der EU und Kanada am 25.06.2014 unterzeichnet wurde), zu ersuchen, entschied das EP ua wegen der sehr kritischen Stellungnahmen des Europäischen Datenschutzbeauftragten, das Abkommen vor einer allfälligen Beschlussfassung dem EuGH zur Prüfung vorzulegen. Im Schlussantrag zum Gutachten des EuGH vom 08.09.2016 ist der Generalanwalt Mengozzi der Ansicht, dass verschiedene Bestimmungen des Abkommens gegen die Charta der Grundrechte der EU verstoßen. (Opinion 1/15 des Generalanwalts Mengozzi vom 08.09.2016). Mit einer Entscheidung des Gerichtshofs ist im Herbst 2016 zu rechnen.
Opinion 1/15 des Generalanwalts Mengozzi vom 08.09.2016:

zur Weiterleitung von Fluggastinformationen an die Behörden dieser Staaten verpflichten, war auf EU-Ebene die Verwendung solcher Daten nicht geregelt, wenngleich eine solche bereits seit 2007 in Verhandlung war. Als Reaktion auf die Anschläge auf die Redaktion von Charlie Hebdo in Paris im Jänner 2015 wurden verschiedene Anti-Terrormaßnahmen ins Treffen geführt, deren zentraler Bestandteil die Fluggastdatenverarbeitung war und in der vorliegenden Richtlinie gemündet hat. Diese ist von den Mitgliedstaaten bis 25. Mai 2018 in nationales Recht umzusetzen.

Nach der Richtlinie sollen sämtliche Informationen, die eine Fluggesellschaft über ihre Passagiere, welche im Hoheitsgebiet der EU eintreffen oder dieses verlassen[133], hält, an eine neu einzurichtende Stelle der nationalen Sicherheitsbehörden (PNR-Zentralstelle[134] oder Englisch Passenger Information Unit) 24 bis 48 Stunden vor Abflug weitergegeben[135] werden. Aus den vorliegenden Informationen über das Buchungs-, Zahlungs- und Sitzplatzwahlverhalten sowie über das gesamte Reiseverhalten (Anschlussflüge, Flugscheindaten, Zahlungsinformationen, Vielfliegereinträge, Gepäckangaben, Informationen über Mitreisende etc.) sollen Kenntnisse über Verhaltensmuster gewonnen werden. In der Folge sollen aus diesen Informationen Prüfkriterien abgeleitet werden, anhand derer die PNR-Daten[136] abgeglichen werden[137]. Durch die Aufstellung und Anwendung dieser Prüfkriterien auf terroristische Straftaten und schwere Kriminalität, für die die Anwendung solcher Kriterien maßgeblich ist, soll die Verarbeitung von PNR-Daten auf das Erforderliche beschränkt bleiben und zudem die Zahl an false-positives auf ein Minimum reduziert werden[138]. Bei sog. false-positives handelt es sich um unschuldige Personen, die fälschlicherweise vom System als potentiell gefährlich eingestuft werden und aufgrund der verarbeiteten Daten einer Kontrolle oder diversen Überwachungsmaßnahmen unterzogen werden. An dieser Stelle ist darauf hinzuweisen, dass ein europäisches PNR-System zu einer gigantischen Datensammlung führt und eine große Anzahl von „false positives“ kaum zu verhindern ist. Sämtliche, die EU-Außengrenzen mit dem Flugzeug überquerenden Personen werden in einer Sicherheitsdatei gespeichert, ohne dass für die Speicherung personenbezogener Daten

http://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=702469

[133] Erfasst sind sog. „Drittstaatsflüge“. Ob die Mitgliedstaaten die Richtlinie auch auf Flüge innerhalb der EU anwenden, entscheiden diese selbst.

[134] Art 4 der RL EU/2016/681.

[135] Gem. Art 8 Abs 1 der RL EU/2016/681 ist für die Datenweitergabe die sog. „Push-Methode“ vorgesehen, bei der die Fluggesellschaften die verlangten Daten an die anfragende Behörde übermittelt (im Gegensatz zur sog. „Pull-Methode, bei der die zuständigen Behörden direkt auf das Buchungssystem der Fluggesellschaften zugreifen und Daten extrahieren können).

[136] Eine taxative Liste der von Fluggesellschaften zu erhebenden PNR-Daten findet sich in Anhang I der RL EU/2016/681.

[137] ErwGr 7 und Art 6 Abs 3 lit b der RL EU/2016/681.

[138] ErwGr 7 der RL EU/2016/681.

von Millionen von Menschen[139] ein konkreter Anlass besteht. Diese neue Art der Vorratsdatenspeicherung greift massiv in die von der EU-Grundrechtecharta und der EMRK garantierten Grundrechte auf Datenschutz und auf Achtung des Privatlebens ein. Statt dass im Einzelfall bei Tatverdacht oder Hinweisen auf konkrete Gefahren personenbezogene Daten ermittelt und verarbeitet werden, werden pauschal ganze Personengruppen umfassend registriert und letztlich unter Generalverdacht gestellt. Die von den Fluggesellschaften an die PNR-Zentralstellen übermittelten Daten sollen fünf Jahre[140] lang gespeichert werden, wobei die PNR-Daten nach einer Frist von sechs Monaten durch Unkenntlichmachung bestimmter Datenelemente, mit denen eine Person individualisiert werden kann, entpersonalisiert werden sollen (Pseudonymisierung). Unter bestimmten Voraussetzungen kann aber der volle PNR-Datensatz wiederhergestellt werden[141].

Peter Schaar, ehemaliger Bundesbeauftragter für den Datenschutz und die Informationsfreiheit in der Bundesrepublik Deutschland, hält die Einführung eines PNR-Systems in Europa auch deshalb für verfehlt, weil bisher nicht einmal die bestehenden Rechtsinstrumente wie die API[142]-Richtlinie (2004/82/EG) vollständig umgesetzt[143] wurden. Auch bei dieser Richtlinie geht es um Flugpassagierdaten, die allerdings mit einer klaren Zweckbestimmung erhoben und nicht längerfristig gespeichert werden sollen. Er sieht keinen weiteren Bedarf an Passagierdaten, die über die API-Daten hinausgehen[144], wobei festzuhalten ist, dass selbst dieses Instrument nach Aussage der Kommission nur von einer sehr geringen Zahl an EU-Mitgliedstaaten genutzt wird[145] und der Nutzen zur Verbesserung der Grenzkontrollen und der Bekämpfung der illegalen Einwanderung zumindest zweifelhaft ist. Auch der Europäische Datenschutzbeauftragte erkennt im Richtlinienvorschlag massive Grundrechtseingriffe für eine Vielzahl an Flugpassagieren ohne Differenzierung, Begrenzung oder Ausnahmen in Hinblick auf das Ziel der Bekämpfung von Terrorismus und schwerer Kriminalität[146]. Diese anlasslose, umfassende und nicht unterscheidende Speicherung von personenbezogenen Daten der Bevölkerung wurde schon vom EuGH in der Begründung der Entscheidung, mit der die Vorratsdatenspeicherungs-Richtlinie annulliert wurde, ins Treffen geführt.

---

[139] Der Europäische Datenschutzbeauftragte geht von mehr als 300 Millionen betroffenen nicht-verdächtigen Fluggästen aus, die von der PNR-RL betroffen sind, European Data Protection Supervisor, Opinion 15/2015, 7.

[140] Art 12 Abs 1 der RL EU/2016/681.

[141] Art 12 Abs 2 der RL EU/2016/681.

[142] Advance Passenger Information (Vorabübermittlung von Angaben über die beförderten Personen durch Fluggesellschaften).

[143] In Österreich wurde die Weitergabe von Passagierinformationen (API) im § 111 FPG umgesetzt.

[144] *Schaar*, Rede am 30.01.2009 anlässlich des Europäischen Datenschutztags in Wien.

[145] Europäische Kommission, Overview of information management in the area of freedom, security and justice, COM(2010)385 final, 8.

[146] European Data Protection Supervisor, Opinion 15/2015, 7.

Abkommen zwischen der EU und Kanada zur Übermittlung von PNR-Daten (Passenger Name Records)

Die Rechtsgrundlage (das Abkommen zwischen der EU und Kanada aus dem Jahr 2005) zur Übermittlung von PNR-Daten an kanadische Behörden war nach Ablauf der Geltungsdauer des entsprechenden Beschlusses der Kommission vom 22.09.2009 ab diesem Zeitpunkt nicht mehr gegeben. Nachdem der Rat am 05.12.2013 beschloss, das Europäische Parlament (EP) um seine Zustimmung zum Abschluss eines neuen Abkommens (welches von der EU und Kanada am 25.06.2014 unterzeichnet wurde), zu ersuchen, entschied das EP ua wegen der sehr kritischen Stellungnahmen des Europäischen Datenschutzbeauftragten, das Abkommen vor einer allfälligen Beschlussfassung dem EuGH zur Prüfung vorzulegen.

Im Schlussantrag[147] zum Gutachten des EuGH vom 08.09.2016 ist der Generalanwalt (GA) Mengozzi der Ansicht, dass das geplante Abkommen zwar mit der Charta der Grundrechte der EU vereinbar ist, sofern bestimmte Kriterien erfüllt werden, jedoch verstoßen bestimmte ausverhandelte Vorschriften gegen die Charta.

Zu den erwähnten Kriterien gehören insbesondere die Sicherstellungen, dass

- die Kategorien der Fluggastdatensätze klar und präzise formuliert werden und sensible Daten nicht gespeichert und verwendet dürfen,
- die Straftaten die unter die Definition schwerer grenzübergreifender Kriminalität fallen, abschließend aufgezählt werden sowie
- das Abkommen durch klare und präzise Regelungen garantiert, dass eine unabhängige (kanadische) Behörde die Achtung der Privatsphäre und den Schutz personenbezogener Daten überwachen kann.

Weiters muss eine unabhängige Behörde oder ein kanadisches Gericht ermächtigt werden, zu prüfen, ob die zuständige kanadische Behörde die erhobenen PNR-Daten an andere kanadische oder ausländische Behörden übermitteln darf.

Klar gegen die Charta verstoßen unter anderem Bestimmungen, wonach die Verarbeitung von sensiblen Daten oder die Speicherung von PNR-Daten durch kanadische Behörden für fünf Jahre möglich ist und diese Daten auch für andere Zwecke als zur Aufrechterhaltung der öffentlichen Sicherheit verwendet werden dürfen.

Der Generalanwalt gelangt zu diesem Ergebnis, weil insbesondere aus den Urteilen zur Annullierung der Vorratsdatenspeicherung[148] und zu Safe Harbor[149] neue Erkenntnisse gezogen wurden. Begrüßenswert ist, dass der GA der Ansicht ist, dass der in diesen Urteilen vorgezeichnete Weg fortzuführen und das geplante Abkommen einer strikten Kontrolle im Hinblick auf die Achtung des Privatlebens und das Recht auf Schutz

[147] http://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=702469.
[148] EuGH Verbundene Rs C-293/12 und C-594/12.
[149] EuGH Rs C-362/14.

personenbezogener Daten zu unterziehen ist. Insbesondere in Zeiten, in denen den Sicherheits- und Strafverfolgungsbehörden modernste Technologien zur Überwachung und Auswertung unseres Privatlebens zur Verfügung stehen, ist es notwendig, sicherzustellen, dass die beabsichtigten Maßnahmen (auch wenn sie in Form internationaler Abkommen getroffen werden) eine ausgewogene Gewichtung zwischen Freiheit und Sicherheit widerspiegeln.

Hinsichtlich der EU-PNR Richtlinie zeigt sich erneut, dass eine Anlassgesetzgebung ohne ausreichende Evaluation nicht zielführend ist und das Europäische Parlament, wie vom AKVorrat (Heute: epicenter.works) gefordert, gut beraten gewesen wäre, das Gutachten des EuGHs zum PNR-Abkommen zwischen der EU und Kanada abzuwarten, bevor mit der EU-PNR Richtlinie eine weitere Vorratsdatenspeicherung verabschiedet wurde, deren Rechtsgrundlage starke Zweifel im Hinblick auf ihre Grundrechtskonformität aufkommen lässt. Diese Zweifel werden durch den Schlussantrag des Generalanwalts bestärkt.

Mit einer Entscheidung und Veröffentlichung des Gutachtens des Gerichtshofs ist im Herbst 2016 zu rechnen.

4.6.2 Ein-/Ausreisekontrollen

Parlamentarische Anfrage 4016/J (XXV. GP) BMI

1. Welche Daten werden von österreichischen Behörden bei der Ein- oder Ausreise einer Person erhoben?
2. Mit welchen Datenbanken werden Personendaten von Grenzübertritten in automatisierter oder manueller Form abgeglichen?
3. Wie lange und zu welchen Zwecken werden die bei einem Grenzübertritt erhobenen Daten aufbewahrt bzw. verwendet?
4. Unter welchen Bezeichnungen bzw. Nummern sind die Datenanwendungen für die Verarbeitung von bei Grenzübertritten erhobenen Daten im Verzeichnis der Informationsverbundsysteme (https://dvr.dsb.gv.at/at.gv.bka.dvr.public/IVSRecherche.aspx) zu finden?
5. Wann erfolgte die Registrierung dieser Datenanwendungen und wann erfolgte die Aufnahme des Betriebs?
6. Nach welchen Sicherheitsvorgaben und Standards (z. B. Österreichisches IT-Sicherheitshandbuch, IT-Grundschutzhandbuch, ISO 270xx) wurden die Datensicherheitsmaßnahmen (vgl. §14 DSG 2000) gestaltet und umgesetzt, insbesondere hinsichtlich der Absicherung der
a. zentralen Dankenbank?
b. dezentralen Stellen, von welchen auf die Datenbank lesend oder schreibend zugegriffen werden kann?
c. Verbindungen zwischen der Datenbank und den dezentralen Stellen?

d. des Backups?
7. Wurde die Absicherung der oben genannten zentralen Datenbank und der Zugriffsmöglichkeiten von unabhängiger Stelle evaluiert?
a. Wenn ja, von welcher Stelle und mit welchem Ergebnis?
b. Wenn ja, wie häufig werden diese Evaluierungen wiederholt und wann wurde diese Evaluierung zuletzt durchgeführt?
c. Wenn nein, wieso nicht?
8. Wie werden Zugriffe auf diese Datenbank protokolliert und ausgewertet?
9. Gab es seit der Einführung Missbrauchsfälle in Zusammenhang mit dieser Datenbank?
a. Wenn ja, wie viele?
b. Wenn ja, wurden die betroffenen Personen darüber informiert?
10. Wie hoch sind die Kosten für den laufenden Betrieb der Datenbank und ihrer Absicherung jährlich seit der Einführung?

Parlamentarische Beantwortung 4016/ J (XXV. GP) BMI

Zu Frage 1:
Es werden die in der maschinlesbaren Zone (MRZ) des Reisepasses/Personalausweises bzw. Visums enthaltenen Daten ausgelesen.

Zu Frage 2:
Die ausgelesenen Daten werden mit dem Elektronischen Kriminalpolizeilichen Informationssystem (EKIS), dem Schengener Informationssystem der zweiten Generation (SIS II) und der Datenbank verlorener und gestohlener Reisedokumente (Stolen and Lost Travel Documents Database – SLTD) von Interpol in Lyon abgeglichen.

Zu Frage 3:
Die aus dem Reisedokument ausgelesenen Daten werden nicht aufbewahrt und stehen somit für eine spätere Verwendung nicht zur Verfügung.

Zu den Fragen 4 und 5:
Das bloße automatisierte Auslesen der Daten für Fahndungsabfragen iSd § 15 Abs. 1 Z 1 Grenzkontrollgesetz stellt keine eigenständige Datenanwendung iSd § 4 Z 7 Datenschutzgesetz 2000 dar.

Zu Frage 6:
Alle Sicherheitsmaßnahmen werden gemäß den Vorgaben des Österreichischen Informationssicherheitshandbuches (in der Version 3) gestaltet und umgesetzt.

Zu Frage 7:

Da es sich bei der Anwendung um eine Portalverbundanwendung handelt, erfolgt die Evaluierung gemäß dem Portalverbund-Revisionsleitfaden und den Portalverbund-Datensicherheitsmaßnahmen für Webanwendungen.

Zu Frage 8:
Alle Datenbankzugriffe werden gemäß § 14 Abs. 2 Z 7 Datenschutzgesetz 2000 protokolliert.
Diese Protokolleinträge bilden die Grundlage für eine laufende Prüfung der Rechtmäßigkeit der Datenbankzugriffe im Rahmen der Dienstaufsicht.

Zu Frage 9:
Es sind keine missbräuchlichen Datenbankverwendungen bekannt.

Zu Frage 10:
Aus den laufenden Betriebskosten des EKIS u. des SIS II kann der prozentuelle Anteil für Zwecke der Grenzkontrolle nicht berechnet werden.

Parlamentarische Anfrage 4022/J (XXV. GP) BMEIA

1. Betreibt die Customs Border Patrol (CBP) des US-Department of Homeland Security am Wiener Flughafen oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten ein Büro?
2. Wie viele US-Grenzschutzbeamte befinden sich im Einsatz am Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknoten-punkten? (Bitte um Aufschlüsselung auf den konkreten Standort)
3. Auf welcher rechtlichen Basis operieren US-amerikanische Behörden am Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten und welche Kooperationen gibt es mit österreichischen Behörden?
4. Mit welchen Kompetenzen und Fähigkeiten operieren diese US-amerikanischen Grenzschutzbeamten am Flughafen Schwechat oder an anderen Österreichischen Flughäfen oder Verkehrsknotenpunkten?
5. Kam es schon einmal zu Verhaftungen am Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten durch US-amerikanische Grenzschutzbeamte?
a. Wenn ja, wann, an welchem Flughafen und aufgrund welchen konkreten Verdachts?
6. Welcher Rechtsschutz ist für Personen vorgesehen, die im Transitbereich des Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten von US-Beamten in Gewahrsam genommen werden?
7. Kam es schon einmal zu Verhaftungen am Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten, welche durch Beratungen der US-Polizei vor Ort ausgelöst oder von diesen vorgenommen wurden?

8. In welche Terrorfrühwarnsysteme werden von Österreich welche Daten eingespeist oder daraus bezogen? (Bitte um Aufzählung inkl. Beginn der Einspeisung)

Parlamentarische Beantwortung 4022/ J (XXV. GP) BMEIA

Zu den Fragen 1 bis 8:

Die Inhalte der Fragen fallen nicht in die Vollziehung des Bundesministeriums für Europa, Integration und Äußeres (BMEIA).

Parlamentarische Anfrage 4023/J (XXV. GP) BMLV

1. Betreibt die Customs Border Patrol (CBP) des US-Department of Homeland Security am Wiener Flughafen oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten ein Büro?
2. Wie viele US-Grenzschutzbeamte befinden sich im Einsatz am Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten? (Bitte um Aufschlüsselung auf den konkreten Standort)
3. Auf welcher rechtlichen Basis operieren US-amerikanische Behörden am Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten und welche Kooperationen gibt es mit österreichischen Behörden?
4. Mit welchen Kompetenzen und Fähigkeiten operieren diese US-amerikanischen Grenzschutzbeamten am Flughafen Schwechat oder an anderen Österreichischen Flughäfen oder Verkehrsknotenpunkten?
5. Kam es schon einmal zu Verhaftungen am Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten durch US-amerikanische Grenzschutzbeamte?
a. Wenn ja, wann, an welchem Flughafen und aufgrund welchen konkreten Verdachts?
6. Welcher Rechtsschutz ist für Personen vorgesehen, die im Transitbereich des Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten von US-Beamten in Gewahrsam genommen werden?
7. Kam es schon einmal zu Verhaftungen am Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten, welche durch Beratungen der US-Polizei vor Ort ausgelöst oder von diesen vorgenommen wurden?
8. In welche Terrorfrühwarnsysteme werden von Österreich welche Daten eingespeist oder daraus bezogen? (Bitte um Aufzählung inkl. Beginn der Einspeisung)

Parlamentarische Beantwortung 4023/ J (XXV. GP) BMLV

Zu 1 bis 8:

Da diese Fragen nicht den Vollziehungsbereich des Bundesministeriums für Landesverteidigung und Sport betreffen, nehme ich von einer inhaltlichen Beantwortung Abstand.

Parlamentarische Anfrage 4024/J (XXV. GP) BMI

1. Betreibt die Customs Border Patrol (CBP) des US-Department of Homeland Security am Wiener Flughafen oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten ein Büro?
2. Wie viele US-Grenzschutzbeamte befinden sich im Einsatz am Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten? (Bitte um Aufschlüsselung auf den konkreten Standort)
3. Auf welcher rechtlichen Basis operieren US-amerikanische Behörden am Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten und welche Kooperationen gibt es mit österreichischen Behörden?
4. Mit welchen Kompetenzen und Fähigkeiten operieren diese US-amerikanischen Grenzschutzbeamten am Flughafen Schwechat oder an anderen Österreichischen Flughäfen oder Verkehrsknotenpunkten?
5. Kam es schon einmal zu Verhaftungen am Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten durch US-amerikanische Grenzschutzbeamte?
a. Wenn ja, wann, an welchem Flughafen und aufgrund welchen konkreten Verdachts?
6. Welcher Rechtsschutz ist für Personen vorgesehen, die im Transitbereich des Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten von US-Beamten in Gewahrsam genommen werden?
7. Kam es schon einmal zu Verhaftungen am Flughafen Schwechat oder an anderen österreichischen Flughäfen oder Verkehrsknotenpunkten, welche durch Beratungen der US-Polizei vor Ort ausgelöst oder von diesen vorgenommen wurden?
8. In welche Terrorfrühwarnsysteme werden von Österreich welche Daten eingespeist oder daraus bezogen? (Bitte um Aufzählung inkl. Beginn der Einspeisung)

Parlamentarische Beantwortung 4024/ J (XXV. GP) BMI

Zu Frage 1:
Nein.

Zu Frage 2:
Keine.

Zu den Fragen 3 bis 7:
Entfällt auf Grund der Beantwortung zu den Fragen 1 und 2.

Zu Frage 8:
Im Rahmen bestehender bi- und multilateraler Abkommen sowie der den internationalen Datenaustausch regelnden Gesetze, wie z.B. das Bundesgesetz über die polizeiliche Kooperation mit den Mitgliedstaaten der Europäischen Union und dem Europäischen Polizeiamt (Europol), (EU – Polizeikooperationsgesetz, EU-PolKG), das Bundesgesetz über die internationale polizeiliche Kooperation (Polizeikooperationsgesetz – PolKG), werden Informationen zur Terrorismusbekämpfung ausgetauscht.

Im Rahmen dieser internationalen Verpflichtungen und nationalen Berechtigungen werden die, entsprechend der jeweiligen Rechtsgrundlage zulässigen Daten an die Frühwarnsysteme „Fusion Task Force“ bei Interpol und an die verschiedenen Analysedateien bei EUROPOL übermittelt.

- Die Interpol-FTF (Fusion Task Force) wurde nach den Anschlägen am 9. September 2001 in den USA im Jahre 2002 eingerichtet. Seither wirkt das BM.I dabei mit und übermittelt strategische und operative Informationen zum Themenbereich Terrorismus (islamistischer Terrorismus, Ausländerextremismus, separatistischer Terrorismus usw.).

- Zur Bekämpfung des Terrorismus werden EUROPOL strategische und operative Daten mitgeteilt, die nach den nationalen Gesetzen rechtmäßig erhoben wurden und in den Mandatsbereich von EUROPOL fallen. Im Dezember 1998 wurde dieses Mandat auf die Bekämpfung des Terrorismus ausgeweitet und seit dem erfolgt ein Datenaustausch mit EUROPOL.

Die Anwendungen bei EUROPOL heißen "Analysearbeitsdateien" (Analytical Work Files - AWF). Im Bereich Terrorismusbekämpfung besteht bei EUROPOL derzeit eine Analysearbeitsdatei, nämlich das AWF Counter Terrorism (AWF-CT) an welchem Österreich auch teilnimmt.

Innerhalb des AWF-CT ist die Arbeit in so genannte Focal Points (FP) gegliedert. Derzeit beteiligt sich Österreich innerhalb des AWF-CT an folgenden Focal Points und übermittelt anlassbezogen entsprechende Daten:

- FP - CTW (Check the web): der Focal Point beschäftigt sich mit der Nutzung des Internets für terroristische Zwecke (wurde mit 18.12.2009 eingerichtet).
- FP - HYDRA: der Focal Point legt seinen Schwerpunkt auf religiös motivierten, insbesondere islamistischen Terrorismus (wurde mit 22.02.2000 eingerichtet).
- FP - DOLPHIN: zentrale Thematik des Schwerpunkts sind alle anderen Formen des Terrorismus, insbesondere des nationalistischen, separatistischen und ideologisch motivierten Terrorismus (wurde mit 08.09.2003 eingerichtet).
- FP - TRAVELLERS: dieser Focal Point beschäftigt sich mit Dschihadreisenden (wurde mit 28.04.2014 eingerichtet)

4.6.3 Reisepässe

Parlamentarische Anfrage 4017/J (XXV. GP) BMI

1. An welche Länder wurden oder werden entsprechende Zertifikate geliefert, sodass die in den österreichischen Reisepässen gespeicherten Fingerabdrücke in den jeweiligen Ländern tatsächlich ausgelesen werden können? (Bitte um Aufschlüsselung nach Land sowie seit wann und bis wann diese Zertifikate geliefert werden bzw. wurden.)
2. Wie lange sind diese Zertifikate jeweils gültig? (Bitte um Aufschlüsselung nach Land.)
3. Von welchen anderen Ländern werden Österreich die entsprechenden Zertifikate zum Auslesen der Reisepässe (inkl. Fingerabrücke) der jeweiligen Länder zur Verfügung gestellt? (Bitte um Aufschlüsselung nach Land sowie seit wann und bis wann diese Zertifikate geliefert werden bzw. wurden.)
4. Wie lange sind diese Zertifikate jeweils gültig? (Bitte um Aufschlüsselung nach Land.)
5. Wie viele Kontrollstellen (d. h. Lesegeräte) sind in Österreich in Betrieb, welche die Reisepässe dieser anderen Länder elektronisch (inkl. Fingerabdrücke) auslesen können?
6. Wie hoch waren die Kosten zur Einrichtung dieser Stellen? (Bitte um Aufschlüsselung nach Kontrollstellen.)
7. Bis wann werden mit den übrigen EU-Ländern die notwendigen Zertifikats-Austausch-Infrastrukturen aufgebaut sein, um die Fingerabdrücke in den Reisepässen auslesen zu können?
8. Wie hoch sind die erwarteten Kosten dafür?
9. Wie viele Kontrollstellen sind in den unter Frage 1 genannten Ländern mit der notwendigen Technik (insbesondere Lesegeräte mit den benötigten Zertifikaten) ausgestattet, um die Reisepässe elektronisch (inkl. Fingerabdrücke) auslesen zu können?
10. Wie viele Kontrollstellen sind in Österreich mit der notwendigen Technik (insbesondere Lesegeräte mit den benötigten Zertifikaten) ausgestattet um Reisepässe elektronisch (inkl. Fingerabdrücke) auslesen zu können?
11. Nach welchen Sicherheitsvorgaben und Standards (z. B. Österreichisches IT-Sicherheitshandbuch, IT Grundschutzhandbuch, ISO 270xx) wurden die Datensicherheitsmaßnahmen (vgl. §14 DSG 2000) gestaltet und umgesetzt, insbesondere hinsichtlich der Absicherung der a. zentralen Dankenbank?
b. dezentralen Stellen, von welchen auf die Datenbank lesend oder schreibend zugegriffen werden kann?
c. Absicherung der Verbindungen zwischen der Datenbank und den dezentralen Stellen?
d. des Backups?
12. Wurde die Absicherung der oben genannten zentralen Datenbank und der Zugriffsmöglichkeiten von unabhängiger Stelle evaluiert?
a. Wenn ja, von welcher Stelle und mit welchem Ergebnis?

b. Wenn ja, wie häufig werden diese Evaluierungen wiederholt und wann wurde diese Evaluierung zuletzt durchgeführt?
c. Wenn nein, wieso nicht?
13. Werden Zugriffe auf diese Datenbank protokolliert und ausgewertet?
a. Wenn ja, wie genau?
b. Wenn nein, wieso nicht?
14. Gab es seit der Einführung Missbrauchsfälle in Zusammenhang mit dieser Datenbank?
a. Wenn ja, wie viele?
b. Wenn ja, wurden die betroffenen Personen darüber informiert?
15. Wie hoch sind die Kosten für den laufenden Betrieb der Datenbank und ihrer Absicherung seit der Einführung? (Bitte um Aufschlüsselung auf Jahre)

Parlamentarische Beantwortung 4017/ J (XXV. GP) BMI

Zu den Fragen 1 bis 4 und 9:
Bislang wurden noch mit keinem Land Zertifikate zum Auslesen der Fingerabdrücke ausgetauscht.

Zu den Fragen 5, 6 und 10:
In Österreich sind keine Grenzkontrollstellen in Betrieb, welche Reisepässe inklusive der am Chip gespeicherten Fingerabdrücke elektronisch auslesen können.

Zu den Fragen 7 und 8:
Die Beantwortung dieser Fragen fällt nicht in den Vollzugsbereich des Bundesministeriums für Inneres.

Zu Frage 11:
Die für die Ausstellung, Verwaltung und Nutzung der Zertifikate notwendigen Systeme wurden entsprechend der Entscheidung der Europäischen Kommission K(2008) 8657 vom 22. Oktober 2008 (EAC-Policy) gestaltet und umgesetzt. Darüber hinaus läuft eine Veröffentlichung detaillierter Informationen im Internet, wie dies bei Beantwortung parlamentarischer Anfragen der Fall ist, den Sicherheitsinteressen zuwider.

Zu Frage 12:
Entsprechend der Vorgaben der Common Certificate Policy (BSI TR-03139 Version 2.1 vom 27. Mai 2013) wird vor der Nutzung der Zertifikate bzw. vor Inbetriebnahme des Zertifikats-austausches mit anderen Ländern die österreichische Zertifikatsinfrastruktur einem externen Audit unterzogen. Darüber hinaus läuft eine Veröffentlichung detaillierter Informationen im Internet, wie dies bei Beantwortung parlamentarischer Anfragen der Fall ist, den Sicherheitsinteressen zuwider.

Zu Frage 13:

Die Zertifikatsadministration wird sowohl manuell als auch elektronisch protokolliert. Eine Überprüfung der Rechtmäßigkeit der Tätigkeiten findet im Rahmen der Dienstaufsicht statt.

Zu Frage 14:
Es ist bislang kein Missbrauchsfall bekannt.

Zu Frage 15:
Die laufenden Kosten für die vollständige nationale Public Key Infrastructure, die für die Ausstellung aller nationalen und die Kontrolle aller nationalen und internationalen elektronischer Reisedokumente und Aufenthaltstitel notwendig ist, betrugen
2009: € 4.152.-
2010: € 4.152.-
2011: € 29.051,14.-
2012: € 146.905,32.-
2013: € 146.905,32.-
2014: € 146.905,32.-

Parlamentarische Anfrage 4028/J (XXV. GP) BMI

1. Unter welche(n) Bezeichnungen bzw. Nummern sind die Datenanwendungen im Verzeichnis der Informationsverbundsysteme (https://dvr.dsb.gv.at/at.gv.bka.dvr.public/IVSRecherche.aspx) zu finden?
2. Wann erfolgte die Registrierung dieser Datenanwendungen?
3. Wann erfolgte die Aufnahme des Betriebs?
4. Wird die Sicherheit der Anwendung überprüft?
a. Wenn ja, durch wen, wie genau und in welchen Abständen?
b. Wenn nein, wieso nicht?
5. Wie viele gefälschte Dokumente wurden seit der Einführung aufgrund der gespeicherten Fingerabdrücke erkannt?
6. Wie viele dieser Dokumente hätten ohne die gespeicherte Fingerabdrücke nicht erkannt werden können?
7. Wie viele Betrugsversuche (z. B. fremde Person benutzt echten Reisepass einer anderen Person) wurden seit der Einführung aufgrund der gespeicherten Fingerabdrücke erkannt?
8. Wie viele dieser Dokumente hätten ohne die gespeicherte Fingerabdrücke nicht erkannt werden können?
9. Mit welchen anderen Datenbanken werden die Daten des Antragstellers eines Reisepasses abgeglichen, ausgetauscht oder verknüpft? (Bitte um Aufschlüsselung nach Art und ob dies automatisch oder manuell geschieht)
10. Werden dabei insbesondere Gesichtsbilder oder Fingerabdrücke verglichen?
11. Wie lange werden die Gesichtsbilder in der Datenbank gespeichert?
12. Wie lange werden die Fingerabdruckbilder in der Datenbank gespeichert?

13. Wie wird sichergestellt, dass bei der Aufnahme der Fingerabdrücke keine „gefälschten" Fingerabdrücke präsentiert werden?
14. Werden die Fingerabdrücke nach der Aufnahme bis zur Speicherung im Reisepass gegen Modifikationen gesichert?
a. Wenn ja, wie genau?
b. Wenn nein, wieso nicht?
15. Hat der Reisepassinhaber eine Möglichkeit, die Korrektheit der im Reisepass gespeicherten Fingerabdrücke zu überprüfen?
a. Wenn ja, wie genau?
b. Wenn nein, wieso nicht?

Parlamentarische Beantwortung 4028/ J (XXV. GP) BMI

Zu Frage 1:
Im Verzeichnis der Informationsverbundsysteme (https://dvr.dsb.gv.at/at.gv.bka.dvr.public/IVSRecherche.aspx) sind die Datenanwendungen unter der Bezeichnung „Zentrales Identitätsdokumentenregister" zu finden.

Zu den Fragen 2 und 3:
Die Aufnahme des Vollbetriebs der Informationsverbundsystem-Datenanwendungen „Zentrales Identitätsdokumentenregister" erfolgte nach der jeweiligen Prüfung/Registrierung der jeweiligen Auftraggeber-Meldung der jeweiligen Passbehörde durch die Datenschutzkommission gemäß § 18 Abs. 2 DSG 2000 im Jahr 2001 bzw. im Jahr 2003 (hier: nach Übertragungen des Passwesens von den Bundespolizeidirektionen auf die Magistrate bzw. Stadtgemeinden Leoben und Schwechat).

Zu Frage 4:
Für die Einhaltung der Datensicherheitsmaßnahmen gemäß § 14 DSG 2000 sind die jeweiligen Passbehörden als Auftraggeber (iSd § 4 Z 4 DSG 2000) bzw. der Betreiber des Informationsverbundsystems gemäß § 50 Abs. 1 DSG 2000 verantwortlich. Gemäß § 14 Abs. 2 Z 7 DSG 2000 ist insbesondere Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können.

Zu den Fragen 5 bis 8:
Derzeit wird kein Vergleich der Fingerabdrücke des Passinhabers mit den Bildern der Papillarlinienabdrücke, die auf dem Chip gespeichert sind, durchgeführt. Die technische Umsetzung ist in Vorbereitung.

Zu Frage 9:

Die Mitarbeiterin oder der Mitarbeiter der Passbehörde führt eine manuelle Abfrage im Zentralen Melderegister, in der Personenfahndung und -information, im Strafregister und der Sachenfahndung durch.

Zu Frage 10:
Bei Zweifeln an der Identität der Passwerberin oder des Passwerbers wird im Einzelfall durch die Mitarbeiterin oder durch den Mitarbeiter der Passbehörde das im Identitätsdokumentenregister gespeicherte Lichtbild mit dem Antragsteller verglichen.

Zu Frage 11:
Lichtbilder, die bei Antragstellung verarbeitet werden, sind mit wirksamer Zurückziehung oder rechtskräftiger Zurückweisung des Antrages zu löschen. Im Übrigen sind die Lichtbilder ein Jahr nach der Entwertung des Reisepasses spätestens aber sechs Jahre nach Ablauf der letzten Gültigkeitsdauer für Auskünfte zu sperren und nach zwei weiteren Jahren zu löschen. Die Lichtbilder werden auch bei dem mit der Passproduktion beauftragten Dienstleister innerhalb der gesetzlich vorgeschriebenen Löschfristen gelöscht; der staatliche Kontrolldienst prüft dies im Rahmen der wöchentlichen Datenaudits.

Zu Frage 12:
Die Papillarlinienabdrücke werden spätestens zwei Monate nach Versendung des Dokuments und spätestens vier Monate nach Versendung des Dokuments unter Einbindung des Bundesministeriums für Europa, Integration und Äußeres gelöscht, sonst mit wirksamer Zurückziehung oder rechtskräftiger Zurück- oder Abweisung des Antrages. Die Papillarlinienabdrücke werden auch bei dem mit der Passproduktion beauftragten Dienstleister innerhalb der gesetzlich vorgeschriebenen Löschfristen gelöscht. Dies wird durch den staatlichen Kontrolldienst im Rahmen der wöchentlichen Datenaudits überprüft.

Zu Frage 13:
Die Fingerabdrücke werden durch und unter Aufsicht der Mitarbeiter der Passbehörden abgenommen, denen in Schulungen das notwendige Wissen vermittelt wird.

Zu Frage 14:
Die Bilder der Fingerabdrücke werden dem Bundesministerium für Inneres verschlüsselt übermittelt, dort in einer sicheren Umgebung verarbeitet und über eine gesicherte Datenleitung an den Dienstleister übermittelt.

Zu Frage 15:
Ja. Der Reisepass wird auf Antrag im Bundesministerium für Inneres, Referat III/3/a, mit einem Ausweisdokumentenlesegerät ausgelesen; der Reisepassinhaber erhält ein Datenprotokoll, einschließlich der Bilder der Fingerabdrücke.

4.6.4 Reisedatenermittlung nach dem Polizeilichen Staatsschutzgesetz

Gemäß § 11 Abs 1 Z 6 PStSG darf das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) [150]Auskünfte von Personenbeförderungsunternehmen im Rahmen von diesen erbrachten Leistungen zu Kontaktdaten, Nummer und Art des Reisedokuments sowie Zahlungsinformationen eines Betroffenen nach § 6 Abs 1 Z 2 PStSG (sog. „Gefährder"), Datum der Buchung, Reiseverlauf, Reisestatus, Flugscheindaten sowie Zahl und Namen von Mitreisenden einholen. Wer als "Personenbeförderungsunternehmen" iSd § 11 Abs 1 Z 6 PStSG anzusehen und damit zur Auskunftserteilung verpflichtet ist, ist unklar. Laut den Materialien[151] sind dies natürliche oder juristische Personen, die gewerbsmäßig Personentransporte durchführen oder Transportmittel zur Verfügung stellen oder vermitteln. Als Beispiele werden Fluggesellschaften, Reisebüros oder Mietwagenfirmen genannt. Der Wortlaut des im Gesetz verwendeten Begriffs "Personenbeförderungsunternehmen" deutet jedoch auf den Transport von Menschen durch Dritte hin. Das Zur-Verfügung-Stellen oder Vermitteln von Transportmitteln stellt aber keine Beförderung dar, was auch aus dem klaren Wortlaut des § 111 FPG[152] hervorgeht. Eine Diskrepanz zwischen dem Gesetzeswortlaut und den Materialien sollte im Hinblick auf die Normenklarheit und Transparenz vermieden werden. Überdies wäre nach einer strengen Wortinterpretation beispielsweise die Auskunftseinholung bei einem Reisebüro über Reisedaten eines Betroffenen nach § 6 Abs 1 Z 2 PStSG rechtswidrig, da es dafür keine gesetzliche Grundlage[153] gibt.

§ 11 Abs 1 Z 6 PStSG erlaubt somit den Zugriff auf den „Passenger Name Record" jeder Art von Verkehrsmittel. Ähnlich wie beim Zugriff auf Telekommunikationsdaten (zumindest nach der StPO) sollten die Zugriffsbefugnisse auch hier beschränkt werden, sodass der Gesetzgeber schon in der gesetzlichen Eingriffsgrundlage eine Abwägung vorzeichnet, die durch eine Verhältnismäßigkeitsprüfung im Einzelfall ergänzt werden soll.

Falls der EuGH im Herbst 2016 in seinem Gutachten[154] zum PNR-Abkommen zwischen der EU und Kanada ähnlich wie im Urteil[155] zur „Vorratsdatenspeicherung" von

[150] Ebenso befugt sind die Organisationseinheiten bei den Landespolizeidirektionen gem. § 1 Abs 3 PStSG.
[151] AB 988 BlgNR XXV. GP, 8.
[152] § 111 Abs 1 FPG: "Beförderungsunternehmer, die Personen mit einem Luft- oder Wasserfahrzeug oder im Rahmen des internationalen Linienverkehrs mit einem Autobus über die Außengrenze nach Österreich bringen, sind verpflichtet [...]".
[153] Ein Reisebüro (reine Vermittlertätigkeit) ist nicht vom Wortlaut „Personenbeförderungsunternehmen" erfasst.
[154] Siehe dazu die Ausführungen zu den Schlussanträgen des Generalanwalts Mengozzi in Kapitel 4.6.1, Opinion 1/15 vom 08.09.2016, http://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=702469.
[155] EuGH Verbundene Rs C-293/12 und C-594/12.

Telekommunikationsdaten auch Vorgaben zur Verwendung der Daten aussprechen sollte, sind diese dringend zu berücksichtigen. Im Übrigen besteht auch im Zusammenhang mit Reisebewegungen das Problem, dass damit gesetzlich anerkannte Verschwiegenheitspflichten (oder Berechtigungen) unterwandert werden können.

4.6.5 Rechtsgrundlagen im Überblick

Grundsätzlich gelten für die oben beschriebenen Technologien folgende gesetzlichen Bestimmungen:

- Richtlinie EU/2016/681
  - Im Besonderen:
    - Art 4 – PNR-Zentralstelle
    - Art 6 – Verarbeitung der PNR-Daten
    - Art 10 – Zugang von Europol zu PNR-Daten
    - Art 12 – Speicherfrist und Depersonalisierung

- Polizeiliches Staatsschutzgesetz (PStSG)
  - Im Besonderen:
    - § 11 Abs 1 Z 6 PStSG – Einholung von Auskünften (PNR-Datensätze) von Personenbeförderungsunternehmen

- Strafprozessordnung (StPO)

- Datenschutzgesetz 2000 (DSG 2000)

- Telekommunikationsgesetz 2003 (TKG 2003)

- Fremdenpolizeigesetz (FPG)
  - Im Besonderen:
    - § 111 FPG – Pflichten der Beförderungsunternehmer

4.7 Finanztransaktionen und Bankgeheimnis

Dieser Bereich ist für den Grundrechtsschutz vor allem deshalb höchst brisant, weil es sich um Maßnahmen in jeglichen Verfahren (ohne Parteistellung) handelt, die als gesetzliche Verpflichtung durch private Rechtsträger (Banken und Kreditinstitute) vorgenommen werden 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.: § 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.

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 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 – das sind so gut wie alle, wie ein Blick zumindest in das österreichische Strafgesetzbuch zeigt. Mitte 2015 wurde die 4. Geldwäsche-Richtlinie beschlossen, die bis Mitte 2017 von den Mitgliedstaaten umzusetzen ist.

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 der internationale Datenaustausch.

Der Bürger selbst soll also als Überwacher tätig werden, im – gesetzlich normierten – Auftrag des Staates seine 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 Rechtsanwältinnen und Rechtsanwälte in die absurde Situation geraten, gemäß § 8c RAO hinter dem Rücken ihrer Mandanten Informationen über einen „Verdacht“ auf „Terrorismusfinanzierung“ oder Geldwäschehandlungen an das Bundesministerium für Inneres (sohin den Polizeibehörden) melden zu müssen.

Die Probleme dieser Art des „Outsourcings“ der Überwachung auf Private sind mannigfach: Die Überwachung erfolgt nicht durch – mit hoheitlichen Befugnissen ausgestattete – Behörden, sondern eben durch „Private“, durch Banken, Unternehmen, Notare und Rechtsanwälte. Die Bürgerinnen und Bürger 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 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.

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 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 wobei die Zahl der Betroffenen in die Millionen geht. Diese „Watch Lists" greifen in das Datenschutzgrundrecht, die Bewegungsfreiheit sowie die Eigentumsfreiheit der Betroffenen ein und der Rechtsschutz, also die Mechanismen, um wieder aus einer solchen Liste herausgenommen zu werden, werden als mangelhaft beschrieben.[156]

Geldwäscherei (§ 165 StGB) ist zudem ein sehr weit gefasster Tatbestand. Sehr leicht kann man in die Situation kommen, das Tatbild zu erfüllen, wenn auch ohne jeglichen Vorsatz,[157] und auf diese Weise in den Fokus von Ermittlungen geraten. Ähnlich verhält es sich mit der Terrorismusfinanzierung (§ 278d StGB), ein Tatbestand der überdies sehr weit im Vorfeld der eigentlichen Tat angesiedelt ist.

Diese Umstände, die immer weiter in das Vorfeld verschobenen Straftatbestände, die mangelnde Parteistellung als Betroffener dieser Art der Überwachung und die besondere Gefahr, leicht – auch unschuldig – in den Fokus von Ermittlungen zu geraten, 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

[156] Vgl. *Böszörmenyi Janos/Schweighofer Erich*, Tracking of Financial Movements, in: *Erich Schweighofer/Franz Kummer/Walter Hötzendorfer* (Hrsg.), Transparenz. Tagungsband des 17. Internationalen Rechtsinformatik Symposions IRIS 2014, books@ocg.at, Wien 2014, S. 617-624. Siehe insb. auch EuGH 18. 07. 2013, C‑584/10 P, C‑593/10 P und C‑595/10 P, *Kadi*.

[157] Vgl. die grundsätzliche Kritik von Thomas Fischer, Bundesrichter in Karlsruhe: Woher haben Sie dieses Geld?, Zeit Online, 13. Oktober 2015, abrufbar unter http://www.zeit.de/gesellschaft/zeitgeschehen/2015-10/geldwaesche-fischer-im-recht/komplettansicht (01.07.2016.

untersuchter Sektor der Überwachung. Die Überwachung von Finanztransaktionen würde sich daher vornehmlich für eine sektorspezifische Bereichsevaluation der Überwachungsgesetze eignen.

Betreffend den Aspekt des Bankgeheimnisses hat der Gesetzgeber kürzlich 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 Konteneinschaugesetz (KontRegG) entscheidet ein Einzelrichter 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.

Diesbezüglich ist auch auf die HEAT-Empfehlung zur Durchführung einer Bereichsevaluation betreffend Eingriffe in geschützte Berufsgeheimnisse zu verweisen.

4.8 Private Datenverarbeitung[158]

Die Bestimmung des § 5 Abs 4 Datenschutzgesetz 2000[159] (DSG 2000) sieht vor, dass „gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, [...] soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen [ist]." Die Norm konstituiert somit für Jedermann den grundrechtlichen „Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht" (§ 1 Abs 1 DSG 2000) auch gegenüber privaten Rechtsträgern und verweist ihn in die Zuständigkeit der ordentlichen Gerichte. Das „Grundrecht auf Datenschutz" wird so „mit Drittwirkung ausgestattet", wie in den erläuternden Bemerkungen zur Regierungsvorlage (EBRV) zum DSG 2000[160] schlicht und in dieser Hinsicht zugleich abschließend formuliert.

Der Verfassungsgesetzgeber des Artikel 1 DSG 2000 normierte damit für das Grundrecht auf Datenschutz, was im grundrechtsdogmatischen Schrifttum nicht nur in Österreich seit längerem Gegenstand kontroverser Auseinandersetzungen ist und in systematischer

[158] Siehe dazu Tschohl, Datensicherheit.
[159] BGBl. I Nr. 165/1999 idF BGBl. I Nr. 2/2008 (1. BVRBG).
[160] EB RV 1613 BlgNR XX. GP, 35.

Hinsicht wohl bis heute in Wissenschaft und Praxis nicht einhellig und schon gar nicht dogmatisch konsistent geklärt scheint: Die (hier sogar unmittelbare) Wirkung einer Grundrechtsgarantie auf der horizontalen Ebene der Beziehungen der Privatrechtssubjekte untereinander. Klargestellt ist die Horizontalwirkung allerdings nur dem Grunde nach. So enthält etwa § 1 Abs 2 DSG 2000 im Hinblick auf Eingriffe in das Grundrecht, die nicht durch "den Staat" (in seiner Hoheitsfunktion) erfolgen, keine näheren Parameter dafür, wann ein berechtigtes Informationsinteresse anderer vorliegt, welches die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegt. „Diesbezüglich sind die einfachgesetzlichen Ausführungsbestimmungen zum Grundrecht, und zwar die §§ 7 und 9, heranzuziehen".[161] Ebenso interpretationsbedürftig erscheint, was unter einer „Beschränkung des Anspruchs auf Geheimhaltung" (§ 1 Abs 2 DSG 2000) - also einem Eingriff in das Grundrecht - überhaupt zu verstehen ist. Insbesondere ist die Kategorie eines Grundrechtseingriffs bei der Verwendung personenbezogener Daten im Rahmen vertragsrechtlicher Beziehungen schwieriger zu erfassen. Damit korrespondiert die gleichwohl vorgelagerte Frage, wie weit der Schutzbereich des „Grundrechts auf Datenschutz" reicht. Jedenfalls ist der Schutzbereich unabhängig vom Eingriff zu definieren. Zumal besonders inter privatos die Weitergabe und Verarbeitung personenbezogener Daten regelmäßig zunächst einmal auf Freiwilligkeit beruht und in gegenseitigem Interesse erfolgt. Gleichzeitig sind diese Interessen nicht immer transparent, was wiederum auf die Beurteilung zurückwirkt, ob tatsächlich freiwilliges Einverständnis vorliegt. Damit ist die Frage nach der Zweckbindung bei der Datenverwendung in zivilrechtlichen Beziehungen angesprochen, die schließlich eine entscheidende Rolle hinsichtlich allfälliger Haftungszurechnungen spielt.

4.8.1 Grundrechtliche Schutz- und Gewährleistungspflichten

Die Entwicklung des Datenschutzrechtes vor dem Hintergrund rasant wachsender technologischer Möglichkeiten steckt schon von ihrer individualrechtlichen Grundkonzeption her in eingriffsabwehrrechtlichen Denkschemen fest, die den realen Verhältnissen nicht gerecht zu werden vermögen. Die Beschäftigung mit datenschutzrechtlichen Entscheidungen erweckt vielfach den Eindruck, es wären die Daten selbst, die es zu schützen gilt, also Datenschutz als Selbstzweck und Legitimation für Datenschützer. Die Schutzbedürftigkeit ist aber vielmehr von den dahinterstehenden Verwendungszusammenhängen und den damit verbundenen Risiken her zu beurteilen. Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person führen zwar dazu, dass der Einzelne Einschränkungen seiner Grundrechte hinzunehmen hat, wenn überwiegende Allgemeininteressen dies rechtfertigen. Der Gesetzgeber muss aber zwischen Allgemein- und Individualinteressen einen angemessenen Ausgleich herstellen. Es scheint daher sachgerecht, den „Datenschutz" nach einem Muster des „Risikorechts" und als „teilhaberechtliche" Konstruktion zu erfassen.[162] Den Staat treffen dabei

[161] Siehe die Erläuterungen zum DSG 2000, EBRV 1613 BlgNR XX. GP, 35.

[162] Ladeur, Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?, DÖV 2009, Jg 62, 45ff.

grundrechtliche Schutzpflichten, die so zu verstehen sind, dass er eine normative Gestaltung vorzunehmen hat, die einen wirksamen Schutz von Grundrechtspositionen auf Ebene der Interaktion Privater bietet. Die Grundrechte enthalten dabei immer nur normative Anordnungen und beziehen sich insofern auf eine bestimmte Gestaltung von Rechtsnormen.[163] Die Grundrechte haben dabei in ihren unterschiedlichen Wirkungsdimensionen Einfluss auf die Entwicklung neuer Technologien und deren Innovationspfade, ungewollte Schäden sollen durch grundrechtliche Schutz- und Gewährleistungspflichten verhindert werden.[164] Die staatliche Schutzpflicht gegenüber der Möglichkeit von Grundrechtsverletzungen erfordert, dass ein Rechtsrahmen geschaffen wird, der die Verwendung von Kommunikationsdaten der Kunden von Anbietern öffentlicher Kommunikationsdienste konform mit dem Grundrecht auf Datenschutz gewährleistet.[165]

In Anlehnung an die These, „gleiche Freiheit" als grundsätzlich positive Freiheit von Menschen durch Menschen im Sinne wechselseitiger Instrumentalisierung zu sehen[166], müssen die grundrechtlichen Verfahrens- und Organisationsmaximen stärker ins Zentrum rücken. Im Kontext moderner Informationstechnologie sind damit Fragen technologischer Sicherungsmechanismen untrennbar verknüpft. So sind etwa Dokumentations- und Informationspflichten und deren tatsächliche Erfüllbarkeit unabdingbare Voraussetzungen eines effektiven Rechtsschutzes im Hinblick auf die Gewährleistung der „informationellen Selbstbestimmung". Angesichts einer für das menschliche Auge gänzlich unüberschaubaren Zahl von Informationsverarbeitungsprozessen in nahezu allen Lebensbereichen, lassen sich diese Aufgaben nur mit Hilfe entsprechender elektronischer Hilfsmittel bewältigen. Ähnliches gilt für Zugriffskontrollen etc. Das moderne Schlagwort hierfür lautet „Information Security Management". Das bedeutet, dass innerhalb einer Organisation - ob nun privat oder staatlich - durch die Definition organisatorischer Abläufe, die eindeutige Benennung der verantwortlichen Personen sowie durch die Verwendung technischer Mittel sicherzustellen ist, dass Informationen nur für jene Zwecke verwendet werden, für die sie erhoben wurden.

[163] Dazu ausführlich Holoubek, Grundrechtliche Gewährleistungspflichten, 259 ff.
[164] So das Resümee einer bemerkenswerten Analyse zum Beitrag der Grundrechte im Hinblick auf eine gesellschaftliche und staatliche Innovationsfolgenverantwortung, 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, 128.
[165] Siehe dieselbe Argumentation bei Kotschy, Datenschutzrechtliche Fragen im Zusammenhang mit dem neuen Verbraucherkreditrecht, ÖBA 2011, 312.
[166]Suhr, Freiheit durch Geselligkeit, EuGRZ 1984, Jg 11, 529.

4.9 Internationale Kooperation[167]

Es gibt eine große Anzahl an bilateralen bzw. multilateralen 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[168] (Schengener Übereinkommen, Schengener Durchführungsübereinkommen, Vertrag von Amsterdam)

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

[167] Lachmayer, Transnationales Polizeihandeln – Demokratische und rechtsstaatliche Herausforderungen der europäischen Polizeikooperation, JBl 2011, 409.

[168] *Lachmayer*, Die Wirkung von “Schengen“ nach innen – Polizeiliche Informationsnetzwerke ohne Grenzen? Juridikum 2009, 104.

(N-SIS) in den Mitgliedstaaten. Die zweite Generation des Systems (SIS II) wurde nach langer Vorlaufzeit schließlich 2013 implementiert.

Vertrag von Prüm (inkl. Beschluss des Rates 2008/615/JI vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (Ratsbeschluss Prüm), bilaterales **"Prüm-like" Abkommen Österreich-USA**[169])

Im Mai 2005 unterzeichneten sieben EU-Mitgliedstaaten den sog. Prümer Vertrag, dem seitdem 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 "Beschluss des Rates 2008/615/JI vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität" (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 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.

Bundesgesetz über die internationale polizeiliche Kooperation (Polizeikooperationsgesetz - PolKG)

[169] *Kunnert*, "Tausche Visafreiheit gegen Datenschutz" - Die neue Polizeikooperation auf Basis des US-Österreichischen "Prüm-like"-Abkommens, Jahrbuch Datenschutzrecht und E-Government 2012, 193; vgl. https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2012_III_89 (01.07.2016)).

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 iSd 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)[170]

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.[171] Dem EuGH ist die Kontrolle der mitgliedstaatlichen Maßnahmen innerhalb dieses Rahmens entzogen, vgl. Art 276 AEUV: *Bei der Ausübung seiner Befugnisse im Rahmen der Bestimmungen des dritten Teils Titel V Kapitel 4 und 5 über den Raum der Freiheit, der Sicherheit und des Rechts ist der Gerichtshof der Europäischen Union nicht zuständig für die Überprüfung der Gültigkeit oder Verhältnismäßigkeit von Maßnahmen der Polizei oder anderer Strafverfolgungsbehörden eines Mitgliedstaats oder der Wahrnehmung der Zuständigkeiten der Mitgliedstaaten für die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der inneren Sicherheit.*

Statuten IKPO-Interpol[172]

Die Internationale Kriminalpolizeiliche Organisation (IKPO-Interpol) mit Hauptsitz in Lyon dient dazu, dass die mehr als 190 Mitgliedsländer allgemeinpolizeiliche und fallbezogene Erkenntnisse in allen Bereichen der Kriminalität schnell und sicher austauschen können. 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 Beamten keine

170 Rieser-Angulo García/Bauer, Polizeiliche und justizielle Zusammenarbeit in der EU (Teil II) - Polizeilicher Informationsaustausch und Datenschutz, SIAK-Journal 2013 H 3, 4.
171 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).
172 Vgl. http://www.interpol.int/About-INTERPOL/Legal-materials/The-Constitution (01.07.2016)).

Exekutivbefugnisse zur Strafverfolgung. Ausschließlich das jeweilige nationale Recht in den Mitgliedstaaten bestimmt, welche exekutiven Maßnahmen zur Strafverfolgung von den eigenen nationalen Beamten durchgeführt werden dürfen.

Europol-Übereinkommen (bzw. seit 2009 Europol-Ratsbeschluss)
Mit dem Europol-Ratsbeschluss (Beschluss des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamtes (Europol), 2009/371/JI) 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 -tätern 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.

4.10 Nachrichtendienstliche Datenverarbeitung

In Österreich bestehen auf Rechtsgrundlage des Militärbefugnisgesetzes (MBG) zwei militärische Nachrichtendienste, das Heeresabwehramt und der Heeresnachrichtendienst (§ 20 MBG). Der polizeiliche Staatsschutz, der in Ausübung der Sicherheitspolizei erfolgt, findet seine Rechtsgrundlage im Polizeilichen Staatsschutzgesetz (PStSG, subsidiär ist das SPG anwendbar). Für die (unbedeutenden) polizeilichen und umfassenden nachrichtendienstlichen Tätigkeiten des Staatsschutzes ist das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT), das als Organisationseinheit der Generaldirektion für die öffentliche Sicherheit eingerichtet ist, zuständig. Daneben bestehen eigene Organisationseinheiten in den Landespolizeidirektionen, die gegenüber dem BVT weisungsgebunden sind, wenn der Bundesminister für Inneres dem BVT Aufgaben vorbehält. In Österreich wurde mit Einführung des PStSG eine international nicht besonders übliche und durchaus problematische Vermischung von polizeilicher Tätigkeit mit nachrichtendienstlicher Tätigkeit einer Sicherheitsbehörde[173] Realität.

[173] Nachdem das BVT für den Bundesminister für Inneres und die Organisationseinheiten in den LPDs für diese tätig werden, sind im Rechtssinne die „Behörden" der Bundesminister für Inneres respektive die jeweilige LPD.

4.10.1 Polizeiliches Staatsschutzgesetz (PStSG)

Der Gesetzesvorschlag zum Polizeilichen Staatsschutzgesetz wurde am 27. Jänner 2016 mit den Stimmen der Regierungsparteien (SPÖ und ÖVP) in der 111. Sitzung des Österreichischen Nationalrates in dritter Lesung angenommen und ist am 01.07.2016 in Kraft getreten (BGBl. I 5/2016). Trotz bis zuletzt anhaltender und berechtigter Kritik aus der Zivilgesellschaft wurden gegenüber dem letzten Abänderungsantrag vom November 2015 nur einige, wenn auch zum Teil begrüßenswerte Nachschärfungen am Gesetzestext vorgenommen. Das Gesetz enthält viele unbestimmte Gesetzesbegriffe und dynamische Verweisungen sowie einen Deliktskatalog (zur Definition des verfassungsgefährdenden Angriffs) der einerseits zu weit gefasst ist, andererseits dem Normadressaten gegenüber große Bedenken im Hinblick auf Verständlichkeit und Transparenz aufwirft. Im Zusammenspiel mit den weiten Ermittlungsbefugnissen und den damit verbundenen massiven Grundrechtseingriffen sowie dem zu schwach ausgestalteten Rechtsschutzsystem ist insgesamt sohin von einem Gesetz zu sprechen, das, nach Ansicht der Verfasser dieses Handbuchs, mit der österreichischen Verfassung nicht in Einklang zu bringen ist. Hervorzuheben sind in diesem Zusammenhang insbesondere die Bestimmungen betreffend die Vertrauenspersonen, die Ermittlung von Verkehrs,- Zugangs- und Standortdaten sowie die unklaren und unzureichenden Regelungen über Höchstspeicherfristen und fehlende Informationspflichten.
Insgesamt ist zu sehen, dass mit dem im Plenum beschlossenen Gesetzestext auf die Kritik der Zivilgesellschaft und diversen Stakeholdern nicht oder nur marginal reagiert wurde. Es hat den Anschein, dass man durch diverse Nachschärfungen bei einzelnen Bestimmungen medial Kapital schlagen und so kritische Stimmen verstummen lassen wollte, sich aber in der Sache eines echten und wirksamen Grundrechtsschutzes nicht angenommen hat.

Aufgrund der massiven grund- und verfassungsrechtlichen Bedenken gegenüber dem Gesetz haben zwei Oppositionsparteien im Juni 2016 eine sog. „Drittelbeschwerde“ gem. Art. 140 Abs 1 Z 2 B-VG beim österreichischen Verfassungsgerichtshof eingebracht, der aufgrund der genannten Bestimmung von einem Drittel der Abgeordneten zum Nationalrat mit einer Gesetzesprüfung befasst werden kann. Mit einer Entscheidung ist nicht vor März 2017 zu rechnen.

Die grund- und verfassungsrechtlich bedenklichen Normen des PStSG bewirken nach Auffassung der Verfasser dieses Handbuchs, entweder für sich oder in ihrem Zusammenwirken einen Eingriff

- In das Datenschutzgrundrecht gemäß § 1 DSG 2000
- in den Schutz der Privatsphäre nach Art 8 EMRK und in den Schutz personenbezogener Daten nach Art 8 EU-Grundrechtecharta
- in den Schutz der Meinungs- und Informationsfreiheit nach Art 10 EMRK
- in das (akzessorische) Recht auf einen effektiven Rechtsschutz nach Art 13 EMRK
- in das Fernmeldegeheimnis nach Art 10a Staatsgrundgesetz 1867 (StGG)

sowie weiters eine Verletzung

- des rechtsstaatlichen Prinzips (Art 18 B-VG) sowie
- des Gleichheitsgrundsatzes nach Art 7 B-VG.

Das Polizeiliche Staatsschutzgesetz sowie die im Zusammenhang stehenden Normen des SPG etablieren ein System der Befugnisse zur Ermittlung, Sammlung und Weiterverarbeitung von personenbezogenen Informationen und Daten zu Verdächtigen und deren Kontakt- und Begleitpersonen. Die verschiedenen Ermittlungsmethoden (z.B.: Observation, verdeckte Ermittlung, Einsatz von Bild- und Tonaufzeichnungsgeräten, Kennzeichenerkennungsgeräten, Auskünfte zu Anschlussinhabern und Nutzern von Internetdiensten) sind dabei nicht grundsätzlich neu, sondern finden sich bereits in der Strafprozessordnung und im Sicherheitspolizeigesetz. Das PStSG stattet die für den Staatsschutz zuständigen Sicherheitsbehörden nun konzentriert mit all diesen Ermittlungsinstrumenten unter wesentlich erleichterten Voraussetzungen ohne gerichtliche Kontrolle und mit einer neuen zentralen Datenanwendung aus. Gleichzeitig wird der Bereich der Prävention – in Abgrenzung zur „Abwehr gefährlicher Angriffe“ nach § 21 SPG – noch weiter als bisher in das Vorfeld krimineller Aktivitäten verlagert, während der Kreis der Betroffenen durch flexible und unbestimmte Gesetzesbegriffe weiter ausgedehnt wird und der Rechtsschutz unzureichend ausgestaltet ist.

Das PStSG normiert viele weitreichende Befugnisse zur Überwachung des Verhaltens und der Kommunikation, sowohl im Bereich der unmittelbar zwischenmenschlichen (z.B.: § 11 Abs. 1 Z 1 bis 3) als auch der elektronischen Interaktion (z.B.: § 11 Abs. 1 Z 5 und 7). Durch die gleichzeitig diffuse Eingrenzung des betroffenen Personenkreises und das schwache Kontroll- und Rechtsschutzsystem erwächst daraus die Gefahr, dass die Daten aus Kommunikationsverläufen behördlich aufgezeichnet und verwertet werden. Damit wird ein Klima geschaffen, in dem die Menschen sich bei der Äußerung der eigenen Meinung ebenso wie beim Konsum von Informationen zur Bildung einer eigenen Meinung auch bei völlig legalen Inhalten immer häufiger selbst beschränken, um mögliche nachteilige Folgen zu vermeiden. Diese Selbstbeschränkung bei der Ausübung der durch Art. 10 EMRK garantierten Meinungs- und Informationsfreiheit wird auch als „chilling-Effekt“ bezeichnet.

Einzelne Bestimmungen des PStSG greifen in materielle Grundrechte ein, manche Grundrechte bzw. Verfassungsbestimmungen werden durch das gesamte System des PStSG und der komplementären Vorschriften des SPG verletzt.

Das Polizeiliche Staatsschutzgesetz weist im Hinblick auf die verfassungsrechtlich gebotene hinreichende Normenbestimmtheit und den effektiven Rechtsschutz schwere Mängel auf. Zentrale Begriffe wie „Gruppierung“, „ideologisch motivierte Kriminalität“ oder „ideologisch motivierte Gewalt“ sind nicht hinreichend bestimmt, obwohl diese

Normenbestandteile wesentliche Voraussetzungen für Grundrechtseingriffe beschreiben. Die umfangreichen Befugnisse der Staatsschutzorgane kommen schon bei abstrakten Gefährdungslagen, auch unterhalb der Schwelle eines „gefährlichen Angriffs" zum Tragen. Im Rechtsschutzsystem hingegen bestehen massive Lücken, sodass nur eine geringe Chance besteht, dass das Problem der unbestimmten Begriffe im Rahmen der Kontrollmechanismen kompensiert wird. Das aus Art 18 B-VG abgeleitete Rechtsstaatsprinzip wird daher verletzt.

Da das gesamte System des PStSG und der komplementären Vorschriften des SPG vor allem aus Rechtsnormen zur Ermittlung personenbezogener Daten besteht und letztlich in einer zentralen Datenanwendung kulminiert, wird das PStSG dazu führen, dass der Kreis der Betroffenen immer weiter ausgedehnt wird (d.h. wahrscheinlich binnen weniger Jahre einen relevanten Teil der österreichischen Bevölkerung ausmachen wird) und gleichzeitig keine wirksamen Kontroll- und Rechtsschutzmechanismen bestehen, mit der solche Tendenzen effektiv zurückgedrängt werden (können). Ohne (effektiven) Rechtsschutz stellt dies einen unverhältnismäßigen Grundrechtseingriff dar, wodurch nicht nur § 1 DSG 2000 verletzt wird, sondern auch Art 10 EMRK, da, wie oben schon kurz erwähnt, aufgrund der weitreichenden Befugnisse zur Überwachung des Verhaltens und der Kommunikation, sowohl im Bereich der unmittelbar zwischenmenschlichen als auch der elektronischen Interaktion, ein Klima geschaffen wird, in dem die Menschen sich bei der Äußerung der eigenen Meinung ebenso wie beim Konsum von Informationen zur Bildung einer eigenen Meinung selbst bei völlig legalen Inhalten immer häufiger selbst beschränken werden, um mögliche nachteilige Folgen zu vermeiden.[174]

Art 8 EMRK (und das akzessorische Recht auf einen effektiven Rechtsschutz nach Art 13 EMRK) werden verletzt, da das PStSG zwar festlegt, welche Arten von Informationen gespeichert, gegenüber welchen Personengruppen Überwachungsmaßnahmen ergriffen und unter welchen Umständen Informationen gesammelt werden dürfen, welches Verfahren dabei einzuhalten ist, nach welcher Zeitdauer erlangte Informationen zu löschen sind, welche Personen auf den Datenbestand zugreifen dürfen, wie die Art und Weise der Speicherung und das Verfahren des Informationsabrufs zu erfolgen haben sowie welche Verwendungszwecke für die abgerufenen Informationen zulässig sind. Aber all diese Regelungen sind unklar, lückenhaft und nicht durch einen effektiven Rechtsschutz abgesichert. Damit genügt das PStSG nicht dem von der EMRK (und vom EGMR anerkannten) intendierten Schutzzweck.

Das Polizeirecht und die Strafprozessordnung sind thematisch eng verbundene Bereiche, die jeweils zu tiefgreifenden Eingriffen in verfassungsmäßig gewährleistete Rechte ermächtigen können. Ein wertender Vergleich der jeweiligen Regelungen ist daher gerechtfertigt. Da der Gesetzgeber für die faktisch ineffiziente Ausgestaltung des

174 Vgl. zu dieser Problematik und ihrer Grundrechtsrelevanz insb. VfGH 27.6.2014, G 47/2012-49 u.a., Rz 167.

Rechtsschutzes im Bereich des PStSG und der komplementären Vorschriften des SPG im Vergleich zur StPO jede sachliche Begründung schuldig geblieben ist, wird das vom VfGH aus dem Gleichheitsgrundsatz gemäß Art 7 B-VG abgeleitete Sachlichkeitsgebot verletzt.

Die Summe der schwerwiegenden Verletzungen des aus Art 18 B-VG abgeleiteten Rechtsstaatsprinzips durch die (in der Drittelbeschwerde) angefochtenen Normen des PStSG sowie des SPG bzw. die darauf basierenden potenziellen Vollziehungsakte erweist sich als massive Verletzung dieses „Baugesetzes der Verfassung" und dadurch als Gesamtänderung der österreichischen Bundesverfassung im Sinne von Art 44 Abs.3 B-VG, sodass das gesamte PStSG sowie die angefochtenen Normen des SPG als verfassungswidrig aufzuheben wären.

Unter dem Aspekt einer „Überwachungs-Gesamtrechnung" wiederum kann das PStSG sowie die komplementären Bestimmungen des SPG als eine jener partiell wirkenden Maßnahmen im Sinne der Judikatur des VfGH gelten, die in Summe bzw. im Ergebnis mit den zahlreichen, seit dem 11.09.2001 erlassenen Überwachungsnormen zu einer „schleichenden Gesamtänderung" der österreichischen Bundesverfassung im Sinne von Art 44 Abs. 3 B-VG geführt haben (könnten). Auch aus diesem Grund wäre, nach Ansicht der Verfasser dieses Handbuchs, das gesamte PStSG sowie die angefochtenen Normen des SPG vom VfGH als verfassungswidrig aufzuheben.

4.11 Militärische Nachrichtendienste nach MBG

Auf Grundlage des Militärbefugnisgesetzes (§ 20 MBG) sind in Österreich zwei militärische Nachrichtendienste eingerichtet, einerseits der Heeresnachrichtendienst (Aufklärung) und andererseits das Heeresabwehramt (Abwehr).

Aus den Erläuterungen zum MBG (76 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXI. GP):

Zu § 22 (Verarbeitung von Daten)[175]:
Im Abs. 1 soll in gleicher Weise wie für den Wachdienst (siehe § 15) ausdrücklich normiert werden, dass militärische Organe und Dienststellen, die mit Aufgaben der

[175] *Probst*, Kompetenzen des Rechtsschutzbeauftragten nach MBG und Rechtsprobleme, in: *Vogl/Wenda*, Grundrechte – Rechtsschutz – Datenschutz, 143; *Raschhofer/Feiler*, Die Online-Durchsuchung, in: *Zankl*, Auf dem Weg zum Überwachungsstaat? 171; *Probst*, Menschenwürde, Personenwürde – Datenschutz nach MBG, Amtshilfe, FS Machacek-Matscher (2008) 353; *Probst/Markel*, Die Auswirkungen der MBG-Novelle 2006 auf die Stellung des Rechtsschutzbeauftragten, in: BMI, Integration – Sicherheit – Rechtsschutz, 149; *Probst*, Die rechtlichen Positionen der Rechtsschutzbeauftragten; gesetzliche Unterschiede und Gemeinsamkeiten, in: BMI, Verfassung – Reform – Rechtsschutz, 169; *Probst*, Bericht über den Rechtsschutz nach §§ 22 und 57 MBG nach der Änderung des MBG 2004, in: BMI, Terror – Prävention – Rechtsschutz, 79; *Probst*, Bericht des Rechtsschutzbeauftragten nach § 57 MBG, in: BMI, Der Rechtsschutzbeauftragte, 55.

nachrichtendienstlichen Aufklärung oder Abwehr betraut sind, zur Wahrnehmung ihrer Aufgaben Daten verarbeiten dürfen. Die Definition des "Verarbeitens von Daten" ergibt sich aus § 4 Z 9 DSG 2000. Die zugrundeliegenden Daten begründen im Hinblick auf ihre Unverzichtbarkeit für die Gewährleistung der Einsatzbereitschaft des Bundesheeres "wichtige öffentliche Interessen" im Sinne des § 1 Abs. 2 bzw. § 9 Z 3 DSG 2000.
Die im Abs. 2 vorgesehenen Auskunftsverpflichtungen öffentlicher Institutionen sind den diesbezüglichen Regelungen im § 53 Abs. 3 SPG für den Exekutivbereich bzw. im § 26 StPO für die Strafrechtspflege weitgehend nachgebildet. Im Zusammenhang mit der in gleicher Weise wie im Sicherheitspolizeigesetz ins Auge gefassten Auskunftspflicht öffentlicher Einrichtungen ist hinsichtlich allfälliger Auskünfte aus der Zentralen Informationssammlung nach § 57 SPG darauf hinzuweisen, dass die Einschränkung der Übermittlungsbefugnis im § 57 Abs. 3 letzter Satz SPG lediglich direkte Auskünfte aus dem Informationssystem selbst (speziell im Wege von "Online"-Verbindungen) betrifft. "Mittelbare" Auskünfte über entsprechende Daten durch die Sicherheitsbehörden an militärische Dienststellen werden daher auch künftig auf der Grundlage des § 56 Abs. 1 Z 5 SPG in Verbindung mit § 22 Abs. 2 des vorliegenden Entwurfes zulässig bleiben. Mit dieser Regelung soll im Übrigen wie im Sicherheitspolizeibereich die Verpflichtung der auskunftsverpflichteten Institutionen zur Amtsverschwiegenheit aufgehoben und diese Auskunftsverpflichtung auf die genannten Identitätsdaten und den ausdrücklichen Anfragegegenstand beschränkt werden. Als Beispiele für "sonstige gesetzliche Verpflichtungen zur Verschwiegenheit", die von der in Rede stehenden Auskunftspflicht unberührt bleiben, sind etwa die spezifischen Verschwiegenheitspflichten der Rechtsanwälte nach § 9 der Rechtsanwaltsordnung, RGBl. Nr. 96/1868, der Ärzte nach § 26 des Ärztegesetzes 1984, BGBl. Nr. 373, oder der Psychotherapeuten und ihrer Hilfspersonen nach § 15 des Psychotherapiegesetzes, BGBl. Nr. 361/1990, zu nennen.
Das Ermitteln personenbezogener Daten durch Observation soll nach Abs. 3 lediglich dann erlaubt sein, wenn eine der taxativ gefassten Voraussetzungen der Z 1 bis 3 vorliegt. Zur Vermeidung von Unklarheiten und Zweifelsfragen soll in der Z 1 im Hinblick auf den Grundsatz der Subsidiarität eines militärischen Einschreitens gegenüber einem Tätigwerden von Organen des öffentlichen Sicherheitsdienstes zur Abwehr vorsätzlicher Angriffe gegen militärische Rechtsgüter (vgl. § 2 Abs. 2 des vorliegenden Entwurfes sowie die diesbezüglichen Erläuterungen) ausdrücklich vorgesehen werden, dass dieser Grundsatz auch bei der Observation uneingeschränkt zum Tragen kommen wird. Hinsichtlich der Datenermittlung durch "Beobachten" ist darauf hinzuweisen, dass eine solche Maßnahme ein bewusstes, systematisches Tätigwerden staatlicher Organe mit dem ausdrücklichen Ziel einer Eruierung spezifischer personenbezogener Daten verlangt. Im Falle bloß zufälliger Beobachtungen oder einer (durchaus auch gezielten) Erhebung nicht-personenbezogener Daten wird daher keine "Observation" im gegenständlichen Sinne vorliegen. Nach Abs. 5 soll die Ermittlung personenbezogener Daten durch den Einsatz von Bild- und Tonaufzeichnungsgeräten ebenfalls ausschließlich auf die in den Z 1 bis 3 taxativ angeführten Fälle beschränkt sein. Auch hier soll in der Z 1 der Grundsatz der Subsidiarität normiert werden. Der Einsatz von Bild- und Tonübertragungsgeräten ist,

sofern im Anschluss an die Übertragung keine Aufzeichnung erfolgt, immer dann erlaubt, wenn die Ermittlung personenbezogener Daten zulässig ist. Es handelt sich hierbei nämlich lediglich um ein Hilfsmittel direkter Überwachung. Unter den Voraussetzungen des Abs. 4 dürfen im Rahmen der verdeckten Ermittlung auch Bild- und Tonaufzeichnungsgeräte eingesetzt und die auf diesem Wege ermittelten Daten aufgezeichnet werden. Die Anwendbarkeit des verfassungsrechtlich verankerten Fernmeldegeheimnisses (Art. 10a des Staatsgrundgesetzes über die allgemeinen Rechte der Staatsbürger, RGBl. Nr. 142/1867) soll jedoch uneingeschränkt aufrecht bleiben. Bei jeglichem Einsatz von Bild- und Tonaufzeichnungsgeräten wird besonders darauf zu achten sein, dass Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit zum Anlass wahren. Dabei wird insbesondere darauf Bedacht zu nehmen sein, dass der angestrebte Erfolg in einem vertretbaren Verhältnis zu den voraussichtlich bewirkten Eingriffen in die Rechte unbeteiligter Dritter steht, und zu prüfen sein, ob nicht auch mit weniger eingreifenden Maßnahmen begründete Aussicht auf den angestrebten Erfolg besteht.
Die im Justizbereich mit Wirkung vom 1. Jänner 1998 neu eingeführte "optische und akustische Überwachung von Personen unter Verwendung technischer Mittel" (sog. "Späh- und Lauschangriff"; § 136 StPO) wird im Bereich der militärischen Landesverteidigung – ebenso wie der "automatische Datenabgleich" (sog. "Rasterfahndung"; § 141 StPO) – in keiner Weise zur Verfügung stehen. Nach Abs. 6 soll nämlich eine Datenermittlung mit Bild- und Tonaufzeichnungsgeräten jedenfalls unzulässig sein, wenn sie im Inland in die "Privatsphäre" von Personen eingreift. Eine vergleichbare, dem § 120 Abs. 1 StGB über den Missbrauch von Tonaufnahme- oder Abhörgeräten weitgehend entsprechende Regelung war als Änderung des § 54 Abs. 4 SPG in nahezu wortgleicher Form in der Regierungsvorlage einer Novelle zum Sicherheitspolizeigesetz vom März 1999 (1708 BlgNr, XX. GP) enthalten.

Die im Abs. 7 vorgesehenen Regelungen sollen der speziellen Prävention hinsichtlich Angriffen gegen militärische Rechtsgüter dienen. Demnach sollen die in Rede stehenden Organe und Dienststellen bei einer Zusammenkunft mehrerer Personen zur Ermittlung personenbezogener Daten mit Bild- und Tonaufzeichnungsgeräten ermächtigt werden, sofern konkrete Hinweise darauf bestehen, dass es bei diesen Zusammenkünften zu derartigen Angriffen kommen werde. Aus Billigkeitsgründen soll der Einsatz derartiger Geräte den betroffenen Personen ausdrücklich anzukündigen sein. Das durch eine solche Maßnahme rechtmäßig ermittelte (Bild- und Ton-) Material soll in weiterer Folge auch zur konkreten Abwehr oder Beendigung dieser Angriffe verwendet werden.

Für den Exekutivbereich wurde mit Wirkung vom 1. Jänner 1998 die sog. "Legende" im Rahmen der Normierung besonderer Ermittlungsmaßnahmen, BGBl. I Nr. 105/1997, in das Sicherheitspolizeigesetz (§ 54a) aufgenommen. Eine entsprechende Norm soll auch im vorliegenden Entwurf (Abs. 8) für verdeckte Ermittlungen im Bereich der militärischen Landesverteidigung vorgesehen werden. Auch für militärische Organe, die mit Aufgaben

der nachrichtendienstlichen Aufklärung oder Abwehr betraut sind, stellt nämlich die Ausstattung mit Urkunden, die über die amtliche Eigenschaft und damit die Identität des Ermittlers täuschen, vielfach eine unabdingbare Voraussetzung für eine erfolgreiche Tätigkeit sowie für den Schutz dieser Organe dar. Die Befugnis zur Verwendung solcher Urkunden soll auf den unbedingt notwendigen Dienst- und Privatbereich eingeschränkt sein; der täuschende Gebrauch solcher Urkunden im (privaten) Rechtsverkehr gegenüber Dritten ohne Vorliegen eines konkreten Ermittlungsauftrages wird daher nicht zulässig sein. Aus Gründen der Nachvollziehbarkeit und Täuschungssicherheit sollen die entsprechenden "Falsifikate" – auf Verlangen des Bundesministers für Landesverteidigung – von den für die Ausstellung der jeweiligen Urkunden an sich zuständigen Behörden hergestellt werden. Aus kompetenzrechtlichen Erwägungen sollen von der in Rede stehenden Maßnahme nur jene Verwaltungsmaterien betroffen sein, die bundesgesetzlich zu regeln sind; im autonomen Wirkungsbereich der Länder wird daher die Schaffung einer "Legende" nicht in Betracht kommen.

Die vorgesehenen besonderen Regelungen über Datenermittlungen im Bereich der militärischen Landesverteidigung entsprechen, unter Bedachtnahme auf die spezifischen Besonderheiten der Aufgaben im militärischen Bereich, hinsichtlich Inhalt und Umfang weitgehend den diesbezüglichen Ermächtigungen im § 54 SPG für Ermittlungen im Sicherheitspolizeibereich.

4.11.1 Rechtsgrundlagen im Überblick

- Bundesverfassungsgesetz (B-VG)
    - Im Besonderen:
        - Art 7 B-VG (Gleichheitsgrundsatz)
        - Art 18 B-VG (Legalitätsprinzip / Rechtsstaatlichkeitsprinzip)
        - Art 44 Abs 3 B-VG (Gesamtänderung der Verfassung)
- Datenschutzgesetz (DSG 2000)
    - Im Besonderen:
        - § 1 DSG (Datenschutzgrundrecht)
- Europäische Menschenrechtskonvention (EMRK)
    - Im Besonderen:
        - Art 8 EMRK (Schutz der Privatsphäre)
        - Art 10 EMRK (Schutz der Meinungs- und Informationsfreiheit)
        - Art 13 EMRK (Recht auf effektiven Rechtsschutz)
- Militärbefugnisgesetz (MBG)
    - Im Besonderen:
        - § 2 Abs 2 MBG (Vorrang SPG)
        - § 3 MBG (Grundsätze der Befugnisausübung)
        - § 4 MBG (Konkretisierung des Verhältnismäßigkeitsgrundsatzes)

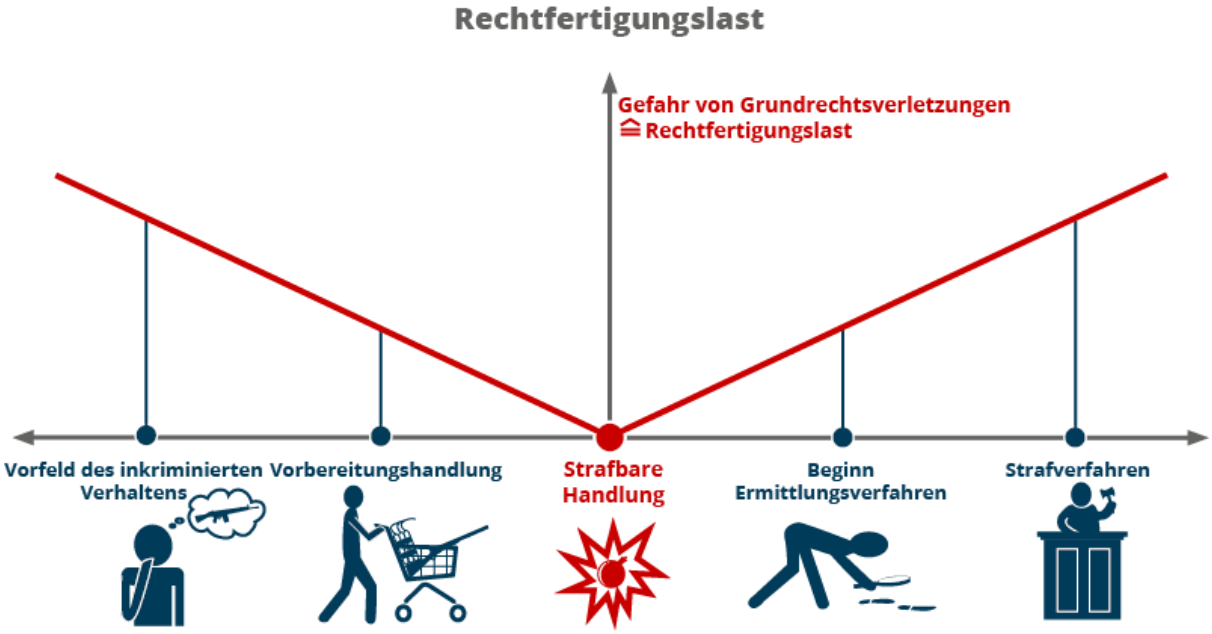
        - § 5 MBG (Rechte der betroffenen Person)
        - § 20 MBG (Nachrichtendienstliche Aufklärung und Abwehr)
        - § 22 (Verarbeitung von Daten)
        - § 25 MBG (Datenübermittlung)
        - § 57 Abs 1 MBG (Rechtsschutzbeauftragter)
- Polizeiliches Staatsschutzgesetz (PStSG)
    - Im Besonderen:
        - § 1 PStSG (Anwendungsbereich)
        - § 6 PStSG (Erweiterte Gefahrenerforschung und Schutz vor verfassungsgefährdenden Angriffen)
        - § 10 PStSG (Ermittlung personenbezogener Daten)
        - § 11 Abs 1 PStSG (Besondere Ermittlungsmethoden)
        - § 12 PStSG (Analysedatenbank)
        - § 14 PStSG (Rechtsschutzbeauftragter)
        - § 16 PStSG (Information Betroffener)
- Sicherheitspolizeigesetz (SPG)
- Staatsgrundgesetz (StGG)
    - Im Besonderen:
        - Art 10a StGG (Fernmeldegeheimnis)
- Strafprozessordnung

5 Rechtswissenschaftliche Analyse

5.1 Grundrechte und Verfassungsrecht

Der gesamte Bereich der Strafverfolgung wie auch der Prävention ist davon geprägt, dass die gesetzlichen Grundlagen eine Vielzahl von Grundrechtseingriffen normieren, die im Hinblick auf die Zwecke der Strafrechtspflege im öffentlichen Interesse liegen und üblicherweise gerechtfertigt sind. Das ändert aber nichts daran, dass den Staat die Rechtfertigungslast trifft, wenn er neue Befugnisse schafft oder bestehende ausweitet, inwiefern die damit verbundenen Grundrechtseingriffe notwendig und verhältnismäßig sind.

Als Faustregel lässt sich aus der kasuistischen Judikatur des EGMR ableiten:
Je weiter weg die in Grundrechte eingreifenden Maßnahmen von der eigentlichen Tat sind, desto größer ist die Last zur Rechtfertigung der Eingriffe auf Seiten des Staates, sowohl generell abstrakt als auch im konkreten Einzelfall. Ein systematisches Problem ist in dieser Hinsicht die immer weitere Ausdehnung polizeilicher Befugnisse in den Bereich der Prävention, der sich immer weiter von konkreten Gefährdungshandlungen entfernt. Gleichzeitig werden die Hürden zur Aktivierung dieser Befugnisse speziell für die Prävention ständig weiter gesenkt, während in der klassischen Strafverfolgung (Aufklärung bereits begangener Straftaten) wohl überlegte und gesicherte Schranken und Safeguards existieren.



5.1.1 Rechtsstaatliches Prinzip und Verfahrens-Grundrechte

Das rechtsstaatliche Prinzip kommt nach herrschender Auffassung insbesondere in der Gesetzesbindung der Vollziehung nach **Artikel 18 B-VG** zum Ausdruck. Für den Gesetzgeber ergibt sich daraus vor allem die Verantwortung, Normen hinreichend bestimmt und klar zu formulieren.

Pflichten und vor allem auch Rechte des/der Einzelnen müssen gesetzlich (möglichst) präzise geregelt und deren Durchsetzung durch entsprechende Institutionen garantiert sein. Durch die Bestimmtheit – genauer: Vorherbestimmtheit – der Rechte und Pflichten durch Gesetz unterscheidet sich der Rechtsstaat von seinem Gegentyp, dem Polizeistaat.

Der EGMR verlangt bei geheimen Überwachungsmaßnahmen, dass das Gesetz in seinen Bestimmungen hinreichend klar sein muss, um dem Bürger adäquate Hinweise über die Bedingungen und Umstände zu geben, unter denen die Behörden befugt sind, in das Recht auf Achtung des Privatlebens und des Briefverkehrs einzugreifen.[176] Im Hinblick auf das Missbrauchsrisiko, da jedem geheimen Überwachungssystem innewohnt, müssen solche Maßnahmen auf einem besonders präzisen Gesetz beruhen. Es ist notwendig, klare, detaillierte Bestimmungen in dieser Sache zu haben, insbesondere da die zur Verfügung stehende Technologie immer komplexer wird.[177]

Das der österreichischen Rechtsordnung immanente Konzept des „Fehlerkalküls" (Adolf Julius Merkl) antizipiert, dass in der Praxis des Rechts Fehler unvermeidbar sind und daher entsprechende Rechtsschutzsysteme geschaffen werden müssen, um einen Rechtsstaat zu etablieren. In diesem Sinne ist auch das in **Artikel 13 EMRK** ausdrücklich verfassungsgesetzlich verankerte Gebot eines effektiven Rechtsschutzes eine wesentliche Säule des rechtsstaatlichen Prinzips.

Der Begriff „rechtsstaatliches Prinzip" fand 1949 erstmals Eingang in die Begründung eines Erkenntnisses des VfGH.[178] Schon drei Jahre später qualifizierte der VfGH das rechtsstaatliche Prinzip als leitenden Grundsatz der Bundesverfassung, dessen Abänderung als Gesamtänderung der Bundesverfassung zu qualifizieren ist: „Dem rechtsstaatlichen Prinzip entspricht es, dass alle Akte staatlicher Organe im Gesetz und

[176] EGMR Urteil Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, §§ 74-75 unter Verweis auf die Urteile Malone gg. das Vereinigte Königreich, § 67; Valenzuela Contreras gg. Spanien, § 46; und Khan gg. das Vereinigt Königreich, § 26.
[177] EGMR Urteil Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, §§ 74-75 unter Verweis auf die Urteile Kruslin gg. Frankreich, § 33; Huvig gg. Frankreich, § 32; Amann gg. die Schweiz, § 56; und Weber und Saravia gg. Deutschland, § 93.
[178] VfSlg 1804/1949. Der VfGH vertrat die Ansicht, dass das AVG in der Wahrung des Parteiengehörs „*in verfahrensrechtlicher Beziehung einer der wichtigsten Sicherungen des rechtsstaatlichen Prinzips*" erblicke.

mittelbar letzten Endes in der Verfassung begründet sein müssen, und dass für die Sicherung dieses Postulates wirksame Rechtsschutzeinrichtungen bestehen".[179] Das Gebot des effektiven Rechtsschutzes blieb die zentrale Konstante in der Rechtsstaatsjudikatur des VfGH[180].

In seinem Erkenntnis VfSlg 11.196/1986 führte der VfGH Grundsätzliches zur faktischen Effektivität des Rechtsschutzes aus:

„Der VfGH kann von seiner im Prüfungsbeschluss bezogenen ständigen Judikatur zum rechtsstaatlichen Prinzip ausgehen (….). Ihr zufolge gipfelt der Sinn des rechtsstaatlichen Prinzips darin, dass alle Akte staatlicher Organe im Gesetz und mittelbar letzten Endes in der Verfassung begründet sein müssen und ein System von Rechtsschutzeinrichtungen die Gewähr dafür bietet, dass nur solche Akte in ihrer rechtlichen Existenz als dauernd gesichert erscheinen, die in Überstimmung mit den sie bedingenden Akten höherer Stufe erlassen wurden. Der Gerichtshof bleibt auch bei der im Einleitungsbeschluss an diese Annahme geknüpften Annahme, dass die hier unabdingbar geforderten Rechtsschutzeinrichtungen ihrer Zweckbestimmung nach ein bestimmtes Mindestmaß an faktischer Effizienz für den Rechtsschutzwerber aufweisen müssen. Zunächst ist hierzu die Klarstellung geboten, dass von faktischer Effizienz deshalb die Rede ist, weil unter Effizienz allein unter Umständen bloß das letzten Endes bewirkte erreichen einer Entscheidung rechtsrichtigen Inhalts durch das Ergreifen von Rechtsbehelfen verstanden werden könnte, nicht aber auch die mitgemeinte Übersetzung einer solchen Entscheidung in den Tatsachenbereich. ‚Schutz' als Teilaspekt des Ausdrucks ‚Rechtsschutz' ist auf den Rechtsunterworfenen bezogen und meint nicht zuletzt die – rechtzeitige – Wahrung und Gewährleistung einer faktischen Position, weshalb Rechtsschutzeinrichtungen diesen Zweck notwendig in sich schließen. Der VfGH hält im Hinblick auf diesen Inhalt des Begriffes Rechtsschutzeinrichtung, mithin insbesondere des Begriffs Rechtsbehelf, auch an der Ansicht fest, dass es nicht angeht, den Rechtsschutzsuchenden generell einseitig mit allen Folgen einer potenziell rechtswidrigen behördlichen Entscheidung solange zu belasten, bis sein Rechtsschutzgesuch endgültig erledigt ist. Zu berücksichtigen ist in diesem Zusammenhang allerdings nicht nur seine Position, sondern auch – Zweck und Inhalt der Regelung, ferner die Interessen Dritter sowie schließlich das öffentliche Interesse. Der Gesetzgeber hat unter diesen Gegebenheiten einen Ausgleich zu schaffen, wobei aber dem Grundsatz der faktischen Effektivität eines Rechtsbehelfs der Vorrang zukommt und dessen Einschränkung nur aus sachlich gebotenen, triftigen Gründen zulässig ist."

Diesen Grundgedanken bekräftigte der VfGH in seiner Entscheidung VfSlg 13.182/1992, in der er ausführte, dass

179 VfSlg 2455/1952

180 Vgl. *Hiesel*, Die Rechtsstaatsjudikatur des Verfassungsgerichtshofes, ÖJZ 1999,522 (Heft 14-15)

„… gesetzliche Regelungen, die sachlicher Weise dazu führen, dass ein behördliches Fehlverhalten vorläufig hingenommen werden muss, (…) – wenn es irgendwie vermeidbar ist –, nicht so ausgestaltet werden (dürfen), dass daraus endgültige Belastungen entstehen".

Die Kombination aus der mangelnden Bestimmtheit wichtiger Eingriffsvoraussetzungen und einem schwachen Rechtsschutz erzeugt ein hohes Risiko, dass das dichte Netz der Überwachungsbefugnisse (siehe Überblick in Kapitel V. 5.5.2) auf immer weitere Teile der Bevölkerung ausgeworfen wird. Die in der Vergangenheit öffentlich bekannt gewordenen Beispiele, bei denen die Staatsanwaltschaft Wiener Neustadt bzw. die Kriminalpolizei gegen Tierschützer des Vereins gegen Tierfabriken (VGT) oder das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) gegen Mitglieder der studentischen Protestbewegung „Uni brennt" wegen Mitgliedschaft zu einer terroristischen Vereinigung (§ 278b StGB) ermittelt hat, zeigen, dass dieses Risiko sehr real und naheliegend ist.

5.1.2 Grundsatz der Verhältnismäßigkeit

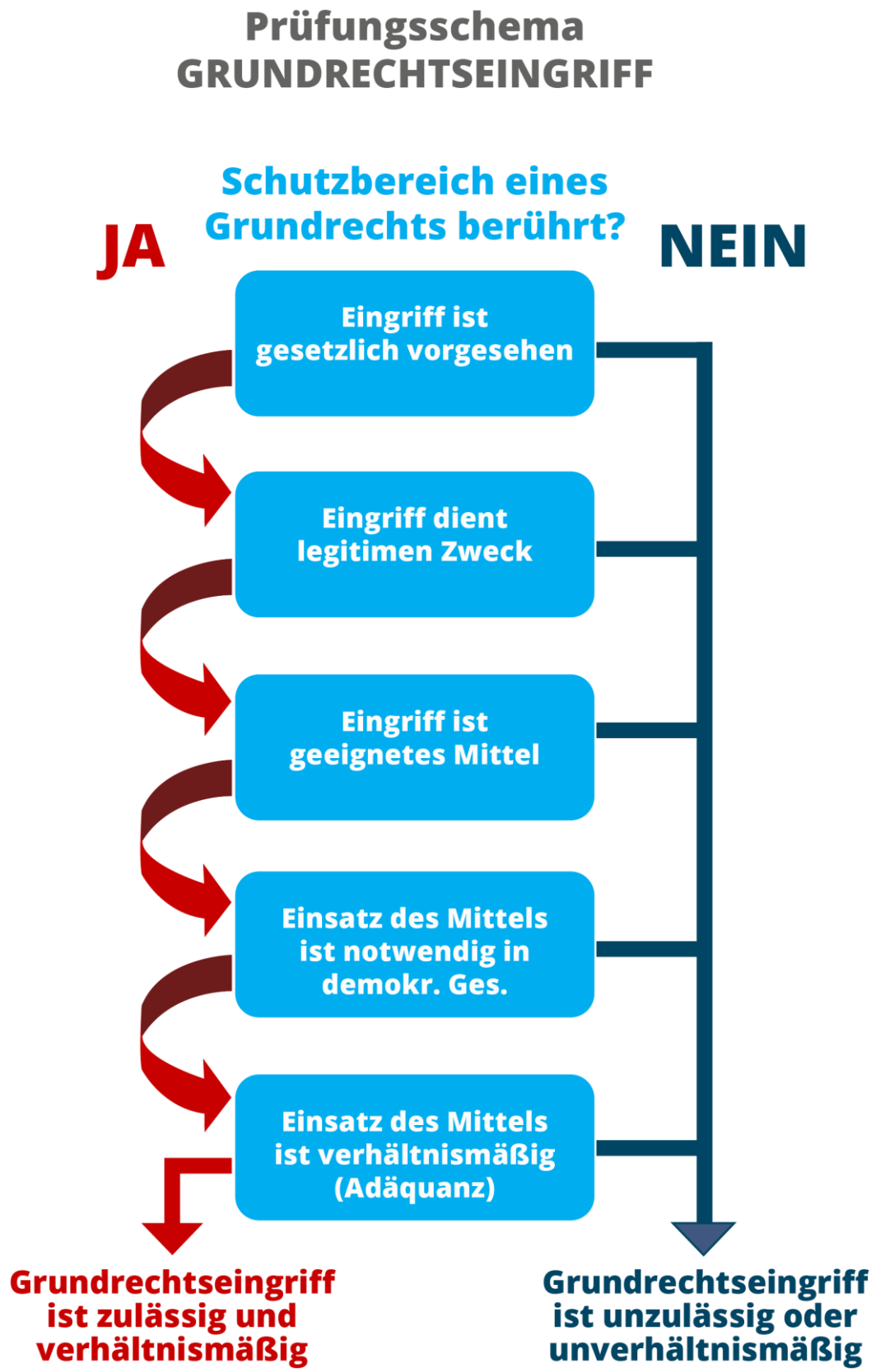
HEAT folgt dem klassischen Schema zur Prüfung der Verhältnismäßigkeit bei Grundrechtseingriffen. Geprüft wird, in welches verfassungsgesetzlich gewährleistete Recht durch die jeweils beleuchtete Norm eingegriffen wird. Dem folgt die Frage, welchen (allenfalls mehreren) legitimen Zielen der Eingriff jeweils dienen soll und ob die gewählte Maßnahme geeignet ist, das jeweilige Ziel zu erreichen. Darüber hinaus wird geprüft, ob das gewählte Mittel in einer demokratischen Gesellschaft erforderlich ist oder ob gelindere Mittel zur Verfügung stehen, die angestrebten Ziele im selben Maß zu erreichen. Den Abschluss bildet die Prüfung der Adäquanz, bei der die Verhältnismäßigkeit im engeren Sinn einer eigentlichen Güterabwägung geprüft wird.

Diese Ebenen der Verhältnismäßigkeitsprüfung korrelieren. Wenn zum Beispiel die Eignung eines Grundrechtseingriffs zur Zielerreichung abstrakt zwar durchaus fragwürdig, aber nicht auszuschließen ist (Stichwort „Vorsorgeprinzip"), bedarf es zur Adäquanz regelmäßig eines sehr hochwertigen Schutzgutes und möglichst konkreter Bedingungen. Diese Korrelation ist bei der Grundrechtsprüfung zu berücksichtigen.

Die Prüfung der Verhältnismäßigkeit von Grundrechtseingriffen wird in der Grundrechtswissenschaft durch folgendes Frageschema gekennzeichnet, das aus der ständigen Praxis der europäischen und nationalen Höchstgerichte ableitbar ist:

- Ist die Datenverarbeitung ein Eingriff in die informationelle Selbstbestimmung?
- Ist der Eingriff gesetzlich vorgesehen und hinreichend bestimmt?
- Dient der Eingriff einem legitimen Ziel?
- Ist die Datenverarbeitung abstrakt geeignet, den Zweck zu erreichen?
- Gibt es gelindere Mittel, den Zweck zu erreichen?

- Besteht ein angemessenes Verhältnis zwischen nachteiligen Konsequenzen und Nutzen?



Liegt eine gesetzliche Grundlage der fraglichen Maßnahme nach den genannten Kriterien vor, so muss die Maßnahme nach Art 8 Abs 2 EMRK zusätzlich 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 sein. Die einzelnen Staaten haben nach der Rechtsprechung des Gerichtshofs einen Beurteilungsspielraum bezüglich der Frage, ob eine Maßnahme zu einem der in Art 8 Abs 2 EMRK genannten Zwecke notwendig ist. Hinter der Formulierung „in einer demokratischen Gesellschaft (...) notwendig" verbirgt sich der Grundsatz der Verhältnismäßigkeit, wie er in vergleichbarer Weise auch bei vielen Grundrechten nationaler Verfassungen als Bedingung für die Zulässigkeit von Grundrechtseingriffen normiert ist.[181]

In einer demokratischen Gesellschaft notwendig ist eine Maßnahme nur, wenn ein in Anbetracht des Stellenwerts des garantierten Freiheitsrechts hinreichend „dringendes soziales Bedürfnis" nach ihr besteht, sie einen legitimen Zweck verfolgt und ihre Eingriffsintensität nicht außer Verhältnis zu dem Gewicht des Zwecks steht.[182] Der EGMR hat dazu eindeutig erklärt, dass das Interesse des Staates gegenüber den Interessen des Einzelnen an der Achtung seiner Privatsphäre abgewogen werden müsse.[183] Eingriffe sind zwar nicht auf das unerlässliche Maß beschränkt, aber ein bloßes Nützlichsein oder Wünschenswertsein genügt nicht.[184] Sind die genannten Kriterien erfüllt, so liegt keine Verletzung von Art 8 EMRK vor. Eine Beschränkung von Grundrechten ist nur insoweit zulässig, als sie zur Erreichung des angestrebten Zweckes geeignet und erforderlich ist, und der Eingriff seiner Intensität nach nicht außer Verhältnis zur Bedeutung der Sache und den von den Betroffenen hinzunehmenden Einbußen steht.

Zur Beurteilung der Verhältnismäßigkeit von Grundrechtseingriffen ist wesentlich, unter welchen Voraussetzungen welche und wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind. Maßgebend sind also insbesondere die Gestaltung der Einschreitschwellen, die Zahl der Betroffenen (Streubreite des Eingriffs) und die Intensität der Beeinträchtigungen. Im Bereich der Telekommunikationsüberwachung ist von Bedeutung, ob die Betroffenen als Personen anonym bleiben, welche Informationen erfasst werden können und welche Nachteile den Grundrechtsträgern aufgrund der Überwachungsmaßnahme drohen. Auf Seiten der mit dem Eingriff verfolgten Zwecke ist das Gewicht der Ziele maßgeblich, denen die Telekommunikationsüberwachung dient. Es hängt unter anderem davon ab, wie bedeutsam die Rechtsgüter sind, die mit Hilfe der Maßnahme geschützt werden sollen und wie wahrscheinlich der Eintritt einer Rechtsgutverletzung ist.[185]

---

[181] Grabenwarter, EMRK[4], § 18 Rz 14, S. 116.

[182] EGMR 25.03.1983 Silver gg. das Vereinigte Königreich = EuGRZ 1984, S. 147 ff.

[183] EGMR 26.03.1987 Leander gg. Schweden.

[184] EGMR 25.03.1983 Silver gg. das Vereinigte Königreich = EuGRZ 1984, S. 147 ff.

[185] So auch das deutsche Bundesverfassungsgericht in BVerfGE 100, 313 (375 f).

Es ist also ersichtlich, dass insbesondere die Streubreite bestimmter Überwachungsmaßnahmen einen entscheidenden Einfluss auf die Beurteilung der Verhältnismäßigkeit hat:

5.1.3 Datenschutz als Katalysator

Der im Verfassungsrang stehende § 1 Abs. 1 DSG normiert:
„Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht.“
Mit „Jedermann“ ist jede natürliche und juristische Person gemeint. Der Anspruch auf Geheimhaltung bedeutet das Recht, dass keine Daten an Dritte übermittelt werden und

Daten nicht von Dritten ermittelt werden.[186] Auch bei Inhalts-, Verkehrs-, und Standortdaten handelt es sich um „personenbezogene Daten", an denen ein schutzwürdiges Interesse an deren Geheimhaltung bestehen kann. Insofern könnte § 93 TKG auch als konkrete, einfachgesetzliche Ausgestaltung des Grundrechts auf Datenschutz gesehen werden, dem nach § 1 Abs 5 DSG 2000 auch unmittelbare Drittwirkung gegenüber Privaten zukommt.[187] Im Gegensatz zu Art 10a StGG und auch zu § 93 TKG 2003 ist der Geheimnisbegriff des § 1 DSG materiell zu verstehen[188]. Insofern stehen personenbezogene Daten, die bereits allgemein bekannt sind – unabhängig davon, ob sie als Inhalts-, Verkehrs-, oder Standortdaten anfallen – nicht unter dem grundrechtlichen Schutz des Art 1 Abs 1 DSG, sind aber sehr wohl vom Kommunikationsgeheimnis nach § 93 TKG 2003 erfasst und im Fall von Verkehrs- und Standortdaten jedenfalls nach Ansicht der Autoren dieses Handbuchs – auch von Art 10a StGG geschützt. Die aus Art 1 § 1 DSG ableitbaren Schutzpflichten der Anbieter werden in den datenschutzrechtlichen Bestimmungen der §§ 96 ff TKG (strenge Zweckbindung, Datensparsamkeit, Auskunft, Löschungspflicht) weiter konkretisiert.

Der in Art 1 § 1 DSG ausdrücklich genannte Anspruch auf Achtung des „Privat- und Familienlebens" ist primär durch Art 8 EMRK geschützt, weshalb in materieller Hinsicht das Datenschutzgrundrecht auch durch Art 8 EMRK und die Rechtsprechung des EGMR zu diesem Grundrecht ausgeprägt ist. Wenngleich die beiden Grundrechtsgarantien auch einen völlig eigenständigen Charakter haben, wird aus diesem Grund der Schwerpunkt der Ausführungen in diesem Handbuch auch auf diese Norm und die Rechtsprechung des EGMR dazu gelegt. Wesentlich ist die Einsicht, dass Datenschutz kein Selbstzweck ist, sondern vielmehr eine Art „Katalysator" für jede erdenkliche Grundrechtsposition (insb. das Recht auf Schutz der Privatsphäre und das Recht auf freie Meinungsäußerung) oder auch sonstige schutzwürdige Interessen einer Person, deren Daten verarbeitet werden. Für die Verhältnismäßigkeitsprüfung im Datenschutz ist es daher notwendig, die konkreten Risiken einer Datenverarbeitung für die Betroffenen zu reflektieren, weil ansonsten nicht klar ist, welche Interessen eigentlich abgewogen werden sollen.

5.1.4 Privatsphäre

Art 8 EMRK garantiert:
„Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs."

[186] Lehner, Recht auf Datenschutz, in: Heißl (Hrsg.), Handbuch Menschenrechte, 213; dort findet sich insgesamt eine sehr übersichtliche Darstellung des Datenschutzgrundrechts mit ausführlichen Judikaturnachweisen.
[187] Dohr (u.a.), Art 1 § 1, DSG Kommentar, 2008[2],8.Er.-Lfg., 19.
[188] OGH, JBl 1995, 332; Damjanovic (u.a.), Handbuch des Telekommunikationsrechts (2006), 242.

Dadurch werden die wesentlichen Ausdrucksmöglichkeiten der Persönlichkeit geschützt sowie ein Grundsatz der Selbstbestimmung normiert.[189] Der Schutzbereich des Rechts auf Privatleben iSd Art 8 EMRK umfasst jedenfalls ein Abwehrrecht gegen die staatliche Erforschung der Privatsphäre. Die Möglichkeiten der modernen computergestützten Sammlung und Verwertung von Informationen machen den Schutz persönlicher Daten zu einem wichtigen Teilbereich der Gewährleistungen des Art 8 EMRK.[190] Darüber hinaus garantiert Art 8 EMRK auch ein Recht auf Achtung des Briefverkehrs. Davon umfasst sind private und nicht-private schriftliche Mitteilungen, wobei sich der Schutz auf den Kommunikationsvorgang –sowie den Kommunikationsweg einerseits und auf die infolge der Kommunikation gespeicherten Mitteilungen andererseits erstreckt.[191] Vorbild ist der Schutz des Briefverkehrs: Die nichtöffentlichen Mitteilungen einer Person an eine andere sollen vor Eingriffen des Staates geschützt werden. Daher fallen unter den Begriff des Briefverkehrs im Sinne des Art 8 EMRK auch die Kommunikation per E-Mail und das Telefonieren über das Internet.[192]

Der EGMR hat bereits wiederholt entschieden, dass auch Telefongespräche als „Briefverkehr/Korrespondenz" iSd Art 8 EMRK anzusehen sind.[193] Art 8 EMRK schützt dabei sowohl geschäftliche als auch private Kommunikation.[194] Aus der Rechtsprechung des EGMR ergibt sich klar, dass auch „äußere Gesprächsdaten", also gewählte Nummer, Zeitpunkt und Dauer der Kommunikation, vom Schutzbereich des Art 8 EMRK umfasst sind und ein Eingriff in dieses Grundrecht insbesondere auch dann vorliegt, wenn solche Daten ohne Zustimmung des Betroffenen an staatliche Behörden übermittelt werden.[195] Dies gilt neben Telefonaten auch für die Erhebung von näheren Umständen der E-Mail-Nutzung und der Internetnutzung.[196] Sowohl die Erhebung wie auch die Speicherung dieser Daten stellen einen Grundrechtseingriff dar, selbst wenn die Daten auf legalem Wege erlangt werden.[197]

Ein System geheimer Überwachungs- und Ermittlungsbefugnisse zur Wahrung der nationalen Sicherheit ist auch nach ständiger Rechtsprechung des EGMR an den Vorgaben des Art 8 EMRK zu messen. Zuletzt hat der EGMR in der Rechtssache Szabó und Vissy v. Ungarn[198] das zentrale Risiko eines solchen Systems auf den Punkt gebracht:

---

[189] Heißl, Recht auf Privatleben, in: Heißl (Hrsg.), Handbuch Menschenrechte, 161, mit einer umfassenden und übersichtlichen Darstellung zu Art 8 EMRK.
[190] Grabenwarter, Europäische Menschenrechtskonvention, 4. Auflage, 2009, Art 8 Rz 10.
[191] Vgl. Grabenwarter, Europäische Menschenrechtskonvention, 4. Auflage, 2009, Art 8 Rz 24.
[192] EGMR 22.10.2002 Taylor–Sabori gg. das Vereinigte Königreich.
[193] EGMR 04.05.2000 Rotaru gg. Rumänien = ÖJZ 2001, S. 74 ff.
[194] EGMR 16.12.1992 Niemietz gg. Deutschland = NJW 1993, S. 718.
[195] EGMR 02.08.1984 Malone gg. das Vereinigte Königreich, RN. 83 f.= EuGRZ 1985, S. 17ff.
[196] EGMR 03.07.2007 Copland gg. das Vereinigte Königreich = EuGRZ 2007, S. 415ff.
[197] EGMR 03.07.2007 Copland gg. das Vereinigte Königreich = EuGRZ 2007, S. 415ff.
[198] EGMR Szabó und Vissy v. Ungarn, Urteil 12.1.2016, Bspw. Nr. 37138/14.

„In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse."[199]

Schon kurz davor hat der EGMR in der Rechtssache Roman Zakharov v. Russland[200] strikte Eingrenzungskriterien beschrieben und hat dabei Folgendes verlangt: *„reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security."*[201]

Um dies sicherzustellen, fordert der Gerichtshof die folgenden Mindestsicherungen, die ausdrücklich im kodifizierten Recht angeordnet werden müssen, um Missbrauch zu vermeiden:

- Das Wesen der Straftaten, die Anlass zu einem Abhörbeschluss geben können;
- eine Definition jener Personengruppen, deren Kommunikation überwacht werden kann;
- eine Begrenzung der Dauer einer solchen Überwachung; das Verfahren, nach dem bei der Untersuchung, Verwendung und Speicherung der erlangten Daten vorgegangen wird;
- die Schutzmaßnahmen, die zur Anwendung kommen, wenn die Daten an Dritte übertragen werden;
- und die Umstände, unter denen die erlangten Daten gelöscht oder die Aufnahmen vernichtet werden können oder müssen.[202]

Für den Fall einer Informationssammlung und -speicherung durch einen Geheimdienst wurde ähnlich entschieden, dass nämlich das nationale Recht detailliert festlegen muss,

- welche Arten von Informationen gespeichert werden dürfen;
- gegenüber welchen Personengruppen Überwachungsmaßnahmen ergriffen werden dürfen;
- unter welchen Umständen Informationen gesammelt werden dürfen;
- welches Verfahren dabei einzuhalten ist;
- nach welcher Zeitdauer erlangte Informationen zu löschen sind;
- welche Personen auf den Datenbestand zugreifen dürfen;
- die Art und Weise der Speicherung;
- das Verfahren des Informationsabrufs
- sowie die zulässigen Verwendungszwecke für die abgerufenen Informationen.[203]

[199] EGMR Szabó und Vissy v. Ungarn, Rn 57.
[200] EGMR Roman Zakharov v. Russland, Urteil (große Kammer) 4.12.2015, Bspw. Nr. 47143/06.
[201] EGMR Roman Zakharov v. Russland, Rn 260.
[202] EGMR Urteil Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, § 76, unter Verweis auf das Urteil Weber und Saravia gg. Deutschland, § 95, mit weiteren Rechtsprechungshinweisen.
[203] EGMR Rotaru gg. Rumänien, Urteil 4.5.2000, Bsw. Nr. 28341/95.

5.1.5 Meinungs- und Informationsfreiheit

Artikel 10 EMRK garantiert:
„Jedermann 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.“

Die österreichische Rechtsordnung normiert viele weitreichende Befugnisse zur Überwachung des Verhaltens und der Kommunikation, sowohl im Bereich der unmittelbar zwischenmenschlichen (z.B.: § 11 Abs 1 Z 1 bis 3 PStSG) als auch der elektronischen Interaktion (z.B.: § 11 Abs 1 Z 5 und 7 PStSG). Durch die regelmäßig diffuse Eingrenzung des betroffenen Personenkreises und das schwache Kontroll- und Rechtsschutzsystem im Bereich des SPG und des PStSG entsteht daraus eine latent drohende Gefahr, dass die Daten aus Kommunikationsverläufen behördlich aufgezeichnet und verwertet werden. Damit wird ein Klima geschaffen, in dem die Menschen sich bei der Äußerung der eigenen Meinung ebenso wie beim Konsum von Informationen zur Bildung einer eigenen Meinung selbst bei völlig legalen Inhalten immer häufiger selbst beschränken, um mögliche nachteilige Folgen zu vermeiden. Diese Selbstbeschränkung bei der Ausübung der durch Art 10 EMRK garantierten Meinungs- und Informationsfreiheit wird auch als „chilling effect“ bezeichnet.

In dieser Hinsicht hat der EGMR im Urteil Rotaru gg. Rumänien[204] erkannt, dass bereits eine einschüchternde Wirkung einer Maßnahme einen Eingriff in das Grundrecht darstellen kann. Der Eingriff in die Meinungs- und Informationsfreiheit ist eben typischerweise nicht direkt und beruht auf einem empirischen sozialwissenschaftlichen Argument.

5.1.6 Verfahrensgrundrechte und Zusammenhänge (Beweisverwertung)

Neben dem aus der Rechtsordnung abgeleiteten Rechtsstaatsprinzip garantiert die in Österreich im Verfassungsrang stehende Europäische Menschenrechtskonvention (EMRK) spezifische Verfahrensgrundrechte durch Art 6 EMRK mit den Garantien eines fairen Verfahrens[205] sowie Art 13 EMRK, der immer in Verbindung mit einem bestimmten Konventionsgrundrecht ein Recht auf „eine wirksame Beschwerde bei einer nationalen Instanz“ garantiert. Allerdings ist der Zusammenhang zwischen den materiellen Grundrechten und den Verfahrensgrundrechten nicht trivial.

[204] EGMR, Wille v. Litauen, Urteil 28.10.1999, Bsw. Nr. 28396/95.
[205] Anwendbar ist Art 6 EMRK in Verfahren zur Geltendmachung zivilrechtlicher Ansprüche oder im Verfahren über die Stichhaltigkeit der gegen einen Betroffenen erhobenen strafrechtlichen Anklage.

Schwierigkeiten bereitet die Frage des Zusammenhangs vor allem dann, wenn es um die Verwertung von rechtswidrig erlangten Beweisen geht. Grundsätzlich ist zwischen Beweiserhebungsverboten und Beweisverwertungsverboten zu unterscheiden. Die Normierung von Beweisverwertungsverboten ist grundsätzlich Sache des nationalen Gesetzgebers, der EGMR betont in solchen Fällen immer wieder, dass es nicht seine Kompetenz sei, allgemeine Beweisverwertungsverbote zu judizieren, sondern die EMRK lediglich verlange, dass ein Verfahren insgesamt fair sei. In diesem Licht ist zu sehen, dass es auch beim EGMR kaum Fälle gibt, bei denen eine Verletzung von Art 8 EMRK (Privatsphäre, Datenschutz) bei der Beweisgewinnung automatisch zu einem unfairen Verfahren und einer Verletzung von Art 6 EMRK führt, wenn solche Beweise in der Folge auch verwertet werden. Das heißt, der EGMR stellt dann zwar eine Verletzung des Art 8 EMRK fest, die Verwendung der dabei gewonnenen Beweise bewirkt aber keine Verletzung des Art 6 EMRK. Bislang wurde allein im EGMR Urteil Allan gegen UK[206] ein Beweisverwertungsverbot nach einer Art 8 EMRK Verletzung judiziert. Die Besonderheit in diesem Fall lag allerdings darin, dass der Betroffene hier in Untersuchungshaft saß und ein Zellengenosse als Spitzel eingeschleust worden war, der den Betroffenen zu einem Geständnis verleitete. Aufgrund der besonderen psychischen Verfassung in einer Haftsituation entschied der EGMR, dass die geheime Aufzeichnung und Verwendung dieses Geständnisses das Verbot zum Zwang zur Selbstbezichtigung („nemo tenetur Prinzip“) und daher Art 6 EMRK verletze.

5.1.6.1 Sonderproblem „Geheimnisträger“

Insbesondere Auskünfte über Verkehrsdaten von Telekommunikationsverbindungen, und ganz ähnlich auch Eingriffe in das Bankgeheimnis, beinhalten grundsätzlich die Gefahr, dass dadurch gesetzlich anerkannte Verschwiegenheitspflichten und Berufsgeheimnisse umgangen werden (Redaktionsgeheimnis, geistliche Verschwiegenheit, Ärzte, Rechtsanwälte,...). Dieses Problem hat schon bisher bestanden, bekommt aber durch die stetige Ausweitung von Überwachungsbefugnissen bei gleichzeitig schwachem Rechtsschutz eine neue Dimension.

Dementsprechend führt auch das deutsche Bundesverfassungsgericht in dem die deutsche Umsetzung der Vorratsdatenspeicherung aufhebenden Urteil zu 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 238, aus:

„Verfassungsrechtlich geboten ist als Ausfluss des Verhältnismäßigkeitsgrundsatzes jedoch, zumindest für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen ein grundsätzliches Übermittlungsverbot vorzusehen. Zu denken ist hier etwa an Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen

[206] EGMR, Allan v. United-Kingdom, Urteil 5.11.2002, Bspw. Nr. 48539/99.

anbieten und die selbst oder deren Mitarbeiter insoweit anderen Verschwiegenheitsverpflichtungen unterliegen (vgl. § 99 Abs. 2 TKG).“

Weitere Ausführungen zu diesem Problem enthält das Urteil keine. Insbesondere wird dort auch nicht erwähnt, ob solche Ausnahmen an die Provider (also im TKG) oder an die Ermittlungsbehörden (also in StPO bzw. SPG) zu adressieren sind. Der Verweis auf § 99 Abs 2 dt. TKG bezieht sich nämlich nur auf die Regelung zum Einzelgesprächsnachweis. Zur Frage, in welchen Materien und auf welche Weise ein Umgehungsverbot effektiv geregelt werden könnte, nachfolgend einige Überlegungen mit Bezug auf den Status Quo:

Umgehungsverbote und Nichtigkeitsgründe in der StPO:

Nach § 144 StPO dürfen Ermittlungsmaßnahmen bei sonstiger Nichtigkeit des Verfahrens nicht zur Umgehung der geistlichen Amtsverschwiegenheit (§ 144 Abs 1 StPO) oder sonstiger Aussageverweigerungsrechte (§§ 144 Abs 2 iVm 157 Abs 1 Z 2 bis 4 StPO) angeordnet werden. Geschützt sind nach § 157 Abs 1 Z 2 bis 4 StPO:
2. Verteidiger, Rechtsanwälte, Patentanwälte, Notare und Wirtschaftstreuhänder über das, was ihnen in dieser Eigenschaft bekannt geworden ist,
3. Fachärzte für Psychiatrie, Psychotherapeuten, Psychologen, Bewährungshelfer, eingetragene Mediatoren nach dem Zivilrechts-Mediations-Gesetz, BGBl. I Nr. 29/2003, und Mitarbeiter anerkannter Einrichtungen zur psychosozialen Beratung und Betreuung über das, was ihnen in dieser Eigenschaft bekannt geworden ist,
4. Medieninhaber (Herausgeber), Medienmitarbeiter und Arbeitnehmer eines Medienunternehmens oder Mediendienstes über Fragen, welche die Person des Verfassers, Einsenders oder Gewährsmannes von Beiträgen und Unterlagen betreffen oder die sich auf Mitteilungen beziehen, die ihnen im Hinblick auf ihre Tätigkeit gemacht wurden

Allerdings besteht nach § 144 Abs 3 StPO insoweit kein Umgehungsverbot, *als die betreffende Person selbst der Tat dringend verdächtig ist.* In diesem Fall muss die Anordnung und Durchführung der Ermittlungsmaßnahme jedoch durch Ermächtigung des Rechtsschutzbeauftragten (§ 147 Abs 2 StPO) genehmigt werden.

Konsequenzen für eine Diskussion über Ausnahmen im TKG:
Würde man nun im TKG Ausnahmen zur Datenübermittlung bezüglich der genannten Gruppe normieren, entstünde die Situation, dass es letztlich dennoch in der Verantwortung der Gerichte bleibt, die Ermittlungsmaßnahme mit einer Art „Beharrungsbeschluss“ anzuordnen, wenn nämlich ein dringender Tatverdacht bezüglich der „privilegierten“ Person selbst besteht. Ausnahmen im TKG wiederum würden erfordern, dass zunächst über eine staatliche Behörde (z.B.: die RTR) eine zentrale „Whitelist“ nach einem zu definierenden Verfahren erstellt und diese Liste schließlich von allen Anbietern vor jeder Auskunft abgeglichen werden müsste. Sowohl die „Whitelist“ als

auch der (automatisierte) Abgleich durch die Provider sind ohne Zweifel mit einem enormen Aufwand und vielen Unklarheiten verbunden (wer kommt auf die Liste, mit welchen Anschlüssen, wer trägt die Verantwortung für Richtigkeit, Vollständigkeit aber auch Geheimhaltung der Liste,...?). Einschlägige Erfahrungen mit der In-Effektivität eines solchen „White-List" Verfahrens wurden abgesehen davon in der jüngeren Vergangenheit bereits mit der sogenannten „Robinson-Liste" zur Verhinderung unerwünschter Werbung gesammelt. Dabei wäre trotz des hohen Aufwands der entsprechende Schutz nicht effektiv sichergestellt, weil das Gericht in eigener Verantwortung die Auskunft letztlich durchsetzen kann[207].

Aus diesen Gründen sollte die berechtigte Forderung nach einem besonderen Schutz von Berufsgeheimnisträgern primär jene adressieren, die dafür die Verantwortung tragen, also die Gerichte (über die StPO) und die Sicherheitsbehörden (über das SPG und das PStSG). Hierzu ist jedoch wegen bestehender Unklarheiten notwendig, die Regeln im Detail anzupassen, insbesondere:

1. durch die ausdrückliche Klarstellung, dass die Nichtigkeitsanordnung für die Umgehung der geistlichen Amtsverschwiegenheit in § 144 Abs 1 StPO sich auch auf die sonstigen Geheimnisträger gemäß § 144 Abs 2 StPO und sämtliche Ermittlungsmaßnahmen nach dem 8. Hauptstück der StPO bezieht
2. durch die ausdrückliche Klarstellung, dass die in § 144 StPO angeordnete Nichtigkeit des Verfahrens im Umgehungsfall absolut wirkt, Betroffene also nicht im Rechtsmittel argumentieren müssen, inwiefern der Verfahrensfehler überhaupt negative Auswirkungen auf das Verfahren hatte
3. durch die Klarstellung, dass die Voraussetzungen und der Rechtsschutz gemäß §§ 134 ff StPO auch für Auskünfte über IP-Adressen[208] anwendbar sind
4. durch Anpassungen, welche die schon derzeit in § 138 StPO normierten nachträglichen Informationspflichten auch in der Vollzugspraxis sicherstellen
5. durch die Schließung bestehender Lücken bei den Befugnissen des Rechtsschutzbeauftragten (RSB) der Justiz, insbesondere zur Kontrolle einer nachträglichen Genehmigung durch die Staatsanwaltschaft bei Gefahr in Verzug, zur Kontrolle der laufenden Durchführung einer Maßnahme, zur mangelnden Befugnis, eine Maßnahme bei nachträglichem Wegfall der Voraussetzungen zu beenden (derzeit nur Beschwerderecht) sowie zu den durch die StPO-Reform weggefallenen umfassenden Informations- und Einsichtsrechten des RSB
6. durch die Bereitstellung ausreichender (personeller) Mittel der RSB sowohl des Innen- als auch des Justizministeriums
7. durch materielle Einschränkungen der Auskunftsansprüche nach § 53 Abs 3a SPG

[207] Zumindest unter der Voraussetzung eines dringenden Tatverdachts bzgl. der Betroffenen selbst auch können soll; vgl. dazu z.B.: EGMR vom 16.10.2007, Wieser und Bicos Beteiligungen GmbH vs. Österreich, Newsletter Menschenrechte 2007, 258.
[208] § 76a StPO - Auskunft über Stammdaten (dazu zählt eine statische IP-Adresse).

8. durch die Schaffung einer der Genehmigungspflicht durch den RSB gemäß § 144 Abs 3 StPO nachgebildeten Bestimmung im SPG
9. durch die Schaffung von (nachträglichen) Informationspflichten gegenüber Personen, die von einer Verkehrsdatenauskunft nach dem SPG betroffen sind

Diese rechtspolitischen Anregungen sind der Zuständigkeit entsprechend an das BMJ bzw. BM.I zu adressieren.

Stärkung der Kompetenzen der Rechtsschutzbeauftragten:

Der „kommissarische" Rechtsschutz durch die Rechtsschutzbeauftragten nach StPO, PStSG und SPG könnte dadurch gestärkt werden, dass den RSB von allen Providern (etwa monatlich) eine Liste mit jenen Auskunftsfällen übermittelt werden, bei denen Geheimnisträger betroffen sind – –sofern die Anordnung nicht bereits die Ermächtigung durch den RSB beinhaltet. Dies würde vor allem jene Fälle betreffen, in denen die besondere Schutzwürdigkeit eines von der Ermittlungsmaßnahme Betroffenen dem Gericht entweder vorher gar nicht bekannt war oder die Einholung der Ermächtigung durch den RSB rechtswidrig unterblieben ist. Die Anbieter könnten hierzu in der eigenen Kundendatenbank einen Vermerk anlegen, dass es sich beim jeweiligen Anschluss um einen besonders geschützten handelt. Allerdings nicht mit der Konsequenz, dass die Auskunft verweigert wird, sondern nur, um den RSB diese Fälle gesondert zur Kenntnis zu bringen und gewissermaßen deren Aufmerksamkeit auf die besonders prüfenswerten Fälle zu lenken. Wegen dieser eher „weichen" Auswirkung würde auch ausreichen, wenn der Kunde seine „Geheimnisträger-Eigenschaft" nur bescheinigt – ohne besonders hohen Verfahrensaufwand. Der automatisierte Abgleich der Auskunftsfälle mit einer „Geheimnisträger-Liste" des jeweiligen Anbieters stellt zwar auch einen Aufwand in der Implementierung und Abwicklung dar, der jedoch gegenüber einem echten „White-List" Verfahren deutlich geringer ausfallen würde.

Schließlich könnten die oben unter 9. geforderten Informationspflichten von einer durch den Anbieter nach Ablauf einer bestimmten Zeitspanne flankiert werden, die etwa greifen könnte, wenn der Anbieter weder über die Gerichtsanhängigkeit noch über eine bereits durch die Behörden erfolgte Information in Kenntnis gesetzt wird.

5.1.6.2 Lockspitzelverbot und Verlockung zu einem Geständnis (§ 5 Abs 3 StPO)

Mit dem Strafprozessrechtsänderungsgesetz 2016 (BGBl- I 26/2016) wurde § 5 Abs 3 StPO geändert und an die Rechtsprechung des EGMR zu Art 6 EMRK angepasst. Gemäß § 5 Abs 3 StPO (idgF) ist es unzulässig, Personen zur Begehung von strafbaren Handlungen in einer dem Grundsatz des fairen Verfahrens gem. Art 6 EMRK widerstreitenden Weise zu verleiten, oder durch heimlich bestellte Personen zu einem Geständnis zu verlocken. Der

ständigen Rechtsprechung des EGMR zufolge liegt eine polizeiliche Provokation (Agent-Provocateur-Problem) dann vor, wenn sich die beteiligten Polizeibeamten nicht auf eine weitgehend passive Strafermittlung beschränken, sondern die betroffene Person derart beeinflussen, dass diese zur Begehung einer Straftat verleitet wird, die sie andernfalls nicht begangen hätte, und zwar mit dem Zweck (durch Beweiserbringung und Einleitung eines Strafverfahrens) die Feststellung einer Straftat zu ermöglichen.

Durch die Neufassung des § 133 Abs 5 StPO wird klargestellt, dass eine solche Verleitung zu einer Straftat ein prozessuales Strafverfolgungshindernis darstellt. In seiner bisherigen Rechtsprechung hat der österreichische OGH die Ansicht vertreten, dass aus der Verletzung des Lockspitzelverbotes weder ein materieller Strafausschließungsgrund noch ein prozessuales Verfolgungshindernis abgeleitet werden kann. Allerdings müsste ein Strafgericht einen in unzulässiger, dem Staat zuzurechnender Tatprovokation gelegenen Konventionsverstoß ausdrücklich im Urteil feststellen sowie durch eine ausdrückliche und messbare Strafmilderung ausgleichen. Eine bloße Strafmilderung ist angesichts der Rechtsprechung des EGMR aber keine angemessene Wiedergutmachung für eine Verletzung des Grundsatzes des fairen Verfahrens durch eine unzulässige Tatprovokation. Der EGMR verlangt nämlich, dass alle als Ergebnis polizeilicher Provokation gewonnenen Beweismittel ausgeschlossen werden oder ein Verfahren mit vergleichbaren Konsequenzen greift (EGMR Furcht v. Deutschland)[209]. Im Urteil 12 Os 5/16a vom 14. Juli 2016 nimmt der Gerichtshof auf die EGMR-Rechtsprechung und den neuen § 133 Abs 5 StPO Bezug. Im zugrundeliegenden Verfahren fand diese Vorschrift jedoch mangels Geltung zum Zeitpunkt des Urteils erster Instanz keine Anwendung (keine Rückwirkung von Strafgesetzen unter prozessualen Gesichtspunkten[210]). Der Entscheidung des EGMR zu Furcht v. Deutschland konnte darüber hinaus nicht Rechnung getragen werden, da in der verfahrensgegenständlichen Hauptverhandlung kein Antrag gestellt wurde, die Verwendung von Beweismitteln, die mit Hilfe der verdeckten polizeilichen Ermittlung erlangt wurden, zu unterlassen. Nichtsdestotrotz ist davon auszugehen, dass die Rechtsprechung des Obersten Gerichtshofs zur unzulässigen Tatprovokation in künftigen Strafverfahren mit der EMRK in Einklang stehen wird.

Auch wenn ein ausdrückliches Beweisverwertungsverbot nicht Einzug in die StPO gehalten hat, dürfte die Normierung des prozessualen Strafverfolgungshindernisses ein Verfahren mit vergleichbaren Konsequenzen im Sinne der Anforderungen des EGMR darstellen. Nach dem Wortlaut des Gesetzes gilt dieses allerdings nur für die Tatprovokation, nicht aber für die Verlockung zu einem Geständnis. Der Verdächtige darf gem. § 5 Abs 3 StPO weder von polizeilichen Organen, noch von diesen heimlich bestellten oder beauftragten Personen ausgehorcht werden, ohne dass man ihn in diese Situation einweiht. Der EGMR hat in seiner bislang einzigen Entscheidung zu dieser Problematik

[209] EGMR 23.10.2014, 54648/09, Furcht v. Deutschland.
[210] OGH 13 Os 127/15y.

nicht nur eine Verletzung von Art 8 EMRK, sondern auch von Art 6 EMRK festgestellt[211], da durch das Vorgehen der Strafverfolgungsbehörden das Recht des Antragstellers (dem durch einen Informanten der Polizei in der Untersuchungshaft ein Geständnis herausgelockt wurde) zu schweigen bzw. das Verbot des Zwangs zur Selbstbezichtigung verletzt wurde.

Das Verbot des Einsatzes von Lockspitzeln und der Hinwirkung auf ein Geständnis durch verdeckte Verhöre besteht seit der Strafprozessordnung 1853, stand jedoch der Legalisierung von Scheingeschäften oder von verdeckten Ermittlungen nicht entgegen. Die beiden letztgenannten Maßnahmen haben erst ab Mitte der 1970er Jahre Einzug in den österreichischen Rechtsbestand gehalten. In den ersten hundert Jahren ihres Bestehens kannte die StPO keine einzige Methode der Beweisbeschaffung, die heimlich oder getarnt abgewickelt bzw. eingesetzt wurde. Vernehmungen und die herkömmlichen Zwangsmittel (z.B. Beschlagnahme oder Hausdurchsuchung) werden dem Betroffenen gegenüber offen vorgenommen. Sie sind sogar auf kommunikatives Auftreten der Behörde ausgelegt und Ausdruck eines Konzepts der Information des Betroffenen. Es war fast selbstverständlich, dass die ermittelnden Behörden ihre Arbeit offen erledigen müssen. Die transparente Durchführung der aufgezählten Methoden lässt sich auch nicht mit einem Mangel an Abhörtechnologie zur Zeit der Gesetzesentstehung begründen, denn eine heimliche Hausdurchsuchung oder eine heimliche Überwachung der Briefpost wäre auch damals leicht möglich gewesen, ebenso wie der Einsatz von Spitzeln (vgl. dazu auch das Spitzelwesen im Metternichschen Überwachungsstaat).

Mit dem Lockspitzel- und dem Aushorchverbot, in denen die ursprüngliche Ablehnung getarnter Strafverfolgung am stärksten zum Ausdruck kommt, hat sowohl der historische als auch der moderne Gesetzgeber eine fundamentale Entscheidung getroffen – Täuschungen dieser Art sind nämlich schlicht unfair. Der EGMR hat beispielsweise sowohl die Tatprovokation, als auch das Aushorchen durch einen Spitzel in der Untersuchungshaft als unheilbare Fairnessverletzung qualifiziert[212]. Grundsätzlich soll niemand (und schon gar nicht der Staat) davon profitieren, dass er einem anderen eine Falle stellt. In einem Strafverfahren ist jede Person als Subjekt anzuerkennen und der Schuldige soll in einem kommunikativen Prozess überführt werden[213]. Diese Anerkennung definiert auch das Verhältnis zwischen Staat und Individuum. Bei rechtsstaatlicher Ausübung von hoheitlicher Macht ist der Staat nicht Herrscher und die Betroffenen sind nicht Untertanen, sondern der Staat ist Letzteren Rechenschaft bezüglich seines Handelns schuldig. Daneben gehört neben der Bindung an die Gesetze, vereinfacht gesagt auch, dass er eigens verantwortete Versprechen hält. Der Bürger, der den der Staat als Träger von Rechtspositionen ernst nehmen muss, kann daher von den

[211] EGMR 05.11.2002, 48539/99, Allan v. UK.
[212] EGMR Teixera de Castro v. Portugal, 25829/94, Ramanauskas v. Litauen, 74420/01 und Allan v. UK, 48539/99.
[213] *Zerbes*, Spitzeln, Spähen, Spionieren (2010), 70.

Behörden verlangen, dass sie sich an ihre Zusicherungen halten und das in sie gesetzte Vertrauen nicht missbrauchen. Aus dieser Maxime könnten sich Schranken heimlicher Verfolgungstätigkeit ergeben, nämlich, dass behördlich inszenierte Täuschungen dem Grundsatz der Transparenz widersprechen. Das muss konsequenterweise nicht nur für den gesamten Strafprozess, sondern auch für die präventiven Ermittlungsmaßnahmen nach dem PStSG[214] und dem SPG[215] gelten.

5.1.6.3 Vertrauenspersonenevidenz und „V-Leute" in der Kriminalitätsbekämpfung

Die Legalisierung (staatlicher bezahlter) „V-Leute" für die Ermittlung oder Prävention von Straftaten birgt zunächst ein systematisches Risiko: Bezahlte Spitzel kommen zumeist aus dem kriminellen Umfeld, gegen das ermittelt wird. Wesentlich ist daher die Begründung, weshalb die Ermittler eine konkrete „Vertrauensperson" in einem konkreten Zusammenhang für zuverlässig halten. Formale Begründungspflichten im Rahmen begleitender Sicherungsmechanismen sieht das PStSG dazu allerdings nicht vor. Hierzu wäre nicht nur eine richterliche Kontrolle (der Ermittlungsmaßnahme) wünschenswert, notwendig wäre überdies ein Katalog von Zulässigkeitsvoraussetzungen und Begründungspflichten für den Einsatz von V-Leuten.

Ein Problem besteht außerdem im potentiellen Spannungsverhältnis zum „Recht auf ein faires Verfahren" gemäß Art. 6 EMRK. Um dies zu verstehen, muss man die Ermittlungen der „Staatsschutzorgane" im Erfolgsfall zu Ende denken: Im besten Fall mündet die Amtshandlung in eine abgewehrte Sicherheitsbedrohung und in ein Strafverfahren gegen konkrete Beschuldigte. Wenn das Ermittlungsverfahren wesentlich durch „V-Leute" und verdeckte Ermittler getragen ist, wird in der Praxis die Wahrscheinlichkeit erhöht, dass der Vorwurf einer (nach§ 5 Abs. 3 StPO ausdrücklich verbotenen) Tatprovokation erhoben wird. Eine Tatprovokation und die Verwertung darauf basierender Beweise im Strafprozess stellt grundsätzlich eine Verletzung des Rechts auf ein faires Verfahren dar.[216]

Ein System staatlich bezahlter V-Leute birgt hier zunächst auch das Problem der Zurechnung zum Staat: Wenn ein V-Mann bezahlt wird, muss sich der Staat dessen Handlungen (z.B.: eine Tatprovokation) auch zurechnen lassen. Wenn nun der Beschuldigte in einem Strafverfahren substantiiert eine Tatprovokation behauptet, trifft den Staatsanwalt die Beweislast, diese Behauptung zu widerlegen. Das Gericht hat dann eingehend zu untersuchen, ob die polizeilichen Organe innerhalb der gesetzlichen Grenzen agiert haben. In einem derartigen Fall wird man die „Vertrauensperson"

[214] Polizeiliches Staatsschutzgesetz, in Kraft seit 01.07.2016.
[215] Sicherheitspolizeigesetz.
[216] Vgl. EGMR 9.6.1998, Teixeira de Castro gg. Portugal, EuGRZ 1999, 660; ÖJZ 1999, 434 (eingehend dazu *Fuchs*, Verdeckte Ermittler – anonyme Zeugen, ÖJZ 2001, 495 [496 ff.] sowie EGMR 5.2.2008, Ramanauskas gg. Litauen, NL 2008, 21 und 4.11.2010, Bannikova gg. Russland.

regelmäßig als Zeugen benötigen. Allerdings gibt es keine Rechtsgrundlage, auf der ein Gericht das BM.I zwingen kann, die Identität eines V-Manns oder eines verdeckten Ermittlers offen zu legen. Wenn also die Identität nicht preisgegeben wird, kann der Zeuge nicht unmittelbar vom Gericht und vor allem nicht vom Angeklagten befragt werden. Mit Blick auf den Unmittelbarkeitsgrundsatz (§ 13 StPO) und das in Art 6 Abs 3 lit d EMRK verbriefte Recht, Fragen an die Belastungszeugen zu stellen oder stellen zu lassen, qualifiziert der OGH z.B.: schon die Vernehmung einer Verhörsperson über die ihr gegenüber getätigten Angaben eines namentlich nicht bekannt gegebenen verdeckten Ermittlers als (Nichtigkeit begründende) Umgehung des Verlesungsverbotes (§ 252 Abs 1 StPO). Eine auf die Amtsverschwiegenheit zum Schutz eines (anonymen) Zeugen gestützte Verlesung iSd § 252 Abs 1 Z 1 StPO ist nur in sehr engen Grenzen denkbar zulässig, etwa bei besonders schwerwiegenden Straftaten, wenn die in Rede stehende Zeugenaussage unverzichtbar ist und die Gefährdungslage durch andere geeignete Maßnahmen (§§ 162, 229, 250 Abs 1 StPO) nicht beseitigt werden kann.[217]

Aus den dargelegten Gründen sollte schon beim Einsatz von verdeckten Ermittlern und V-Leuten bedacht werden, inwieweit diese Methoden lediglich einen Zwischenschritt zur Gewinnung anderer Beweismittel (Hausdurchsuchung, Überwachung der Telekommunikation etc.) darstellen sollen, widrigenfalls deren (ausschließliche) Verwertung im Wege anonymer Zeugenaussagen im Hauptverfahren iSd dargestellten Judikatur Probleme bereiten kann. Sind weitere Erkenntnisquellen nicht in Sicht, sollte dies im Einzelfall – zumal bei nicht eindeutig gewahrter Verhältnismäßigkeit – im Zweifel unzulässig sein. Der Gesetzesentwurf und die Erläuterungen des PStSG zeigen nicht einmal ansatzweise, dass die beschriebenen Herausforderungen bedacht und reflektiert wurden. Hierzu sollte dringend eine sachliche öffentliche Diskussion geführt werden.

5.2 Gesetzliche Grundlagen und Zusammenhänge

Bedienungsanleitung zur Übersicht

Bei den folgenden Grafiken handelt es sich um eine systematische Aufstellung und Übersicht der Straftatbestände, die nach dem Polizeilichen Staatsschutzgesetz (in Kraft seit 01.07.2016, BGBl. I 5/2016) als verfassungsgefährdender Angriff zu werten sind. Gleichzeitig wird eine Darstellung der jeweils möglichen bzw. zulässigen Ermittlungsbefugnisse der Strafverfolgungs- und Sicherheitsbehörden auch nach anderen Rechtsgrundlagen geboten.

Einerseits werden die Delikte mit ihrem jeweiligen Strafrahmen genannt, andererseits werden die verschiedenen Ermittlungsbefugnisse bzw. –maßnahmen gegenüberstellt und die formellen Voraussetzungen der Zulässigkeit farblich kodiert. Die Grenzen

[217] 13 Os 153/03; 15 Os 63/04; *Kirchbacher*, WK-StPO § 252 Rz 66 f; EGMR 23.4.1997, Van Mechelen und andere gg. die Niederlande, NL 1997, 91; kritisch: *Schwaighofer*, Der Unmittelbarkeitsgrundsatz beim Zeugenbeweis und seine Ausnahmen, ÖJZ 1996, 124 (134) mit Berufung auf (die mittlerweile überholte Entscheidung) 14 Os 40/95.

zwischen Prävention bzw. Präemption (Vorbeugung, Gefahrenabwehr) und Repression (Strafverfolgung) verschwimmen zusehends, als diverse Delikte bereits Handlungen weit im Vorfeld der eigentlichen strafbaren Handlung zum Straftatbestand erheben und zwecks Vorbeugung die Ermittlungsbefugnisse der StPO auslösen. Die farbliche Kodierung soll hervorheben, ob bei einem Delikt eine Rechtsgrundlage für eine bestimmte Ermittlungsmaßnahme besteht und falls ja, was die formellen Voraussetzungen der Zulässigkeit sind und wie der Rechtsschutz ausgestaltet ist.

Auffällig ist, dass sich die Sicherheitsbehörden bei gewissen Ermittlungsmaßnahmen quasi aussuchen können, ob sie nach dem PStSG bzw. im Dienste der Strafjustiz nach der StPO (Vorbeugung) tätig werden, und so die strengeren formellen Zulässigkeitsvoraussetzungen der StPO umgehen. Hervorzuheben ist in diesem Zusammenhang, dass es eine echte richterliche Kontrolle (Genehmigung einer Ermittlungsmaßnahme durch den Haft- und Rechtsschutzrichter bei den (Straf-)Landesgerichten) nur gibt, wenn die Sicherheitsbehörden auf Grundlage der StPO und damit im Dienste der Justiz tätig werden. Im Regime des PStSG bzw. des SPG sind bloß Genehmigungs- bzw. Kontrollpflichten des Rechtsschutzbeauftragten (bzw. Rechtsschutzsenates) normiert, die nach Ansicht der Verfasser dieses Handbuchs Rechtsschutzdefizite aufweisen und deshalb nicht verfassungskonform sind. Das Rechtsschutzsystem des PStSG (und der zugehörigen Normen des SPG) ist Gegenstand eines laufenden Verfahrens aufgrund einer „Drittelbeschwerde“ gem. Art 140 Abs 1 Z 2 B-VG[218], die von einem Drittel der Abgeordneten zum Nationalrat beim österreichischen Verfassungsgerichtshof im Juni 2016 eingebracht wurde. Mit einer Entscheidung ist nicht vor März 2017 zu rechnen.

Die nachfolgende tabellarische Darstellung zeigt bereits bei Beschränkung auf die unmittelbaren Rechtsgrundlagen der Sicherheitsbehörden (StPO, PStSG, SPG, StGB) die hohe Komplexität der Zusammenhänge. Zum besseren Überblick folgt hier noch die Liste aller Normen mit direkten Eingriffsbefugnissen durch Sicherheitsbehörden in das Datenschutzgrundrecht:

- Polizeiliches Staatsschutzgesetz (PStSG)
- Strafprozessordnung (StPO)
- Strafgesetzbuch (StGB)
- Finanzstrafgesetz (FinStrG)
- Sicherheitspolizeigesetz (SPG)
- Militärbefugnisgesetz (MBG)
- Telekommunikationsgesetz (TKG)
- E-Commerce Gesetz (ECG)
- Mediengesetz (MedG)

[218] Der Text der „Drittelbeschwerde“ ist hier nachzulesen: https://akvorrat.at/sites/default/files/drittelantragvfgh_pstsg_einbringung_28.6.2016.pdf

- Wirtschaftstreuhändergesetz (WTG)
- Bankwesengesetz (BWG)
- Polizeikooperationsgesetz (PolKoG)
- Internationale Abkommen

Mapping der Delikte 1/4

- unzulässig... keine Rechtsgrundlage oder ausdrücklich verboten
- nur Staatsanwaltschaft + Gericht... Polizei wird im Dienste der Strafjustiz (Kriminalpolizei) aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft tätig
- nur Staatsanwaltschaft... Polizei wird im Dienste der Strafjustiz (Kriminalpolizei) aufgrund einer Anordnung der Staatsanwaltschaft tätig
- "Staatsschutzorgane" (BVT, LVT) werden auf Basis der (gegenüber der Polizei ausschließlichen) Befugnisse nach dem PStSG tätig
- Polizei und BVT werden auf Basis der Befugnisse nach dem SPG tätig

Norm*	Bezeichnung	Strafdrohung	„Große Rasterfahndung" Datenabgleich § 141 Abs 3 StPO (Abgleich auch mit privaten/gewerblichen Datenbanken)	„Kleine Rasterfahndung" Datenabgleich § 141 Abs 2 StPO (Abgleich nur Daten von Sicherheits- und Strafverfolgungsbehörden)	IP-Adressen (Zugangsdaten) § 76a Abs 2 StPO	IP-Adressen (Zugangsdaten) § 11 Abs 1 Z 7 PStSG	IP-Adressen (Zugangsdaten) § 53 Abs 3a SPG	Datenabgleich öffentliche Quellen/ Internet (OSINT) § 10 Abs 5 PStSG (?Abgrenzung § 141 (2) StPO?)	Datenabgleich öffentliche Quellen/ Internet (OSINT) § 53 Abs 4 SPG (?Abgrenzung § 141 (2) StPO?)
75	Mord	bis lebenslang							
75	Mord iZ Terror	bis lebenslang							
84	schwere Körperverletzung	bis 3 Jahre	X	X					
84	schwere Körperverletzung iZ Terror	bis 4,5 Jahre							
85	Körperverletzung mit schweren Dauerfolgen	bis 5 Jahre	X						
85	Körperverletzung mit schweren Dauerfolgen iZ Terror	bis 7,5 ahre							
86	Körperverletzung mit tödlichem Ausgang	bis 10 Jahre	X						
86	Körperverletzung mit tödlichem Ausgang iZ Terror	bis 15 Jahre							
87	Absichtliche schwere Körperverletzung	bis 5 Jahre	X						
87	Absichtliche schwere Körperverletzung iZ Terror	bis 7,5 Jahre							
102	Erpresserische Entführung	bis 20 Jahre							
102	Erpresserische Entführung iZ Terror	bis 20 Jahre							
106	schwere Nötigung	bis 5 Jahre	X						
106	schwere Nötigung iZ Terror	bis 7,5							
107 Abs 2	qualifizierte gefährliche Drohung	bis 3 Jahre	X	X					
107 Abs 2	qualifizierte gefährliche Drohung iZ Terror	bis 4,5							
118a	Widerrechtlicher Zugriff auf ein Computersystem	bis 6 Monate	X	X					
118a (3)	Widerrechtlicher Zugriff auf ein Computersystem iZ OK (Kriminelle Vereinigung)	bis 3 Jahre		X					
119	Verletzung des Telekommunikationsgeheimnisses	bis 6 Monate	X	X					
119a	Missbräuchliches Abfangen von Daten	bis 6 Monate	X	X					
124	Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands	bis 3 Jahre	X	X					
126	schwere Sachbeschädigung	bis 2 Jahre	X	X					
126	schwere Sachbeschädigung iZ Terror	bis 3,5							
126a	Datenbeschädigung	bis 6 Monate	X	X					
126a (2)	Datenbeschädigung iZ OK (Kriminelle Vereinigung)	bis 5 Jahre							
126 iVm 278c	Datenbeschädigung iZ OK/Terror	bis 9 Monate		X					
126b	Störung der Funktionsfähigkeit eines Computersystems	bis 6 Monate	X	X					
126b (2)	Störung der Funktionsfähigkeit eines Computersystems iZ OK	bis 5 Jahre							
126c	Missbrauch von Computerprogrammen oder Zugangsdaten	bis 6 Monate	X	X					
165 Abs. 3	Geldwäscherei iZ OK/Terror	bis 3 Jahre		X					
169	Brandstifung	bis 10 Jahre	X						
169	Brandstifung iZ Terror	bis 15 Jahre							
171	Vorsätzliche Gefährdung durch Kernenergie oder ionisierende Strahlen	bis 10 Jahre	X						
171	Vorsätzliche Gefährdung durch Kernenergie oder ionisierende Strahlen iZ Terror	bis 15 Jahre							
173	Vorsätzliche Gefährdung durch Sprengmittel	bis 10 Jahre	X						
173	Vorsätzliche Gefährdung durch Sprengmittel iZ Terror	bis 15 Jahre							
175	Vorbereitung eines Verbrechens durch Kernenergie	bis 5 Jahre	X						
175	Vorbereitung eines Verbrechens durch Kernenergie ionisierende Strahlen oder Sprengmittel iZ Terror	bis 7,5 Jahre							
176	Vorsätzliche Gemeingefährdung	bis 10 Jahre	X						
176	Vorsätzliche Gemeingefährdung iZ Terror	bis 15 Jahre							

* (ohne Angabe bezieht sich diese auf das StGB)

Mapping der Delikte 2/4

- unzulässig... keine Rechtsgrundlage oder ausdrücklich verboten
- nur Staatsanwaltschaft + Gericht... Polizei wird im Dienste der Strafjustiz (Kriminalpolizei) aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft tätig
- nur Staatsanwaltschaft... Polizei wird im Dienste der Strafjustiz (Kriminalpolizei) aufgrund einer Anordnung der Staatsanwaltschaft tätig
- "Staatsschutzorgane" (BVT, LVT) werden auf Basis der (gegenüber der Polizei ausschließlichen) Befugnisse nach dem PStSG tätig
- Polizei und BVT werden auf Basis der Befugnisse nach dem SPG tätig

Norm*	Bezeichnung	Strafdrohung	„Große Rasterfahndung" Datenabgleich § 141 Abs 3 StPO (Abgleich auch mit privaten/gewerblichen Datenbanken)	„Kleine Rasterfahndung" Datenabgleich § 141 Abs 2 StPO (Abgleich nur Daten von Sicherheits- und Strafverfolgungsbehörden)	IP-Adressen (Zugangsdaten) § 76a Abs 2 StPO	IP-Adressen (Zugangsdaten) § 11 Abs 1 Z 7 PStSG	IP-Adressen (Zugangsdaten) § 53 Abs 3a SPG	Datenabgleich öffentliche Quellen/ Internet (OSINT) § 10 Abs 5 PStSG (Abgrenzung § 141 (2) StPO?)	Datenabgleich öffentliche Quellen/ Internet (OSINT) § 53 Abs 4 SPG (Abgrenzung § 141 (2) StPO?)
177a	Herstellung und Verbreitung von Massenvernichtungswaffen	bis 10 Jahre							
177a	Herstellung und Verbreitung von Massenvernichtungswaffen iZ Terror	bis 15 Jahre							
177b	Unerlaubter Umgang mit Kernmaterial, radioaktiven Stoffen oder Strahleneinrichtungen	bis 3 Jahre							
177b	Unerlaubter Umgang mit Kernmaterial, radioaktiven Stoffen oder Strahleneinrichtungen iZ Terror	bis 4,5 Jahre							
178	Vorsätzliche Gefährdung von Menschen durch übertragbare Krankheiten	bis 3 Jahre							
178	Vorsätzliche Gefährdung von Menschen durch übertragbare Krankheiten iZ Terror	bis 4,5 Jahre							
180	vorsätzliche Beeinträchtigung der Umwelt	bis 3 Jahre							
180	vorsätzliche Beeinträchtigung der Umwelt iZ Terror	bis 4,5 Jahre							
185	Luftpiraterie	bis 10 Jahre							
185	Luftpiraterie iZ Terror	bis 15 Jahre							
186	vorsätzliche Gefährdung der Sicherheit der Luftfahrt	bis 10 Jahre							
186	vorsätzliche Gefährdung der Sicherheit der Luftfahrt iZ Terror	bis 15 Jahre							
242	Hochverrat	bis 20 Jahre							
244	Vorbereitung eines Hochverrats	bis 10 Jahre							
246	Staatsfeindliche Verbindungen	bis 5 Jahre							
249	Gewalt und gefährliche Drohung gegen den Bundespräsidenten	bis 10 Jahre							
250	Nötigung eines verfassungsmäßigen Vertretungskörpers, einer Regierung, des Verfassungsgerichtshofs, des Verwaltungsgerichtshofs oder des Obersten Gerichtshofs	bis 10 Jahre							
251	Nötigung von Mitgliedern eines verfassungsmäßigen Vertretungskörpers, einer Regierung, des Verfassungsgerichtshofs, des Verwaltungsgerichtshofs oder des Obersten Gerichtshofs oder des Präsidenten des Rechnungshofs oder des Leiters eines Landesrechnungshofs	bis 5 Jahre							
252	Verrat von Staatsgeheimnissen	bis 10 Jahre							
253	Preisgabe von Staatsgeheimnissen	bis 3 Jahre							
254	Ausspähung von Staatsgeheimnissen	bis 5 Jahre							
256	Geheimer Nachrichtendienst zum Nachteil Österreichs	bis 3 Jahre							
257	Begünstigung feindlicher Streitkräfte	bis 10 Jahre							
258	Landesverräterische Fälschung und Vernichtung von Beweisen	bis 5 Jahre							
274 (2) erster Fall	Landfriedensbruch	bis 3 Jahre							
278 b	Terroristische Vereinigung	bis 15 Jahre							
278c	siehe Delikte mit der Bezeichnung „iZ Terror"								
278 d	Terrorismusfinanzierung	bis 10 Jahre							
278 e	Ausbildung für terroristische Zwecke	bis 10 Jahre							
278 f	Anleitung zur Begehung einer terroristischen Straftat	bis 2 Jahre							
279	Bewaffnete Verbindungen	bis 3 Jahre							
280	Ansammeln von Kampfmitteln	bis 3 Jahre							
282a	Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten	bis 2 Jahre							
282a	Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten iZ Terror	bis 3,5 Jahre							
283 Abs 3	Verhetzung	bis 5 Jahre							
316	Hochverräterische Angriffe gegen einen fremden Staat	bis 5 Jahre							
319	Militärischer Nachrichtendienst für einen fremden Staat	bis 2 Jahre							
320	Verbotene Unterstützung von Parteien bewaffneter Konflikte	bis 5 Jahre							
Verbotsgesetz	Zusammengefasst	Grunddelikte bis 20 Jahre							
7 KMG >	nur bei rw + vorsätzlicher Verwirklichung	bis 3 Jahre							
7 KMG	iZ Terror > nur bei rw + vorsätzlicher Verwirklichung	bis 4,5 Jahre							
79-82 AußWG	Zusammengefasst; > nur bei rw + vorsätzlicher VerwirklichungGrunddelikte	bis 5 Jahre							
50 WaffenG	Gerichtlich strafbare Handlungen	bis 1 Jahr							
50 WaffenG	Gerichtlich strafbare Handlungen iZ Terror	bis 1,5 Jahre							
11 SanktG	Gerichtliche Strafbestimmung	bis 2 Jahre							

* (ohne Angabe bezieht sich diese auf das StGB)

Mapping der Delikte 3/4

- unzulässig... keine Rechtsgrundlage oder ausdrücklich verboten
- nur Staatsanwaltschaft + Gericht... Polizei wird im Dienste der Strafjustiz (Kriminalpolizei) aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft tätig
- nur Staatsanwaltschaft... Polizei wird im Dienste der Strafjustiz (Kriminalpolizei) aufgrund einer Anordnung der Staatsanwaltschaft tätig
- "Staatsschutzorgane" (BVT, LVT) werden auf Basis der (gegenüber der Polizei ausschließlichen) Befugnisse nach dem PStSG tätig
- Polizei und BVT werden auf Basis der Befugnisse nach dem SPG tätig

Norm*	Bezeichnung	Strafdrohung	Optische & akustische Überwachung avon Personen § 136 Abs 1 Z 3 StPO	Optische & akustische Überwachung von Personen § 11 (1) (3) PStSG (ohne Ermittler)	Optische & akustische Überwachung von Personen § 54 (4) SPG (ohne Ermittler)	Verkehrsdatenauskunft § 135 Abs 2 Z 3 StPO	historische Standortdatenauskunft § 135 Abs 2 Z 3 StPO	gegenwärtige Standortdatenauskunft § 135 Abs 2 Z 3 StPO (Stille SMS - strittig)	Inhaltsüberwachung § 135 Abs 3 Z 3 StPO	Auskünfte „Dienst der Informationsgesellschaft" (§ 18 ECG)	Gefährder	Gefährdeter	gegenwärtige Standortauskunft § 53 Abs 3b SPG (IMSI-Catcher)
75	Mord	bis lebenslang											
75	Mord iZ Terror	bis lebenslang											
84	schwere Körperverletzung	bis 3 Jahre											
84	schwere Körperverletzung iZ Terror	bis 4,5 Jahre											
85	Körperverletzung mit schweren Dauerfolgen	bis 5 Jahre											
85	Körperverletzung mit schweren Dauerfolgen iZ Terror	bis 7,5 ahre											
86	Körperverletzung mit tödlichem Ausgang	bis 10 Jahre											
86	Körperverletzung mit tödlichem Ausgang iZ Terror	bis 15 Jahre											
87	Absichtliche schwere Körperverletzung	bis 5 Jahre											
87	Absichtliche schwere Körperverletzung iZ Terror	bis 7,5 Jahre											
102	Erpresserische Entführung	bis 20 Jahre											
102	Erpresserische Entführung iZ Terror	bis 20 Jahre											
106	schwere Nötigung	bis 5 Jahre											
106	schwere Nötigung iZ Terror	bis 7,5											
107 Abs 2	qualifizierte gefährliche Drohung	bis 3 Jahre											
107 Abs 2	qualifizierte gefährliche Drohung iZ Terror	bis 4,5											
118a	Widerrechtlicher Zugriff auf ein Computersystem	bis 6 Monate											
118a (3)	Widerrechtlicher Zugriff auf ein Computersystem iZ OK (Kriminelle Vereinigung)	bis 3 Jahre											
119	Verletzung des Telekommunikationsgeheimnisses	bis 6 Monate											
119a	Missbräuchliches Abfangen von Daten	bis 6 Monate											
124	Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands	bis 3 Jahre											
126	schwere Sachbeschädigung	bis 2 Jahre											
126	schwere Sachbeschädigung iZ Terror	bis 3,5											
126a	Datenbeschädigung	bis 6 Monate											
126a (2)	Datenbeschädigung iZ OK (Kriminelle Vereinigung)	bis 5 Jahre											
126 iVm 278c	Datenbeschädigung iZ OK/Terror	bis 9 Monate											
126b	Störung der Funktionsfähigkeit eines Computersystems	bis 6 Monate											
126b (2)	Störung der Funktionsfähigkeit eines Computersystems iZ OK	bis 5 Jahre											
126c	Missbrauch von Computerprogrammen oder Zugangsdaten	bis 6 Monate											
165 Abs. 3	Geldwäscherei iZ OK/Terror	bis 3 Jahre											
169	Brandstifung	bis 10 Jahre											
169	Brandstifung iZ Terror	bis 15 Jahre											
171	Vorsätzliche Gefährdung durch Kernenergie oder ionisierende Strahlen	bis 10 Jahre											
171	Vorsätzliche Gefährdung durch Kernenergie oder ionisierende Strahlen iZ Terror	bis 15 Jahre											
173	Vorsätzliche Gefährdung durch Sprengmittel	bis 10 Jahre											
173	Vorsätzliche Gefährdung durch Sprengmittel iZ Terror	bis 15 Jahre											
175	Vorbereitung eines Verbrechens durch Kernenergie	bis 5 Jahre											
175	Vorbereitung eines Verbrechens durch Kernenergie ionisierende Strahlen oder Sprengmittel iZ Terror	bis 7,5 Jahre											
176	Vorsätzliche Gemeingefährdung	bis 10 Jahre											
176	Vorsätzliche Gemeingefährdung iZ Terror	bis 15 Jahre											

* (ohne Angabe bezieht sich diese auf das StGB)

Mapping der Delikte 4/4

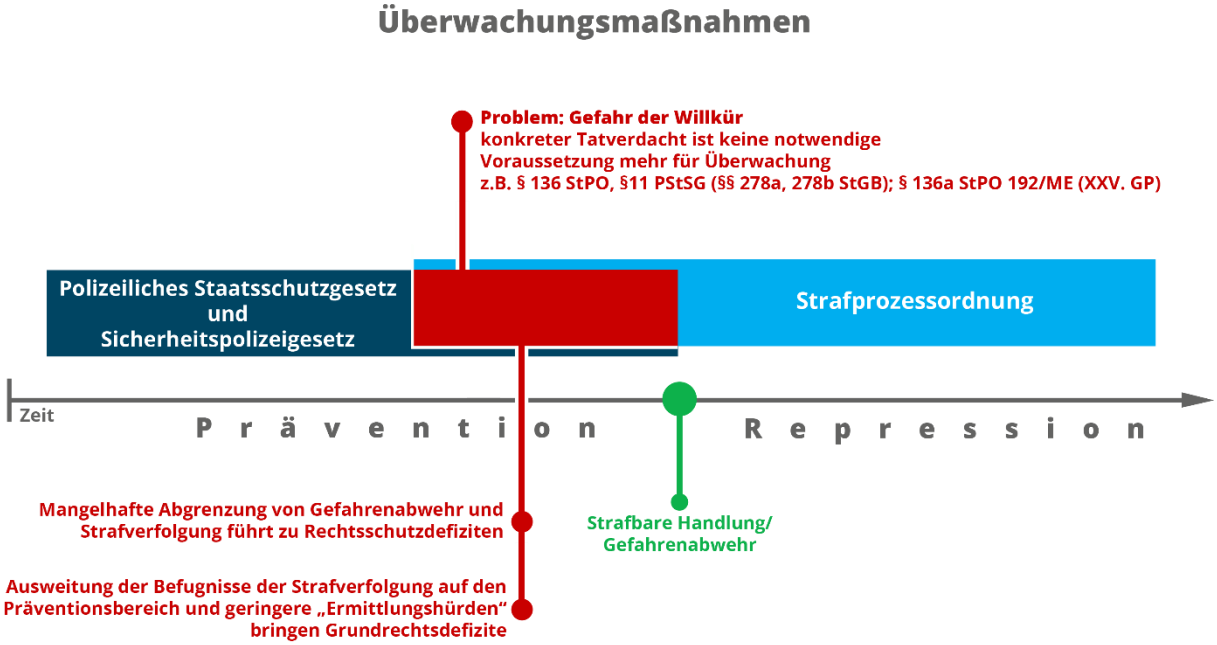
- unzulässig... keine Rechtsgrundlage oder ausdrücklich verboten
- nur Staatsanwaltschaft + Gericht... Polizei wird im Dienste der Strafjustiz (Kriminalpolizei) aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft tätig
- nur Staatsanwaltschaft... Polizei wird im Dienste der Strafjustiz (Kriminalpolizei) aufgrund einer Anordnung der Staatsanwaltschaft tätig
- "Staatsschutzorgane" (BVT, LVT) werden auf Basis der (gegenüber der Polizei ausschließlichen) Befugnisse nach dem PStSG tätig
- Polizei und BVT werden auf Basis der Befugnisse nach dem SPG tätig

Norm*	Bezeichnung	Strafdrohung	Optische & akustische Überwachung a von Personen § 136 Abs 1 Z 3 StPO	Optische & akustische Überwachung von Personen § 11 (1) (3) PStSG (ohne Ermittler)	Optische & akustische Überwachung von Personen § 54 (4) SPG (ohne Ermittler)	Verkehrsdatenauskunft § 135 Abs 2 Z 3 StPO	historische Standortdatenauskunft § 135 Abs 2 Z 3 StPO	gegenwärtige Standortdatenauskunft § 135 Abs 2 Z 3 StPO (Stille SMS - strittig)	Inhaltsüberwachung § 135 Abs 3 Z 3 StPO	Auskünfte „Dienst der Informationsgesellschaft" (§ 18 ECG)	gegenwärtige Standortauskunft § 53 Abs 3b SPG (IMSI-Catcher)	
										Gefährder	Gefährdeter	
177a	Herstellung und Verbreitung von Massenvernichtungswaffen	bis 10 Jahre	✗		✗							
177a	Herstellung und Verbreitung von Massenvernichtungswaffen iZ Terror	bis 15 Jahre			✗							
177b	Unerlaubter Umgang mit Kernmaterial, radioaktiven Stoffen oder Strahleneinrichtungen	bis 3 Jahre	✗		✗							
177b	Unerlaubter Umgang mit Kernmaterial, radioaktiven Stoffen oder Strahleneinrichtungen iZ Terror	bis 4,5 Jahre			✗							
178	Vorsätzliche Gefährdung von Menschen durch übertragbare Krankheiten	bis 3 Jahre	✗		✗							
178	Vorsätzliche Gefährdung von Menschen durch übertragbare Krankheiten iZ Terror	bis 4,5 Jahre			✗							
180	vorsätzliche Beeinträchtigung der Umwelt	bis 3 Jahre	✗		✗							
180	vorsätzliche Beeinträchtigung der Umwelt iZ Terror	bis 4,5 Jahre			✗							
185	Luftpiraterie	bis 10 Jahre	✗		✗							
185	Luftpiraterie iZ Terror	bis 15 Jahre			✗							
186	vorsätzliche Gefährdung der Sicherheit der Luftfahrt	bis 10 Jahre	✗		✗							
186	vorsätzliche Gefährdung der Sicherheit der Luftfahrt iZ Terror	bis 15 Jahre			✗							
242	Hochverrat	bis 20 Jahre			✗							
244	Vorbereitung eines Hochverrats	bis 10 Jahre	✗		✗							
246	Staatsfeindliche Verbindungen	bis 5 Jahre	✗		✗							
249	Gewalt und gefährliche Drohung gegen den Bundespräsidenten	bis 10 Jahre	✗		✗							
250	Nötigung eines verfassungsmäßigen Vertretungskörpers, einer Regierung, des Verfassungsgerichtshofs, des Verwaltungsgerichtshofs oder des Obersten Gerichtshofs	bis 10 Jahre	✗		✗							
251	Nötigung von Mitgliedern eines verfassungsmäßigen Vertretungskörpers, einer Regierung, des Verfassungsgerichtshofs, des Verwaltungsgerichtshofs oder des Obersten Gerichtshofs oder des Präsidenten des Rechnungshofs oder des Leiters eines Landesrechnungshofs	bis 5 Jahre	✗		✗							
252	Verrat von Staatsgeheimnissen	bis 10 Jahre	✗		✗							
253	Preisgabe von Staatsgeheimnissen	bis 3 Jahre	✗		✗							
254	Ausspähung von Staatsgeheimnissen	bis 5 Jahre	✗		✗							
256	Geheimer Nachrichtendienst zum Nachteil Österreichs	bis 3 Jahre	✗		✗							
257	Begünstigung feindlicher Streitkräfte	bis 10 Jahre	✗		✗							
258	Landesverräterische Fälschung und Vernichtung von Beweisen	bis 5 Jahre	✗		✗							
274 (2) erster Fall	Landfriedensbruch	bis 3 Jahre	✗		✗							
278 b	Terroristische Vereinigung	bis 15 Jahre			✗							
278c	siehe Delikte mit der Bezeichnung „iZ Terror"											
278 d	Terrorismusfinanzierung	bis 10 Jahre	✗		✗							
278 e	Ausbildung für terroristische Zwecke	bis 10 Jahre	✗		✗							
278 f	Anleitung zur Begehung einer terroristischen Straftat	bis 2 Jahre	✗		✗							
279	Bewaffnete Verbindungen	bis 3 Jahre	✗		✗							
280	Ansammeln von Kampfmitteln	bis 3 Jahre	✗		✗							
282a	Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten	bis 2 Jahre	✗		✗							
282a	Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten iZ Terror	bis 3,5 Jahre			✗							
283 Abs 3	Verhetzung	bis 5 Jahre	✗		✗							
316	Hochverräterische Angriffe gegen einen fremden Staat	bis 5 Jahre	✗		✗							
319	Militärischer Nachrichtendienst für einen fremden Staat	bis 2 Jahre	✗		✗							
320	Verbotene Unterstützung von Parteien bewaffneter Konflikte	bis 5 Jahre	✗		✗							
Verbotsgesetz	Zusammengefasst	Grunddelikte bis 20 Jahre			✗							
7 KMG >	nur bei rw + vorsätzlicher Verwirklichung	bis 3 Jahre	✗		✗							
7 KMG	iZ Terror > nur bei rw + vorsätzlicher Verwirklichung	bis 4,5 Jahre			✗							
79-82 AußWG	Zusammengefasst; > nur bei rw + vorsätzlicher VerwirklichungGrunddelikte	bis 5 Jahre	✗		✗							
50 WaffenG	Gerichtlich strafbare Handlungen	bis 1 Jahr	✗		✗	✗	✗	✗	✗			
50 WaffenG	Gerichtlich strafbare Handlungen iZ Terror	bis 1,5 Jahre			✗							
11 SanktG	Gerichtliche Strafbestimmung	bis 2 Jahre	✗		✗							

* (ohne Angabe bezieht sich diese auf das StGB)

5.2.1 Unterscheidung Prävention und Aufklärung von Straftaten

Die relativ große Zahl verschiedener Rechtsgrundlagen, die im Zusammenhang mit Terror- bzw. Kriminalitätsbekämpfung für Ermittlungs- und Überwachungsmaßnahmen relevant ist, bewirken eine sehr hohe rechtliche Komplexität. Innerhalb dessen ist im Hinblick auf die grundrechtlichen Auswirkungen jedoch die Abgrenzung zwischen präventiver Gefahrenerforschung und der repressiven Strafverfolgung ein besonderes Problem. Lange Zeit war in der österreichischen Rechtsordnung erkennbar, dass die Befugnisse im Rahmen der Strafverfolgung – mit obligatorischer richterlicher Kontrolle und sonstigen Schutzmechanismen – deutlich weiter gingen als jene der Polizei im präventiven Bereich. Vor allem in den letzten 15 Jahren ist eine stetige Entwicklung feststellbar, bei der die Strafbarkeit immer weiter in den Bereich der Vorbereitungshandlungen gelegt wurde, während gleichzeitig die polizeilichen Befugnisse zur präventiven Gefahrenerforschung und Gefahrenabwehr abseits einer gerichtlichen Kontrolle massiv gestärkt wurden.



5.2.2 Abgrenzung zwischen StPO und SPG

Vom Begriff der Sicherheitsbehörden zu unterscheiden sind die operativen Einsatzkräfte der Polizei, also die Organe der Sicherheitsbehörden (§ 5 SPG), welchen in der Praxis die Besorgung des Exekutivdienstes und insbesondere die Wahrnehmung der Aufgabe der „Sicherheitspolizei“[219] obliegt. Unter Strafverfolgungsbehörden sind die Staatsanwaltschaft sowie die Strafgerichte zu verstehen. Die Polizei erfüllt hier gewissermaßen eine hybride Rolle: Organisatorisch gibt es in Österreich eine Bundespolizei, deren oberste Behörde der Bundesminister für Inneres ist[220] und deren Organisation, Aufgaben und Befugnisse sich aus dem Sicherheitspolizeigesetz ergeben. Dieselbe Polizei kann funktionell aber auch im Dienste der Strafrechtspflege und damit als Kriminalpolizei (§ 18 StPO) agieren. Die Organe des öffentlichen Sicherheitsdienstes (§ 5 Abs. 2 SPG) versehen gemäß § 18 Abs. 2 StPO den kriminalpolizeilichen Exekutivdienst, der in der Aufklärung und Verfolgung von Straftaten nach den Bestimmungen der Strafprozessordnung (StPO) besteht. Mit anderen Worten lässt sich die Unterscheidung zwischen Sicherheitspolizei und Kriminalpolizei nicht aufgrund organisatorischer Zuordnungen, sondern allein aufgrund der jeweils konkret zu erfüllenden Aufgaben treffen. Daran ändert auch nichts, dass mit dem Bundeskriminalamt und den Landeskriminalämtern spezialisierte Organisationseinheiten eingerichtet sind, die primär auf die Erfüllung kriminalpolizeilicher Aufgaben ausgerichtet sind –– im Rahmen der Erfüllung sicherheitspolizeilicher Aufgaben sind auch diese durch das SPG determiniert. Aus dieser Konstellation ergibt sich die in der Praxis manchmal nicht einfach zu bewältigende Herausforderung der Abgrenzung, wann nach den Regeln des SPG oder der StPO gehandelt werden soll. Diese Unterscheidung hat im Hinblick auf die Befugnisse und den Rechtsschutz wesentliche Konsequenzen und wird daher nun etwas näher betrachtet.

Die Faustregel zur Abgrenzung lautet: Die Verhinderung von (noch nicht begangenen) Straftaten richtet sich nach dem SPG, die Aufklärung und Verfolgung von Straftaten richtet sich nach der StPO. Allerdings lässt sich diese Abgrenzung in der Praxis oftmals nur schwer oder gar nicht treffen. Wenn beispielsweise ein Angriff auf ein geschütztes Rechtsgut im Gange ist, werden zu einem Zeitpunkt vor dem vollständigen Abschluss der strafbaren Handlung alle Bedingungen für das Vorliegen eines bereits nach dem

[219] Vgl. die Legaldefinition der „Sicherheitspolizei“ gemäß § 3 SPG: „Die Sicherheitspolizei besteht aus der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, ausgenommen die örtliche Sicherheitspolizei (Art. 10 Abs. 1 Z 7 B-VG), und aus der ersten allgemeinen Hilfeleistungspflicht.“

[220] Daneben enthält die Aufzählung des § 5 SPG auch „Angehörige der Gemeindewachkörper, Angehörige des rechtskundigen Dienstes bei Sicherheitsbehörden, wenn diese Organe zur Ausübung unmittelbarer Befehls- und Zwangsgewalt ermächtigt sind, und sonstige Angehörige der Landespolizeidirektionen und des Bundesministeriums für Inneres, wenn diese Organe die Grundausbildung für den Exekutivdienst (Polizeigrundausbildung) absolviert haben und zur Ausübung unmittelbarer Befehls- und Zwangsgewalt ermächtigt sind.“

Strafgesetzbuch (StGB) strafbaren Versuchs (§ 15 StGB) erfüllt sein.[221] Zugleich liegt dann aber auch ein noch nicht abgeschlossener „gefährlicher Angriff" (§ 16 Abs. 2 SPG, dazu sogleich) vor, dessen Abwehr die Polizei nach den Regeln des SPG zu besorgen hat. Dieselben Abgrenzungsschwierigkeiten bestehen, wenn die – noch nicht (vollständig) verwirklichte – Bedrohung eines nach dem StGB geschützten Rechtsguts von einer „kriminellen Vereinigung" (§ 278 StGB), einer „kriminellen Organisation" (§ 278a StGB) oder einer „terroristischen Vereinigung" (§ 278b StGB) ausgeht. In dieser Konstellation liegt nämlich im Hinblick auf das bedrohte Rechtsgut ein nach dem SPG zu begegnender „gefährlicher Angriff" vor, während schon die Mitgliedschaft zur jeweiligen Organisation bzw. Vereinigung selbst eine (abgeschlossene) strafbare Handlung darstellt, die nach den Regeln der StPO aufzuklären bzw. zu verhindern ist. Gerade bei „Cyber-Attacken" auf kritische Infrastruktur ist es sogar wahrscheinlicher, dass diese Konstellation und nicht nur ein Angriff einzelner Straftäter vorliegt.

Praktisch hat die Unterscheidung, ob nach dem SPG oder der StPO vorzugehen ist, vor allem die wesentliche Konsequenz, ob für die Ausübung von Befehls- und Zwangsgewalt sowie von Ermittlungshandlungen, die (durchaus gerechtfertigte) Grundrechtseingriffe erfordern, eine Anordnung der Staatsanwaltschaft[222] einzuholen ist (§ 98 StPO) oder die Polizei eigenmächtig oder aufgrund einer Genehmigung durch den Rechtsschutzbeauftragten (RSB) beim BMI handeln darf. Bei akuten Bedrohungslagen ist dieses Problem praktisch zwar dadurch abgeschwächt, dass die Kriminalpolizei bei „Gefahr im Verzug" dringende Ermittlungshandlungen vorerst auch ohne Anordnung der Staatsanwaltschaft vornehmen darf (§ 99 Abs. 2 StPO). Allerdings hat die Polizei dann unverzüglich der Staatsanwaltschaft zu berichten (§ 100 Abs. 2 Z 2 StPO) und um nachträgliche Genehmigung der Handlung zu ersuchen. Sofern eine Maßnahme eine gerichtliche Bewilligung erfordert, ist die Ermittlungsmaßnahme gemäß § 99 Abs. 3 StPO auch bei Gefahr im Verzug ohne diese Bewilligung nur dann zulässig, wenn das Gesetz dies ausdrücklich vorsieht.[223] Dem gegenüber sind die eigenmächtigen Handlungsspielräume der Polizei nach dem SPG deutlich großzügiger. Zwar bestehen auch im Regime des SPG gewisse Beschränkungen in Bezug auf die Einschaltung des RSB des BM.I (§ 91a ff SPG). Anders als nach der StPO ist jedoch nach dem SPG nur in wenigen Fällen die vorhergehende Ermächtigung des RSB erforderlich[224]. Im Regelfall besteht nur eine nachträgliche Informationspflicht gegenüber dem RSB.

---

[221] § 15 Abs. 2 StGB: „Die Tat ist versucht, sobald der Täter seinen Entschluss, sie auszuführen oder einen anderen dazu zu bestimmen (§ 12), durch eine der Ausführung unmittelbar vorangehende Handlung betätigt."

[222] Je nach Art der Ermittlungs- bzw. Eingriffshandlung erfordert diese zuvor eine gerichtliche Bewilligung, beispielsweise bei „Auskünften über Daten einer Nachrichtenübermittlung" gemäß § 135 StPO.

[223] Ein Beispiel hierfür ist die „Durchsuchung von Orten und Gegenständen" nach § 120 StPO.

[224] Eine Ermächtigung des RSB ist nach § 91c Abs. 3 SPG etwa zur Aufgabenerfüllung der „erweiterten Gefahrenerforschung" (§ 21 Abs. 3 SPG) erforderlich.

Während die beschriebenen Abgrenzungsschwierigkeiten zunächst ein internes Problem der Polizei darstellen, treten deren Konsequenzen im Zusammenhang mit Rechtsschutzfragen auch nach außen. Nach § 106 Abs 1 StPO[225] steht ein „Einspruch wegen Rechtsverletzung" an das Gericht jeder Person zu, die behauptet, im Ermittlungsverfahren durch Kriminalpolizei[226] oder Staatsanwaltschaft in einem subjektiven Recht verletzt zu sein, weil ihr die Ausübung eines Rechts nach diesem Gesetz verweigert (Z 1) oder eine Ermittlungs- oder Zwangsmaßnahme unter Verletzung von Bestimmungen dieses Gesetzes angeordnet oder durchgeführt (Z 2) wurde. Dem gegenüber stehen im Anwendungsbereich des SPG „Beschwerden wegen Verletzung subjektiver Rechte" an die Landesverwaltungsgerichte jenen Menschen zur Verfügung, „die behaupten, durch die Ausübung unmittelbarer sicherheitsbehördlicher Befehls- und Zwangsgewalt in ihren Rechten verletzt worden zu sein" (§ 88 SPG). Damit wird die zunächst für die Polizei intern wesentliche Abgrenzung zwischen StPO und SPG auch „nach außen" relevant. Und es steigt der Druck auf die Polizei, bei der Annahme der jeweiligen Rechtsgrundlage des Einschreitens auch entsprechende Sorgfalt walten zu lassen.

5.2.3 Cybercrime und Gefahrenabwehr nach dem SPG

Im Bereich der Gefahrenabwehr ist die erste wesentliche Rechtsfrage, ob ein bestimmter Sachverhalt die Handlungs- und Eingriffsbefugnisse nach dem SPG auslöst. Im Zentrum steht hierbei die Qualifikation eines Sachverhalts als „gefährlicher Angriff" im Sinne des § 16 Abs. 2 und 3 SPG. Dieser Begriff ist akzessorisch zum materiellen Strafrecht definiert. Ein „gefährlicher Angriff" ist unter anderem[227] „die Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die vorsätzlich begangen und nicht bloß auf Begehren eines Beteiligten verfolgt wird,

[225] IdF BGBl I 2013/195.

[226] Durch Erkenntnis des VfGH vom 16. 12. 2010, G 259/09 ua, wurde die Wortfolge "oder Kriminalpolizei" als verfassungswidrig aufgehoben. Dies hatte eine (neuerliche) Teilung des Rechtsschutzes gegen polizeiliche Zwangsakte zur Konsequenz, was der Gesetzgeber ursprünglich im Rahmen des Strafprozessreformgesetzes 2008 (BGBl I 2004/19) gerade verhindern wollte, mangels verfassungsrechtlicher Absicherung vom VfGH als Verletzung der Gewaltenteilung (§ 94 B-VG) bewertet wurde. Der nunmehr neuerlich normierte gerichtliche Rechtsschutz gegen Akte der Kriminalpolizei wird als durch die Änderung des Art 94 Abs 2 B-VG durch die Verwaltungsgerichtsbarkeits-Novelle 2012 (BGBl I 2012/51) gedeckt erachtet. Demnach werden in einzelnen Angelegenheiten Ausnahmen vom Trennungsgrundsatz (Art 94 Abs 1 B-VG) ermöglicht, mithin anstelle der Erhebung einer Beschwerde beim Verwaltungsgericht ein Instanzenzug von der Verwaltungsbehörde zur ordentlichen Gerichtsbarkeit durch einfachgesetzliche Regelung vorgesehen werden kann. Der Anwendungsbereich des Art 94 Abs 2 B-VG idF BGBl I 2012/51 beschränkt sich dabei nicht nur auf Bescheide, sondern erfasst auch sonstiges Verhalten der Verwaltungsbehörde in Vollziehung der Gesetze. Ausführlich dazu Stephanie Öner/Valerie Walcher, Zum Einspruch nach § 106 StPO, ÖJZ 2014/150, 999 ff.

[227] Neben den materiellen Straftatbeständen des StGB zählt § 16 Abs. 2 SPG aus dem sog. „Nebenstrafrecht" auch das Verbotsgesetz, das Fremdenpolizeigesetz, das Suchtmittelgesetz, das Anti-Doping Gesetz sowie das Neue-Psychoaktive-Substanzen-Gesetz auf.

sofern es sich um einen Straftatbestand (Z1) nach dem Strafgesetzbuch (StGB) handelt. Eine praktisch wichtige Erweiterung dazu normiert § 16 Abs. 3 SPG: „Ein gefährlicher Angriff ist auch ein Verhalten, das darauf abzielt und geeignet ist, eine solche Bedrohung (Abs. 2) vorzubereiten, sofern dieses Verhalten in engem zeitlichen Zusammenhang mit der angestrebten Tatbestandsverwirklichung gesetzt wird." Gerade bei typischen „Cybercrime"-Attacken sind aus der Sicht ex ante häufig zunächst nur solche Vorbereitungshandlungen erkennbar, während die vollständige Verwirklichung eines Delikts nach dem StGB (dazu sogleich) oft erst sichtbar wird, wenn es bereits zu spät ist. In dieser Hinsicht ist die Ausdehnung des Begriffs des „gefährlichen Angriffs" auf zeitnahe Vorbereitungshandlungen enorm wichtig, damit die Polizei rechtzeitig auch mit entsprechenden Befugnissen reagieren kann.

Die Kernfrage ist also letztlich, ob die Verwirklichung eines materiellen Straftatbestands des StGB bevorsteht und dieser Straftatbestand nicht als sog. „Privatanklagedelikt" normiert ist, weil solche schon nach § 16 Abs. 2 SPG vom Begriff des „gefährlichen Angriffs" ausgenommen sind. Die in Frage kommenden Straftatbestände sind vor allem die „Cybercrime"-Tatbestände des StGB, konkret sind dies: § 118a („Widerrechtlicher Zugriff auf ein Computersystem"), § 119 („Verletzung des Telekommunikationsgeheimnisses"), § 119a („Missbräuchliches Abfangen von Daten"), § 126a („Datenbeschädigung"), § 126b („Störung der Funktionsfähigkeit eines Computersystems"), § 126c („Missbrauch von Computerprogrammen oder Zugangsdaten"), § 148a („Betrügerischer Datenverarbeitungsmissbrauch") sowie § 225a („Datenfälschung").

Darüber hinaus ist zu untersuchen, ob sich darunter auch „Privatanklagedelikte" befinden, welche die Anwendbarkeit der SPG-Befugnisse ausschließen würden. Hierzu fällt zunächst auf, dass die §§ 118a, 119 und 119a vorsehen, dass „der Täter (…) nur mit Ermächtigung des Verletzten zu verfolgen (ist)". Diese Normierung als sog. „Ermächtigungsdelikte" ist der Einschränkung des § 16 Abs. 2 SPG gegenüberzustellen, wonach ein „gefährlicher Angriff" nur vorliegt, wenn die strafbare Handlung „nicht bloß auf Begehren eines Beteiligten verfolgt wird". Der wesentliche Unterschied liegt darin, dass „Ermächtigungsdelikte" wie die soeben aufgezählten noch immer „Offizialdelikte" sind, deren Abwehr bzw. Verfolgung von den Strafverfolgungs- und Sicherheitsbehörden grundsätzlich von Amts wegen wahrzunehmen ist, hierzu jedoch die Ermächtigung des Verletzten einzuholen ist (§ 92 StPO). Wird diese Ermächtigung erteilt, stehen auch die Befugnisse eines strafprozessualen Ermittlungsverfahrens zur Verfügung. Dem gegenüber findet bei „Privatanklagedelikten", die nur auf Verlangen des Opfers zu verfolgen sind[228], ein Ermittlungsverfahren gemäß § 71 Abs. 1 StPO nicht statt. Aus dem

[228] ZB § 118 StGB: „Verletzung des Briefgeheimnisses und Unterdrückung von Briefen". Bei den Delikten „Datenbeschädigung", „Störung der Funktionsfähigkeit eines Computersystems" und „betrügerischem Datenverarbeitungsmißbrauch" könnte gemäß § 166 StGB dann ein Privatanklagedelikt vorliegen, wenn der Täter aus dem Familienkreis des Verletzten stammt.

Wortlaut der Einschränkung des § 16 Abs. 2 SPG ist unzweifelhaft, dass „Ermächtigungsdelikte“ nicht darunter fallen.

5.2.4 Fiktives Fallbeispiel „Tierschützerprozess 2.0“

Am besten lässt sich die Interdependenz der einzelnen Bestimmungen anhand eines konkreten, im Vergleich zu den realen Begebenheiten leicht modifizierten Sachverhalts erklären, welcher auf dem in Österreich berühmt gewordenen „Tierschützerprozess“[229] basiert. Dabei geht man von dem Sachverhalt aus, dass Person A in Geschäft X geht und dortige Pelzmäntel mit einer Spraydose besprüht (beschädigt). Ein paar Tage später findet das Sicherheitsorgan in einem Forum die Nachricht „Ich gehe in das Geschäft des X und werde die Pelzmäntel besprühen“ und eine E-Mail in welcher Person A die Tat einem Bekannten ankündigt. Aufgrund von Indizien erwägt das Sicherheitsorgan, dass es sich bei Person A um ein Mitglied einer terroristischen Organisation handle. Hier bestehen zwei denkbare Delikte. Zunächst die Sachbeschädigung gem. § 125 StGB mit einem Strafrahmen von bis zu 6 Monaten und die Mitgliedschaft in einer terroristischen Vereinigung gem. § 278b StGB mit einem Strafrahmen von bis zu 10 Jahren.

5.2.5 Erster Ermittlungsschritt – E-Commerce-Gesetz

Das Ziel von Ermittlungen ist es, den Urheber eines bereits bekannten Inhalts auszuforschen. Der erste Schritt besteht in der Ermittlung der IP-Adresse des Absenders bzw. Verfassers der Nachricht/des Forumseintrags. Die Grundlage dafür bildet § 18 Abs 2 ECG. Der Betreiber eines “Chat-Forums“ ist als Host-Provider iSd § 16 ECG anzusehen.[230] Dieser Host-Provider speichert fremde Daten (des Nutzers) und stellt die Infrastruktur für die Kommunikation zur Verfügung. Ein Access-Provider vermittelt, in Abgrenzung zum Host-Provider, nur den Zugang zum Internet. Ein “Chatroom“ oder “Chat-Forum“ ist als ein „Dienst der Informationsgesellschaft“[231] zu verstehen.[232] Somit kann festgestellt werden, dass ein Host-Provider eines Chat-Forums als Diensteanbieter iSd ECG anzusehen ist. Dieser ist nach § 18 Abs 2 ECG verpflichtet, erforderliche Informationen zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen herauszugeben.

5.2.6 Zweiter Ermittlungsschritt – E-Commerce-Gesetz

In einem zweiten Ermittlungsschritt wird der Subscriber einer Internet-Verbindung zu einer bestimmten IP-Adresse ermittelt. § 99 Abs 1 TKG regelt die Lösch– bzw. Anonymisierungspflicht der Anbieter. § 99 Abs 5 TKG regelt die Zulässigkeit der weiteren

[229] Hierbei handelt es sich um einen Strafprozess gegen mehrere Tierschutzaktivisten. Ermittelt und angeklagt wurde auf Grund des Verdachts, sie hätten eine kriminelle Organisation nach § 278a StGB gebildet und im Zuge derer weitere Straftaten ausgeführt. Siehe auch *Mackinger/Pack*, §278a: Gemeint sind wir alle! Der Prozess gegen die Tierbefreiungs-Bewegung und seine Hintergründe (2011).
[230] VwGH 27.05.2009, 2007/05/0280.
[231] § 1 Abs 1 Z 2 Notifikationsgesetz 1999.
[232] VwGH 27.05.2009, 2007/05/0280.

Verwendung. Schon bei den ersten beiden Ermittlungsschritten wird sichtbar, welche Bedeutung der Gesamtbetrachtung bei der Evaluation beigemessen werden muss. Durch die Verweise auf das SPG und die StPO in § 99 Abs 5 TKG wird die Wechselbeziehung und das Zusammenspiel der unterschiedlichen Bestimmungen deutlich. Grundlegend kann gesagt werden, dass Abs 1 eine Lösch– bzw. Anonymisierungspflicht für Verkehrsdaten vorsieht und dass eine weitere Verarbeitung nur auf Grundlage des Abs 5 iVm dem SPG oder der StPO möglich ist.

5.2.7 Verhältnis von SPG und StPO

Um auf das Verhältnis zwischen SPG und StPO näher eingehen zu können und damit die Problematik bei den Ermittlungsbefugnissen und Rechtsschutzmöglichkeiten zu beleuchten, muss man zunächst die beiden Rechtsgrundlagen voneinander abgrenzen. Während die StPO zur Aufklärung und Verfolgung begangener Straftaten dient, wird das SPG zur Gefahrenabwehr sowie zur allgemeinen Gefahrenerforschung als rechtliche Grundlage der Ermittlungstätigkeiten herangezogen. Bei einem noch nicht beendeten gefährlichen Angriff und einer gleichzeitigen bereits erfüllten Straftat kann es zu einem parallel bestehenden Anwendungsbereich von SPG und StPO kommen. Es können somit beide Gesetze als Grundlage für Ermittlungsmaßnahmen herangezogen werden. Deutlich sichtbar wird dies auch wenn Straftaten im Rahmen einer kriminellen oder terroristischen Organisation ausgeführt wurden und weitere Straftaten drohen. Für den Bereich der drohenden Straftat könnte in der Theorie mittels § 21 SPG das Problem entschärft werden, da den Sicherheitsbehörden die Abwehr allgemeiner Gefahren obliegt und davon ausgegangen werden kann, dass ein Vorrang der Gefahrenabwehr und des SPG besteht. Sobald jedoch *„ein bestimmter Mensch der strafbaren Handlung verdächtig ist, gelten ausschließlich die Bestimmungen der StPO“*[233]. Hierdurch wird deutlich, dass für die begangene Straftat die StPO zur Anwendung gelangt, während für die drohende Straftat das SPG Grundlage der Ermittlungstätigkeiten ist. Im Ergebnis kann dies zu einer parallelen Anwendung beider Rechtsgrundlagen führen. Diese Problematik wird in Kapitel 5.2.7.2 durch das “Pick & Choose Principle“ genauer erklärt.

5.2.7.1 Ermittlungsbefugnisse im Rahmen von Stammdaten[234]

Die Sicherheitsbehörden werden durch § 53 Abs 3a Z 1 SPG ermächtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs 3 Z 1 TKG 2003) und sonstigen Diensteanbietern (§ 3 Z 2 ECG) Auskünfte über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses zu verlangen, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist. Diensteanbieter hinsichtlich eines Chatrooms werden von § 3 Z 2 ECG erfasst.[235] Während bei der Ermittlung nach dem SPG keine erweiterten

[233] § 22 Abs 3 SPG. Siehe auch *Keplinger*, SPG und/oder StPO, Öffentliche Sicherheit 9-10/06, 146.
[234] § 92 Abs 3 Z 3 TKG.
[235] VwGH 24.04.2013, 2011/17/0293.

Voraussetzungen[236] benötigt werden, verlangt § 76a Abs 2 StPO die Anordnung der Staatsanwaltschaft[237], um die Herausgabe von Stammdaten der Nutzer, welche von den Diensteanbietern gespeichert werden, verlangen zu können. Gegen diese Anordnung kann im Stadium des Ermittlungsverfahrens gemäß § 106 Abs 1 Z 2 StPO Einspruch wegen Rechtsverletzung erhoben werden, worüber nach § 107 StPO ein sachlich und örtlich zuständiges Gericht zu entscheiden hat.

5.2.7.2 Ermittlungsbefugnisse zu Verkehrsdaten[238]

§ 53 Abs 3a Z 2 SPG berechtigt die Sicherheitsbehörden Auskünfte *„über die Internetprotokolladresse zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr einer entweder konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht, oder eines gefährlichen Angriffs[239] oder einer kriminellen Verbindung[240] benötigen, zu verlangen.“* Ebenfalls umfasst sind Daten darüber, "wann und mit welcher IP-Adresse mit welchem Nicknamen auf einem Chatserver kommunizierte wurde".[241] Im Rahmen der StPO werden Auskünfte über Daten einer Nachrichtenübermittlung wie folgt geregelt:

§ 135 Abs 2 StPO enthält mehrere Optionen, wie es zu einer gesetzmäßigen Auskunft kommen kann. Dabei werden im Rahmen dieses Handbuchs die zwei bedeutendsten Optionen für die hypothetische (aber nahe an die Realität angelehnte) Fallstudie näher erläutert. Bei Z 2 des § 135 Abs 2 StPO bedarf es der ausdrücklichen Zustimmung zur Auskunft durch den Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird. Diese wird für die Herausgabe der Daten für die Aufklärung einer vorsätzlich begangenen Straftat benötigt, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist. Es ist dies jedoch nur erlaubt, wenn zu erwarten ist, dass dadurch die Aufklärung gefördert wird. Handelt es sich um eine vorsätzlich begangene Straftat, die eine Freiheitsstrafe von mehr als einem Jahr nach sich ziehen kann, und kann dadurch die Aufklärung gefördert werden, so ist, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können, die Herausgabe der Daten ohne die ausdrückliche Zustimmung

[236] Zu denken wäre hier an eine staatsanwaltschaftliche Anordnung oder eine gerichtliche Bewilligung.
[237] § 102 StPO.
[238] § 92 Abs 3 Z 4 TKG.
[239] § 16 Abs 1 Z 1 SPG. Es kann festgehalten werden, dass das Besprühen von fremden Pelzmänteln in einem Geschäft den Tatbestand des § 125 StGB erfüllt und die Ankündigung dieser Tat einen gefährlichen Angriff gem. § 16 Abs 1 Z 1 darstellt. Das potentiell beeinträchtigte Rechtsgut stellen die Pelzmäntel dar.
[240] § 16 Abs 1 Z 2 SPG. Eine kriminelle Verbindung ist iSd SPG eine Personengruppe von drei oder mehr Menschen, die sich verbinden um fortgesetzt gerichtlich strafbare Handlungen zu begehen.
[241] VfGH 29.06.2012, B 1031/11-20.

des Inhabers der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, gem. § 135 Abs 2 Z 3 StPO möglich. Grundsätzlich ist festzuhalten, dass kein dringender Tatverdacht erforderlich ist, sondern ein einfacher Tatverdacht genügt[242] und dass jede Ermittlungsart verhältnismäßig iSd § 5 StPO sein muss. Gem. § 137 Abs 1 StPO sind die Ermittlungsmaßnahmen von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen.

Der Unterschied zwischen dem SPG und der StPO liegt bezogen auf Verkehrsdaten also darin, dass es bei einer Heranziehung des SPG als Ermittlungsgrundlage keiner staatsanwaltschaftlichen Anordnung und keiner gerichtlichen Bewilligung bedarf. Daraus entsteht folglich das rechtsstaatlich Risiko, dass es zu einem **"Pick & Choose Principle"** kommt. Je nachdem welche Gesetzesgrundlage man wählt, werden unterschiedliche Voraussetzungen an die Herausgabe von Verkehrsdaten geknüpft. Es gelten unterschiedliche Rechtsschutzniveaus und im Falle einer (angeblichen) anhaltenden Drohung einer Gefahr kann die für die Sicherheitsbehörde „bessere" gesetzliche Grundlage, gewählt werden. „Besser" ist eine Rechtsgrundlage in der Praxis dann, wenn sie weniger Aufwand erfordert, z.B.: weil eine Ermittlungsmaßnahme nicht durch eine schriftliche Genehmigung oder Anordnung einer anderen Stelle „behindert" wird.

5.2.8 Automationsunterstützter Datenabgleich gem. § 141 StPO

Zunächst muss einmal geklärt werden, worum es sich bei dem Datenabgleich iSd § 141 StPO handelt. Demnach ist „„Datenabgleich" der automationsunterstützte Vergleich von Daten (§ 4 Z 1 DSG 2000) einer Datenanwendung, die bestimmte, den mutmaßlichen Täter kennzeichnende oder ausschließende Merkmale enthalten, mit Daten einer anderen Datenanwendung, die solche Merkmale enthalten, um Personen festzustellen, die auf Grund dieser Merkmale als Verdächtige in Betracht kommen."[243] Dabei werden entweder positive- oder negative Abgrenzungskriterien in den Datenabgleich einbezogen. Je nachdem wird dieser dann positiver- oder negativer Datenabgleich genannt. Beispielsweise, ist der Auszuforschende „blond" und wird in den Datenabgleich „brünett" eingegeben, spricht man von einem negativen Abgrenzungsmerkmal. Es werden somit alle Brünetten negativ abgegrenzt. Der Datenabgleich ist nur zulässig, wenn die Aufklärung eines Verbrechens wesentlich erschwert wäre[244], oder wenn es sich um ein Verbrechen nach § 278a oder § 278b StGB handelt.[245]

[242] Vgl. die Unterscheidung z.B.: bei Eingriffen in die Persönliche Freiheit: Während allein die Festnahme mit Freiheitsentziehung für max. 96 Stunden gemäß § 171 StPO einen einfachen Tatverdacht genügen lässt, erfordert der zeitlich viel intensivere Grundrechtseingriff der Untersuchungshaft, nach § 173 StPO einen „dringenden Tatverdacht".
[243] § 141 Abs 1 StPO.
[244] § 141 Abs 2 StPO.
[245] § 141 Abs 3 StPO.

Somit kann festgehalten werden, dass in dem fingierten Fall ein Datenabgleich für das Delikt der Sachbeschädigung keine erlaubte Ermittlungsmethode darstellt, da der Strafrahmen im Falle des § 125 StGB bei maximal 6 Monaten liegt und § 141 StPO entweder ein Verbrechen iSd § 17 Abs 1 StGB[246] oder ein Verbrechen nach § 278a oder § 278b StGB verlangt. Die Problematik besteht darin, dass diese Ermittlungsmethode bei gegebenen Indizien[247] zur Ermittlung von anderen, geringfügigeren Delikten verwendet werden könnte. Sollte nämlich das Sicherheitsorgan annehmen, dass die Tat im Rahmen einer kriminellen Vereinigung oder einer terroristischen Organisation begangen wurde, dann können die Daten einer Person in einem Datenabgleich abgeglichen werden, obwohl es bei der Verwirklichung des Grunddelikts (§ 125 StGB) nicht rechtmäßig wäre.

5.2.9 Conclusio aus dem fiktiven Fallbeispiel

Wie das Fallbeispiel zeigt, bestehen zwischen SPG und StPO Abgrenzungsprobleme, welche bei näherer Betrachtung den Schluss zulassen, dass diese für Ermittlungsmaßnahmen gegen die Rechtsschutzinteressen der Betroffenen genützt werden könnten. Als erstes Beispiel sind die unterschiedlichen Rechtsschutzanforderungen in SPG, PStSG und StPO zu nennen. Hierbei kann es zu einem "Pick & Choose "-Vorgehen kommen, sodass die gesetzlichen Grundlagen für die Ermittlungsbefugnisse je nach Bedarf gewählt werden können. Des Weiteren dürfen bei einer Verbindung zu einer kriminellen- oder terroristischen Organisation Daten auch in den automatischen Datenabgleich einbezogen werden, die sonst bei einer Tatbestandsverwirklichung bei Delikten mit geringerer Strafdrohung wie z.B. einer Sachbeschädigung nach § 125 StGB nicht rechtmäßig verarbeitet werden dürften. Die hier dargestellten Zusammenhänge sind sozusagen nur die „Spitze des Eisbergs" und sollen lediglich illustrieren, dass die Problematik komplex ist und daher auch in der vollen Komplexität einer Evaluation zugänglich gemacht werden soll.

[246] § 17 Abs 1 StGB bezeichnet als Verbrechen Delikte mit einem Strafrahmen von mehr als 3 Jahren.

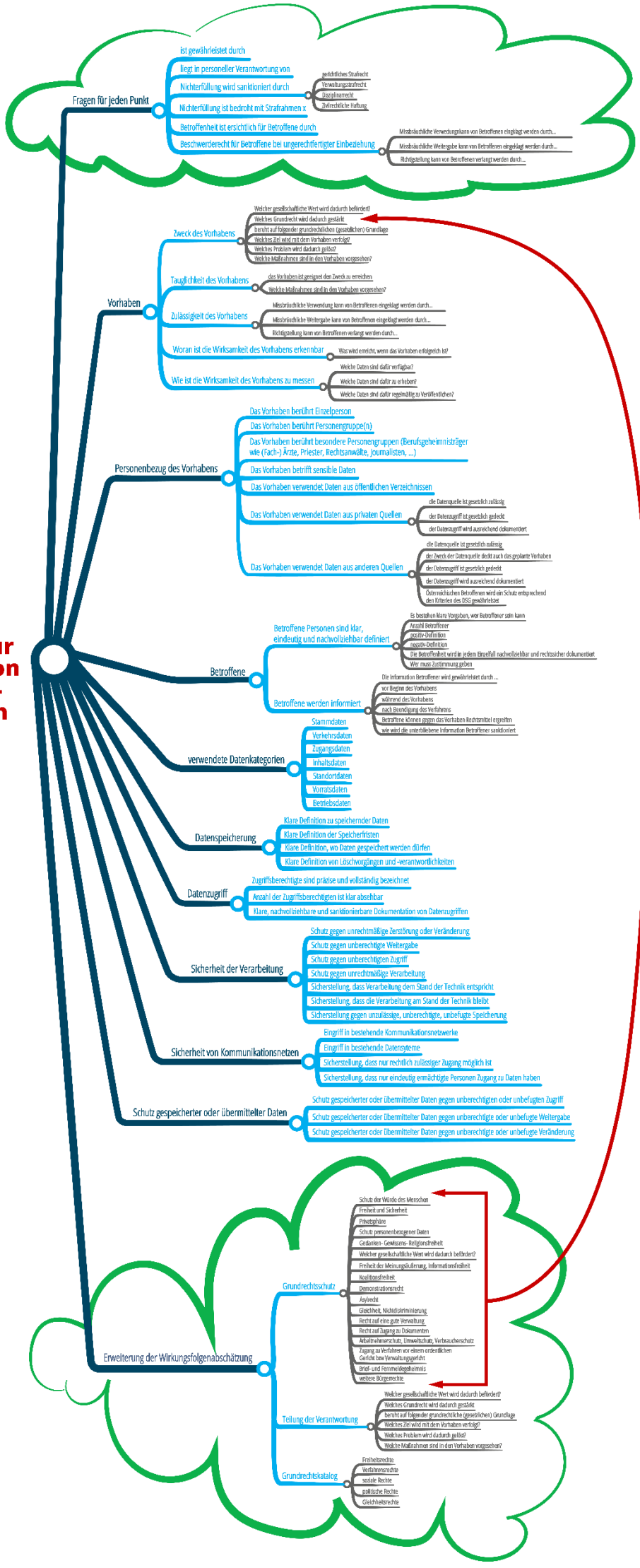
[247] Selbst wenn die Indizien im Nachhinein sich als nicht gegeben herausstellen, so dürfen die Ergebnisse verwertet werden, da sie keinem Verwertungsverbot unterliegen und es zu einer ex ante Prüfung kommt.

6 Handbuch zur Evaluation von Anti-Terrormaßnahmen

Folgend eine Gratik in der der Katalog des Handbuchs zur Evaluation der Anti-Terror-Gesetze (HEAT)) nach inhaltlichen Kriterien geordnet wird. Das Handbuch gibt mit dieser Struktur eine Hilfestellung, die notwendigen Punkte, die bei der Gestaltung von Gesetzesvorhaben zu beachten sind, in einer transparenten und handhabbaren Struktur zu bearbeiten.

Gleichzeitig erleichtert diese Sicht die Evaluation von bestehenden Regelungen, wenn zu den einzelnen Punkten eine qualifizierte Bewertung vorgenommen wird.
In einem weiteren Schritt werden die Punkte dieses Handbuchs zu gruppierten Checklisten verdichtet, um die Bearbeitung noch einfacher zu machen.

Handbuch zur Evaluation von Anti-Terror-Maßnahmen [HEAT]



6.1 Fragestellungen für jeden Punkt

- ist gewährleistet durch
- liegt in personeller Verantwortung von
- Nichterfüllung wird sanktioniert durch
- gerichtliches Strafrecht
- Verwaltungsstrafrecht
- Disziplinarrecht
- Zivilrechtliche Haftung
- Nichterfüllung ist bedroht mit Strafrahmen xy
- Betroffenheit ist ersichtlich für Betroffene durch …
- Beschwerderecht für Betroffene bei ungerechtfertigter Einbeziehung
  - Missbräuchliche Verwendung kann von Betroffenen rechtlich verfolgt werden durch …
  - Missbräuchliche Weitergabe kann von Betroffenen rechtlich verfolgt werden durch …
  - Richtigstellung kann von Betroffenen verlangt werden durch …

6.2 Vorhaben

6.2.1 Zweck des Vorhabens

Ein Vorhaben muss immer ziel- und zweckgerichtet sein.

6.2.1.1 Welcher gesellschaftliche Wert wird dadurch befördert?

Vorhaben und Maßnahmen dienen der Weiterentwicklung der Gesellschaft.
Jedes einzelne Vorhaben und jede einzelne Maßnahme muss daher einem gesamtgesellschaftlichen Wertekatalog zugeordnet werden können. So wie das menschliche Leben nicht konfliktfrei sein kann, sind auch gesellschaftliche Werte nicht frei von Widersprüchen und notwendigen Abwägungen.
Für die Mitgliedsländer der Europäischen Union bildet die Europäische Grundrechtscharta den Grundrechtskatalog.

Aus österreichischer Sicht werden beabsichtigte Weiterentwicklungen in den jährlichen "aktuellen Wirkungszielen" in überschaubare Einzelschritte heruntergebrochen. So lautet z.B. eines der "Aktuellen Wirkungsziele 2016": *"Wirkungsziel 2: Unterstützung bei der Sensibilisierung der Öffentlichkeit für die Bedeutung demokratischer Prozesse, der sozialen Ausgewogenheit und der Gleichstellung von Frauen und Männern. (Gleichstellungsziel)"*

6.2.1.2 Welches Grundrecht wird dadurch gestärkt?

siehe Kapitel "Grundrechtsschutz" in diesem Abschnitt des Handbuchs
und Grundrechtskatalog der EU http://fra.europa.eu/de/charterpedia

6.2.1.3 beruht auf folgender grundrechtlicher (gesetzlicher) Grundlage

Hier ist die grundrechtliche und gesetzliche Grundlage für das geplante Vorhaben anzuführen und zu erläutern. Im gesetzlichen Begutachtungsverfahren kann dieser Abschnitt in die Erläuterungen einfließen.

6.2.1.4 Welches Ziel wird mit dem Vorhaben verfolgt?

Einen sinnvollen und richtigen Ansatz bietet die Wirkungsfolgen-Grundsatz-Verordnung. Diese WFA-GV ist derzeit allerdings nicht ausreichend, da sie den Schwerpunkt auf die finanziellen Auswirkungen des Gesetzesvorhabens legt und Grundrechte nur in Ansätzen berücksichtigt (Umwelt, Gender-Gleichstellung, Ansätze zum Kinder- und Jugendschutz, nicht jedoch Kinderrechte ...).

Aus der Wirkungsfolgen-Grundsatz-Verordnung(WFA-GV): *"(4) Bei der Zielformulierung sind die Regelungs- beziehungsweise Vorhabensziele zu nennen. Es ist ein allfälliger Zusammenhang mit einem Wirkungsziel oder einer Maßnahme im Bundesvoranschlag darzustellen. Je Ziel sind ein bis fünf Indikatoren zur Messung der Zielerreichung anzuführen, die gleichzeitig auch als Grundlage für die interne Evaluierung heranzuziehen sind.*"
Die Wirkungsfolgenabschätzung der WFA-Grundverordnung beschreibt eine sinnvolle Vorgehensweise zu Problembeschreibung und Zielformulierung, ist jedoch in den beschriebenen Wirkungsdimensionen noch unvollständig. Insbesondere die beschriebenen gesellschafts- und grundrechtsrelevanten Wirkungsdimensionen bedürfen einer weitreichenden Ergänzung.

6.2.1.5 Welches Problem wird dadurch gelöst?

Aus der WFA-Grundsatz-Verordnung
„(3) Bei der Problemanalyse sind insbesondere der Grund des Tätigwerdens (Problem und dessen Ursachen), der Gestaltungsspielraum bei der Umsetzung von Unionsrecht, das Ausmaß des Problems, die von dem Problem Betroffenen sowie ein Szenario ohne Tätigwerden (Nullszenario) und allfällige Alternativen zu beschreiben.“.“

6.2.1.6 Welche Maßnahmen sind in dem Vorhaben vorgesehen?

Aus der WFA-GV:
„(5) Bei der Maßnahmenformulierung ist darauf Bedacht zu nehmen, dass Maßnahmen sachlich abgegrenzt ausgewiesen werden und die Wirkungszusammenhänge mit dem Regelungs- bzw. Vorhabensziel dargelegt werden. Je Maßnahme können ein bis fünf Indikatoren angeführt werden, die gleichzeitig auch als Grundlage für die interne Evaluierung heranzuziehen sind.“.“

6.2.2 Tauglichkeit des Vorhabens

6.2.2.1 das Vorhaben ist geeignet, den Zweck zu erreichen

Die Tauglichkeit des Vorhabens ist zu begründen und zu erläutern.

6.2.2.2 das Vorhaben ermöglicht mehr als den vorgesehenen Zweck zu erreichen

Vorhaben, die exakt das intendierte Ziel und nur dieses erreichbar machen, sind nicht der Regelfall. Technische und/oder organisatorische Rahmenbedingungen ermöglichen zumeist, dass auch über das Ziel hinausgehende Effekte möglich sind. Diese Effekte können sowohl positive wie auch negative Auswirkungen haben. Diese außerhalb des Zielbereichs liegenden Effekte sind zu beschreiben. Und zwar sowohl die

- positiven Nebeneffekte, als auch die
- negative Nebeneffekte

6.2.3 Zulässigkeit des Vorhabens

6.2.3.1 Das Vorhaben bewirkt keinen Grundrechtseingriff

Ein Grundrechtseingriff bei einem Vorhaben ist dann ein Hinderungsgrund,

- wenn er nicht gedeckt ist (keinem öffentlichen Interesse bzw. legitimen Ziel entspricht) oder
- nicht tauglich ist zur Erreichung des beabsichtigten Ziels oder
- nicht das gelindeste Mittel zur Erreichung des beabsichtigten Ziels darstellt oder
- unverhältnismäßig ist

6.2.3.2 Das Vorhaben bewirkt einen Grundrechtseingriff

Nach Art. 52 Abs. 1 der Charta muss jede Einschränkung der Ausübung der in der Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten; unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten Anderer tatsächlich entsprechen.

Ein Eingriff ist eine staatliche Maßnahme, die eine vom Schutzbereich erfasste Verhaltensweise verbietet oder erschwert
– Rsp: Intentionalität als Abgrenzungskriterium (fragwürdig)
– überzeugender: Wirkung einer Maßnahme im Schutzbereich
=> auch mittelbare, faktische Beeinträchtigungen greifen in das Grundrecht ein, wenn sie in ihrer Wirkung einem unmittelbaren

Eingriff gleichkommen.

Ein Eingriff ist unzulässig bzw. verletzt das Freiheitsrecht, wenn
(1) keine Eingriffsermächtigung vorliegt oder
(2) der Gesetzgeber eine solche Ermächtigung überschritten hat.

- Das Vorhaben berührt die Privatsphäre Betroffener

  Der Schutz des Grundrechts auf Achtung des Privatlebens verlangt nach ständiger Rechtsprechung des Europäischen Gerichtshofs jedenfalls, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken müssen (Urteil IPI, C-473/12, EU:C:2013:715, Rn. 39 und die dort angeführte Rechtsprechung).
- Das Vorhaben berührt das Recht auf freie Zusammenkunft
- Das Vorhaben berührt das Recht auf freie Meinungsäußerung
- Das Vorhaben berührt das Brief- und Fernmeldegeheimnis
- Das Vorhaben betrifft das Recht auf ein faires Verfahren
- … mittelbarer Grundrechtseingriff

  Mittelbare Auswirkung von Grundrechtseingriffen, Änderungen im individuellen oder gesellschaftlichen Verhalten, können aus einzelnen Eingriffen entstehen. Die Summe der Grundrechtseingriffe führt in der Gesamtschau dazu, dass sich das individuelle Verhalten jedenfalls verändert. Solcherart wird im Windschatten des verbrecherischen Terrorismus unser demokratisches System zunehmend beschädigt und damit indirekt das Ziel des Terrorismus unterstützt. Diese Kollateralschäden bedürfen einer Aufarbeitung und müssen einer Diskussion auf breiter gesellschaftlicher Basis zugänglich gemacht werden.

6.2.3.3 Ist der Grundrechtseingriff gerechtfertigt?

- Entspricht der Zweck des Vorhabens einem legitimen Ziel

  Entspricht der Zweck des Vorhabens einem legitimen Ziel im Rahmen des Eingriffsvorbehalts
- Stehen die identifizierten Nachteile in angemessenem Verhältnis zum

  erreichbaren Nutzen

  "Adäquanz" siehe VfGH-Rsp

6.2.4 Woran ist die Wirksamkeit des Vorhabens zu erkennen?

6.2.4.1 Was wird erreicht, wenn das Vorhaben erfolgreich ist?

erfordert eine präzise Beschreibung

z.B. in der WFA-GV:

(6) Bei der Auswahl der Indikatoren (Abs. 4 und 5) ist jedenfalls auf die Konsistenz mit den für die Angaben zur Wirkungsorientierung auf Untergliederungs- und Globalbudgetebene herangezogenen Indikatoren des für die Durchführung der wirkungsorientierten Folgenabschätzung zuständigen haushaltsleitenden Organs zu achten.

6.2.5 Wie ist die Wirksamkeit des Vorhabens zu messen?

"Messen" ist immer eine quantitative Methode.
Dazu sind Parameter zu identifizieren, die eine Veränderung von einem (unerwünschten) Ist-Zustand hin zu einem beabsichtigten Zustand als Folge der Umsetzung des Vorhabens erkennbar machen.

Ergänzend dazu sollen qualitative Beschreibungen des beabsichtigten Zielzustandes verfügbar gemacht werden, die die beabsichtigte Wirkung des Veränderungsprozesses erläutern.

6.2.5.1 Welche Daten sind dafür verfügbar?

6.2.5.2 Welche Daten sind dafür zu erheben?

Aus der WFA-GV:
„(6) Bei der Auswahl der Indikatoren (Abs. 4 und 5) ist jedenfalls auf die Konsistenz mit den für die Angaben zur Wirkungsorientierung auf Untergliederungs- und Globalbudgetebene herangezogenen Indikatoren des für die Durchführung der wirkungsorientierten Folgenabschätzung zuständigen haushaltsleitenden Organs zu achten.“.“

6.2.5.3 Welche Daten sind dafür regelmäßig zu veröffentlichen?

6.3 Personenbezug des Vorhabens

DSG § 4: Im Sinne der folgenden Bestimmungen dieses Bundesgesetzes bedeuten die Begriffe:
Z 1. „Daten“ („personenbezogene Daten“): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen“ sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;

Z 3. „Betroffener“: jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden;

6.3.1 Das Vorhaben berührt Einzelperson

6.3.2 Das Vorhaben berührt Personengruppe(n)

Hier ist besonders zu prüfen, ob durch Auswahlkriterien Gruppen Betroffener geschaffen werden, die nicht hinreichend begründet sind und damit das Diskriminierungsverbot verletzt wird.

6.3.3 Das Vorhaben berührt besondere Personengruppen (Berufsgeheimnisträger wie (Fach-) Ärzte, Priester, Rechtsanwälte, Journalisten, …)

Es muss sichergestellt sein, dass Personengruppen, die Berufsgeheimnisträger beinhalten, nur mit entsprechender Absicherung und angemessenen Safeguards betroffen sein können.

6.3.4 Das Vorhaben betrifft sensible Daten

DSG § 4: Z 2. „sensible Daten“ („besonders schutzwürdige Daten“): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;

6.3.5 Das Vorhaben verwendet Daten aus öffentlichen Verzeichnissen

DSG § 5: (1) Datenanwendungen sind dem öffentlichen Bereich im Sinne dieses Bundesgesetzes zuzurechnen, wenn sie für Zwecke eines Auftraggebers des öffentlichen Bereichs (Abs. 2) durchgeführt werden.
(2) Auftraggeber des öffentlichen Bereichs sind alle Auftraggeber,
1. die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder
2. soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.

6.3.6 Das Vorhaben verwendet Daten aus privaten Quellen

DSG § 5: (3) Die dem Abs. 2 nicht unterliegenden Auftraggeber gelten als Auftraggeber des privaten Bereichs im Sinne dieses Bundesgesetzes.

6.3.6.1 Die Datenquelle ist gesetzlich zulässig

6.3.6.2 Der Datenzugriff ist gesetzlich gedeckt

Die Rechte Betroffener sind gewährleistet und durchsetzbar:

- Auskunftsrecht
- Recht auf Richtigstellung oder Löschung

- Recht auf Widerruf

6.3.6.3 Der Datenzugriff wird ausreichend dokumentiert

6.3.7 Das Vorhaben verwendet Daten aus anderen Quellen

Dies betrifft besonders Daten und Datenanwendungen ausländischer Herkunft oder Daten aus Quellen, die nicht österreichischem oder EU-Recht unterliegen und deren Legitimität daher fraglich ist.

Diese Anwendungen gelten nach dem DSG zunächst als "Private Datenanwendungen", es ist jedoch explizit der Nachweis zu erbringen, dass Daten und Datenanwendungen den Zulässigkeits- und Verwendungsgrundsätzen des österreichischen Datenschutzgesetzes entsprechen und auch in Zukunft entsprechen werden sowie, dass die Rechte Betroffener gewahrt werden und durchgesetzt werden können.

6.3.7.1 Die Datenquelle ist gesetzlich zulässig

6.3.7.2 Der Zweck der Datenquelle deckt auch das geplante Vorhaben

6.3.7.3 Der Datenzugriff ist gesetzlich gedeckt

6.3.7.4 Der Datenzugriff wird ausreichend dokumentiert

6.3.7.5 Österreichischen Betroffenen wird ein Schutz entsprechend den Kriterien des DSG gewährleistet

6.4 Betroffene

6.4.1 Betroffene Personen sind klar, eindeutig und nachvollziehbar definiert

Hier sind klare und eindeutige Abgrenzungen zu ziehen. Das Fehlen solcher Eingrenzungen hat in mehreren Fällen zur Aufhebung von Gesetzen durch Höchstgerichte beigetragen.

6.4.1.1 Es bestehen klare Vorgaben, wer Betroffener sein kann

6.4.1.2 Anzahl Betroffener

6.4.1.3 positiv-Definition

"vom Vorhaben betroffen ist ... "

6.4.1.4 negativ-Definition

"vom Vorhaben nicht betroffen ist ... "

6.4.1.5 Die Betroffenheit wird in jedem Einzelfall nachvollziehbar und rechtssicher dokumentiert

6.4.1.6 Wer muss Zustimmung geben?

ist Richtervorbehalt 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?

6.4.2 Betroffene werden informiert

6.4.2.1 Die Information Betroffener wird gewährleistet durch …

- technische Maßnahmen im Zuge des Verfahrens
- organisatorische Maßnahmen im Zuge des Verfahrens

6.4.2.2 Vor Beginn des Vorhabens

6.4.2.3 Während des Vorhabens

6.4.2.4 Nach Beendigung des Verfahrens

6.4.2.5 Betroffene können gegen das Vorhaben Rechtsmittel ergreifen

6.4.2.6 Wie wird die unterbliebene Information Betroffener sanktioniert?

6.5 Verwendete Datenkategorien

- Betroffene Datenanwendung Bezeichnung laut Datenschutzregister / gesetzliche Grundlage)
- gesetzlich geregelt in …
- wird verknüpft mit …
- wird erweitert um…

ausführlich → Auskunftspflichten, „Datenkategorien“, „Begrifflichkeiten im TKG“ in diesem Dokument

6.5.1 Stammdaten

6.5.2 Verkehrsdaten

6.5.3 Zugangsdaten

6.5.4 Inhaltsdaten

6.5.5 Standortdaten

6.5.6 Vorratsdaten

6.5.7 Betriebsdaten

6.6 Datenspeicherung

6.6.1 Klare Definition zu speichernder Daten

6.6.2 Klare Definition der Speicherfristen

6.6.3 Klare Definition, wo Daten gespeichert werden dürfen

Entsprechend der Sensitivität der Daten / Datenanwendung ist sicherzustellen, dass die Datenspeicherung nur in Österreich / in einem EU-Land / Drittstaat mit vergleichbarem Datenschutzniveau zulässig ist.

6.6.4 Klare Definition von Löschvorgängen und -verantwortlichkeiten

Wer ist verantwortlich für nicht erfolgte Löschung? Wer haftet dafür?

6.7 Datenzugriff

6.7.1 Zugriffsberechtigte sind präzise und vollständig bezeichnet

Siehe z.B.:
"Insbesondere sieht die Richtlinie 2006/24/EG kein objektives Kriterium vor, das es erlaubt, die Zahl der Personen, die zum Zugang zu den auf Vorrat gespeicherten Daten und zu deren späterer Nutzung befugt sind, auf das angesichts des verfolgten Ziels absolut Notwendige zu beschränken. Vor allem unterliegt der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung den Zugang zu den Daten und ihre Nutzung auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken soll und im Anschluss an einen mit Gründen versehenen Antrag der genannten Behörden im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten ergeht."

6.7.2 Anzahl der Zugriffsberechtigten ist klar absehbar

6.7.3 Klare, nachvollziehbare und sanktionierbare Dokumentation von Datenzugriffen

Dies umfasst Erstellung, Änderung und Zugriff von/auf Daten.

6.8 Sicherheit der Verarbeitung

Datensicherheitsmaßnahmen (DSG) § 14

(1) Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.

(2) Insbesondere ist, soweit dies im Hinblick auf Abs. 1 letzter Satz erforderlich ist,
1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,
2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
3. jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,
4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,
5. die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,
6. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,
7. Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,
8. eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

(3) Nicht registrierte Übermittlungen aus Datenanwendungen, die einer Verpflichtung zur Auskunftserteilung gemäß § 26 unterliegen, sind so zu protokollieren, dass dem

Betroffenen Auskunft gemäß § 26 gegeben werden kann. In der Standardverordnung (§ 17 Abs. 2 Z 6) oder in der Musterverordnung (§ 19 Abs. 2) vorgesehene Übermittlungen bedürfen keiner Protokollierung.
(4) Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck - das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes - unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung, es sei denn, dass es sich um die Verwendung zum Zweck der Verhinderung oder Verfolgung eines Verbrechens nach § 278a StGB (kriminelle Organisation) oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, handelt.
(5) Sofern gesetzlich nicht ausdrücklich anderes angeordnet ist, sind Protokoll- und Dokumentationsdaten drei Jahre lang aufzubewahren. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung oder Dokumentation betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird.
(6) Datensicherheitsvorschriften sind so zu erlassen und zur Verfügung zu halten, dass sich die Mitarbeiter über die für sie geltenden Regelungen jederzeit informieren können.

Datengeheimnis
§ 15. (1) Auftraggeber, Dienstleister und ihre Mitarbeiter - das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis - haben Daten aus Datenanwendungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht (Datengeheimnis).
(2) Mitarbeiter dürfen Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Auftraggeber und Dienstleister haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, dass sie Daten aus Datenanwendungen nur auf Grund von Anordnungen übermitteln und das Datengeheimnis auch nach Beendigung des Arbeits-(Dienst-)verhältnisses zum Auftraggeber oder Dienstleister einhalten werden.
(3) Auftraggeber und Dienstleister dürfen Anordnungen zur Übermittlung von Daten nur erteilen, wenn dies nach den Bestimmungen dieses Bundesgesetzes zulässig ist. Sie haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur Datenübermittlung wegen Verstoßes gegen die Bestimmungen dieses Bundesgesetzes kein Nachteil erwachsen.
Vgl. auch **Art 10a StGG (Staatsgrundgesetz)**:
(1) Das Fernmeldegeheimnis darf nicht verletzt werden.
(2) Ausnahmen von der Bestimmung des vorstehenden Absatzes sind nur auf Grund eines richterlichen Befehles in Gemäßheit bestehender Gesetze zulässig.

6.8.1 Schutz gegen unrechtmäßige Zerstörung oder Veränderung

6.8.2 Schutz gegen unberechtigte Weitergabe

6.8.3 Schutz gegen unberechtigten Zugriff

6.8.4 Schutz gegen unrechtmäßige Verarbeitung

6.8.5 Sicherstellung, dass Verarbeitung dem Stand der Technik entspricht

6.8.6 Sicherstellung, dass die Verarbeitung am Stand der Technik bleibt

6.8.7 Sicherstellung gegen unzulässige, unberechtigte, unbefugte Speicherung

6.9 Sicherheit von Kommunikationsnetzen

Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist.

6.9.1 Eingriff in bestehende Kommunikationsnetzwerke

6.9.2 Eingriff in bestehende Datensysteme

6.9.3 Sicherstellung, dass nur rechtlich zulässiger Zugang möglich ist

6.9.4 Sicherstellung, dass nur eindeutig ermächtigte Personen Zugang zu Daten haben

6.10 Schutz gespeicherter oder übermittelter Daten

- Schutz gespeicherter oder übermittelter Daten gegen unberechtigten oder unbefugten Zugriff
- Schutz gespeicherter oder übermittelter Daten gegen unberechtigte oder unbefugte Weitergabe
- Schutz gespeicherter oder übermittelter Daten gegen unberechtigte oder unbefugte Veränderung

6.11 Erweiterung der Wirkungsfolgenabschätzung

Die WFA-Grundsatzverordnung sieht die Berücksichtigung folgender Dimensionen vor:
Wirkungsdimensionen
§ 6. (1) Die in **Anlage 1** näher ausgeführten Wirkungsdimensionen zu den in § 17 Abs. 1 BHG 2013 aufgezählten Auswirkungen sind:
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.

Diese Wirkungsdimensionen sind um einen echten Grundrechtsschutz zu erweitern. Richtschnur dabei müssen EMRK und EU-Grundrechtskatalog sein.

6.11.1 Grundrechtsschutz

Mit der Charta der Grundrechte der Europäischen Union wurde ein breites Spektrum von Grundrechten der Bürger und Einwohner der EU im EU-Recht verankert. Durch Inkrafttreten des Vertrags von Lissabon am 1. Dezember 2009 wurde die Charta für die Organe, Einrichtungen und Mitgliedstaaten der EU rechtsverbindlich.

6.11.1.1 Schutz der Würde des Menschen[248]

EU-Charta Artikel 1 - **Würde des Menschen**
Die Würde des Menschen ist unantastbar. Sie ist zu achten und zu schützen.
Artikel 2 - **Recht auf Leben**
Jeder Mensch hat das Recht auf Leben. Niemand darf zur Todesstrafe verurteilt oder hingerichtet werden.
Artikel 3 - **Recht auf Unversehrtheit**
Jeder Mensch hat das Recht auf körperliche und geistige Unversehrtheit. Im Rahmen der Medizin und der Biologie muss insbesondere Folgendes beachtet werden:
a) die freie Einwilligung des Betroffenen nach vorheriger Aufklärung entsprechend den gesetzlich festgelegten Einzelheiten,
b) das Verbot eugenischer Praktiken, insbesondere derjenigen, welche die Selektion von Menschen zum Ziel haben,
c) das Verbot, den menschlichen Körper und Teile davon als solche zur Erzielung von Gewinnen zu nutzen,
d) das Verbot des reproduktiven Klonens von Menschen.
Artikel 4 - **Verbot der Folter und unmenschlicher oder erniedrigender Strafe oder Behandlung**
Niemand darf der Folter oder unmenschlicher oder erniedrigender Strafe oder Behandlung unterworfen werden.
Artikel 5 - **Verbot der Sklaverei und der Zwangsarbeit**
Niemand darf in Sklaverei oder Leibeigenschaft gehalten werden. Niemand darf gezwungen werden, Zwangs- oder Pflichtarbeit zu verrichten. Menschenhandel ist verboten.

6.11.1.2 Freiheit und Sicherheit

Artikel 6 - Recht auf Freiheit und Sicherheit Jeder Mensch hat das Recht auf Freiheit und Sicherheit. Die Rechte nach Artikel 6 entsprechen den Rechten, die durch Artikel 5 EMRK garantiert sind, denen sie nach Artikel 52 Absatz 3 der Charta an Bedeutung und Tragweite gleichkommen. Die Einschränkungen, die legitim an diesen Rechten vorgenommen werden können, dürfen daher nicht über die Einschränkungen hinausgehen, die im Rahmen des wie folgt lautenden
Artikel 5 EMRK zulässig sind: „Jeder Mensch hat das Recht auf Freiheit und Sicherheit.
Die Freiheit darf nur in den folgenden Fällen und nur auf die gesetzlich vorgeschriebene Weise entzogen werden:
a) rechtmäßige Freiheitsentziehung nach Verurteilung durch ein zuständiges Gericht;
b) rechtmäßige Festnahme oder Freiheitsentziehung wegen Nichtbefolgung einer

[248] Aus Wikipedia: https://de.wikipedia.org/wiki/Menschenrechte .

rechtmäßigen gerichtlichen Anordnung oder zur Erzwingung der Erfüllung einer gesetzlichen Verpflichtung;
c) rechtmäßige Festnahme oder Freiheitsentziehung zur Vorführung vor die zuständige Gerichtsbehörde, wenn hinreichender Verdacht besteht, dass die betreffende Person eine Straftat begangen hat, oder wenn begründeter Anlass zu der Annahme besteht, dass es notwendig ist, sie an der Begehung einer Straftat oder an der Flucht nach Begehung einer solchen zu hindern;
d) rechtmäßige Freiheitsentziehung bei Minderjährigen zum Zweck überwachter Erziehung oder zur Vorführung vor die zuständige Behörde;
e) rechtmäßige Freiheitsentziehung mit dem Ziel, eine Verbreitung ansteckender Krankheiten zu verhindern, sowie bei psychisch Kranken, Alkohol- oder Rauschgiftsüchtigen und Landstreichern;
f) rechtmäßige Festnahme oder Freiheitsentziehung zur Verhinderung der unerlaubten Einreise sowie bei Personen, gegen die ein Ausweisungs- oder Auslieferungsverfahren im Gange ist.
Jeder festgenommenen Person muss unverzüglich in einer ihr verständlichen Sprache mitgeteilt werden, welches die Gründe für ihre Festnahme sind und welche Beschuldigungen gegen sie erhoben werden. Jede Person, die nach Absatz 1 Buchstabe c von Festnahme oder Freiheitsentziehung betroffen ist, muss unverzüglich einem Richter oder einer anderen gesetzlich zur Wahrnehmung richterlicher Aufgaben ermächtigten Person vorgeführt werden; sie hat Anspruch auf ein Urteil innerhalb angemessener Frist oder auf Entlassung während des Verfahrens. Die Entlassung kann von der Leistung einer Sicherheit für das Erscheinen vor Gericht abhängig gemacht werden.
Jede Person, die festgenommen oder der die Freiheit entzogen ist, hat das Recht, zu beantragen, dass ein Gericht innerhalb kurzer Frist über die Rechtmäßigkeit der Freiheitsentziehung entscheidet und ihre Entlassung anordnet, wenn die Freiheitsentziehung nicht rechtmäßig ist.
Jede Person, die unter Verletzung dieses Artikels von Festnahme oder Freiheitsentziehung betroffen ist, hat Anspruch auf Schadensersatz.“

Die Rechte nach Artikel 6 müssen insbesondere dann geachtet werden, wenn das Europäische Parlament und der Rat Gesetzgebungsakte im Bereich der justiziellen Zusammenarbeit in Strafsachen auf der Grundlage der Artikel 82, 83 und 85 des Vertrags über die Arbeitsweise der Europäischen Union, insbesondere zur Festlegung gemeinsamer Mindestvorschriften über die Tatbestandsmerkmale strafbarer Handlungen und die Strafen sowie über bestimmte Aspekte des Verfahrensrechts erlassen.[249]

[249] Quelle: Amtsblatt der Europäischen Union C 303/17 - 14.12.2007.

Freiheitsrechte sind sehr verschieden - ausgewählte Beispiele Systematisierung

	Schranken	**Beispiele**
Eingriffsvorbehalt formell	öffentl. Interesse + Verhältnismäßigkeit	Art 5, Art 6 3. Tb, Art 13 StGG, Art 1 1. ZPEMRK
Eingriffsvorbehalt materiell	best. Eingriffsgründe + Verhältnismäßigkeit	Art 8-11 EMRK, Art 2 4. ZPEMRK
Eingriffsvorbehalt ungeschrieben	zT wie formeller GV zT Verbot intentionaler Eingriffe + formeller GV	Art 4, Art 6 2. Tb StGG Art 17 + 17a StGG
vorbehaltlos	Eingriff = Verletzung	Art 3 EMRK, B Prov NV
Ausgestaltungsvorbehalt	AusgestaltungsG bestimmt das GR	Art 12 StGG

6.11.1.3 Privatsphäre

- Recht auf persönliche Freiheit (BVG persönliche Freiheit; Art. 5 EMRK)
- Recht auf Achtung des Privat- und Familienlebens (Art. 8 EMRK)
- Unverletzlichkeit des Hausrechtes (Art. 9 StGG; Gesetz zum Schutz des Hausrechts; Art. 8 EMRK)
- EU-Charta:

  Artikel 7 - Achtung des Privat- und Familienlebens: Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

6.11.1.4 Schutz personenbezogener Daten

- **Österreich:**

Recht auf Datenschutz (§ 1 DSG)

- **EU-Charta:**

Artikel 8 - **Schutz personenbezogener Daten**
Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

6.11.1.5 Gedanken- Gewissens- Religionsfreiheit

- **Österreich:**

Recht auf Glaubens- und Gewissensfreiheit einschließlich der Freiheit der Religionsausübung (Art. 14 und 16 StGG; Art. 9 EMRK)

- **EU-Charta:**

Artikel 10 - **Gedanken-, Gewissens- und Religionsfreiheit**
Jede Person hat das Recht auf Gedanken-, Gewissens- und Religionsfreiheit. Dieses Recht umfasst die Freiheit, die Religion oder Weltanschauung zu wechseln, und die Freiheit, seine Religion oder Weltanschauung einzeln oder gemeinsam mit anderen öffentlich oder privat durch Gottesdienst, Unterricht, Bräuche und Riten zu bekennen. Das Recht auf Wehrdienstverweigerung aus Gewissensgründen wird nach den einzelstaatlichen Gesetzen anerkannt, welche die Ausübung dieses Rechts regeln.

6.11.1.6 Freiheit der Meinungsäußerung, Informationsfreiheit

- **Österreich**:

Recht auf Meinungsäußerungsfreiheit (Art. 13 StGG)

- **EU-Charta:**

Artikel 11 - **Freiheit der Meinungsäußerung und Informationsfreiheit**
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. Die Freiheit der Medien und ihre Pluralität werden geachtet.
Art. 10 EMRK

6.11.1.7 Koalitionsfreiheit

- **Österreich:**

Recht auf Vereins- und auf Versammlungsfreiheit (Art. 12 StGG)

- **EU-Charta:**

Artikel 12 - **Versammlungs- und Vereinigungsfreiheit**

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. Politische Parteien auf der Ebene der Union tragen dazu bei, den politischen Willen der Unionsbürgerinnen und Unionsbürger zum Ausdruck zu bringen.

6.11.1.8 Demonstrationsrecht

- **Österreich:**

Recht auf Vereins- und auf Versammlungsfreiheit (Art. 12 StGG)

- **EU-Charta:**

Artikel 12 - **Versammlungs- und Vereinigungsfreiheit**
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. Politische Parteien auf der Ebene der Union tragen dazu bei, den politischen Willen der Unionsbürgerinnen und Unionsbürger zum Ausdruck zu bringen.

6.11.1.9 Asylrecht

EU-Charta:
Artikel 18 - **Asylrecht**
Das Recht auf Asyl wird nach Maßgabe des Genfer Abkommens vom 28. Juli 1951 und des Protokolls vom 31. Januar 1967 über die Rechtsstellung der Flüchtlinge sowie nach Maßgabe des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union (im Folgenden "die Verträge") gewährleistet. Artikel 19 - Schutz bei Abschiebung, Ausweisung und Auslieferung Kollektivausweisungen sind nicht zulässig. Niemand darf in einen Staat abgeschoben oder ausgewiesen oder an einen Staat ausgeliefert werden, in dem für sie oder ihn das ernsthafte Risiko der Todesstrafe, der Folter oder einer anderen unmenschlichen oder erniedrigenden Strafe oder Behandlung besteht.

6.11.1.10 Gleichheit, Nichtdiskriminierung

EU-Charta:
Artikel 20 - **Gleichheit vor dem Gesetz** Alle Personen sind vor dem Gesetz gleich.
Artikel 21 - **Nichtdiskriminierung** Diskriminierungen insbesondere wegen des Geschlechts, der Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Ausrichtung sind verboten. Unbeschadet besonderer Bestimmungen der Verträge ist in ihrem Anwendungsbereich jede Diskriminierung aus Gründen der Staatsangehörigkeit verboten.
Artikel 22 - **Vielfalt der Kulturen, Religionen und Sprachen**
Die Union achtet die Vielfalt der Kulturen, Religionen und Sprachen.
Artikel 23 - **Gleichheit von Frauen und Männern**

Die Gleichheit von Frauen und Männern ist in allen Bereichen, einschließlich der Beschäftigung, der Arbeit und des Arbeitsentgelts, sicherzustellen. Der Grundsatz der Gleichheit steht der Beibehaltung oder der Einführung spezifischer Vergünstigungen für das unterrepräsentierte Geschlecht nicht entgegen.

Artikel 24 - **Rechte des Kindes**

Kinder haben Anspruch auf den Schutz und die Fürsorge, die für ihr Wohlergehen notwendig sind. Sie können ihre Meinung frei äußern. Ihre Meinung wird in den Angelegenheiten, die sie betreffen, in einer ihrem Alter und ihrem Reifegrad entsprechenden Weise berücksichtigt. Bei allen Kinder betreffenden Maßnahmen öffentlicher Stellen oder privater Einrichtungen muss das Wohl des Kindes eine vorrangige Erwägung sein. Jedes Kind hat Anspruch auf regelmäßige persönliche Beziehungen und direkte Kontakte zu beiden Elternteilen, es sei denn, dies steht seinem Wohl entgegen.

Artikel 25 - **Rechte älterer Menschen**

Die Union anerkennt und achtet das Recht älterer Menschen auf ein würdiges und unabhängiges Leben und auf Teilnahme am sozialen und kulturellen Leben.

Artikel 26 - **Integration von Menschen mit Behinderung**

Die Union anerkennt und achtet den Anspruch von Menschen mit Behinderung auf Maßnahmen zur Gewährleistung ihrer Eigenständigkeit, ihrer sozialen und beruflichen Eingliederung und ihrer Teilnahme am Leben der Gemeinschaft.

6.11.1.11 Recht auf eine gute Verwaltung

EU-Charta:

Artikel 41 - **Recht auf eine gute Verwaltung**

(1) Jede Person hat ein Recht darauf, dass ihre Angelegenheiten von den Organen, Einrichtungen und sonstigen Stellen der Union unparteiisch, gerecht und innerhalb einer angemessenen Frist behandelt werden.

(2) Dieses Recht umfasst insbesondere

a) das Recht jeder Person, gehört zu werden, bevor ihr gegenüber eine für sie nachteilige individuelle Maßnahme getroffen wird,

b) das Recht jeder Person auf Zugang zu den sie betreffenden Akten unter Wahrung des berechtigten Interesses der Vertraulichkeit sowie des Berufs- und Geschäftsgeheimnisses,

c) die Verpflichtung der Verwaltung, ihre Entscheidungen zu begründen.

(3) Jede Person hat Anspruch darauf, dass die Union den durch ihre Organe oder Bediensteten in Ausübung ihrer Amtstätigkeit verursachten Schaden nach den allgemeinen Rechtsgrundsätzen ersetzt, die den Rechtsordnungen der Mitgliedstaaten gemeinsam sind.

(4) Jede Person kann sich in einer der Sprachen der Verträge an die Organe der Union wenden und muss eine Antwort in derselben Sprache erhalten.

6.11.1.12 Recht auf Zugang zu Dokumenten

EU-Charta:
Artikel 42 - **Recht auf Zugang zu Dokumenten**
Die Unionsbürgerinnen und Unionsbürger sowie jede natürliche oder juristische Person mit Wohnsitz oder satzungsmäßigem Sitz in einem Mitgliedstaat haben das Recht auf Zugang zu den Dokumenten der Organe, Einrichtungen und sonstigen Stellen der Union, unabhängig von der Form der für diese Dokumente verwendeten Träger.

6.11.1.13 Arbeitnehmerschutz, Umweltschutz, Verbraucherschutz

EU-Charta
Artikel 27 bis 38
"Solidarität"[250]

6.11.1.14 Zugang zu Verfahren vor einem ordentlichen Gericht bzw. Verwaltungsgericht

- **Österreich:**

Recht auf ein Verfahren vor dem gesetzlichen Richter (Art. 83 Abs. 2 B-VG)
Recht auf eine gerichtliche Entscheidung in Zivil- und Strafsachen und auf ein faires Verfahren sowie auf einen rechtsstaatlichen Mindeststandard im Strafprozess (Art. 6 EMRK)

- **EU-Charta:**

Artikel 47 - Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht:
Jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, hat das Recht, nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht einen wirksamen Rechtsbehelf einzulegen. Jede Person hat ein Recht darauf, dass ihre Sache von einem unabhängigen, unparteiischen und zuvor durch Gesetz errichteten Gericht in einem fairen Verfahren, öffentlich und innerhalb angemessener Frist verhandelt wird. Jede Person kann sich beraten, verteidigen und vertreten lassen. Personen, die nicht über ausreichende Mittel verfügen, wird Prozesskostenhilfe bewilligt, soweit diese Hilfe erforderlich ist, um den Zugang zu den Gerichten wirksam zu gewährleisten.
Artikel 48 - Unschuldsvermutung und Verteidigungsrechte:
(1) Jeder Angeklagte gilt bis zum rechtsförmlich erbrachten Beweis seiner Schuld als unschuldig.
(2) Jedem Angeklagten wird die Achtung der Verteidigungsrechte gewährleistet.
Artikel 49 - Grundsätze der Gesetzmäßigkeit und der Verhältnismäßigkeit im Zusammenhang mit Straftaten und Strafen:

[250] Lt. Laut Charterpedia http://fra.europa.eu/de/charterpedia/title/iv-solidarity .

(1) Niemand darf wegen einer Handlung oder Unterlassung verurteilt werden, die zur Zeit ihrer Begehung nach innerstaatlichem oder internationalem Recht nicht strafbar war. Es darf auch keine schwerere Strafe als die zur Zeit der Begehung angedrohte Strafe verhängt werden. Wird nach Begehung einer Straftat durch Gesetz eine mildere Strafe eingeführt, so ist diese zu verhängen.
(2) Dieser Artikel schließt nicht aus, dass eine Person wegen einer Handlung oder Unterlassung verurteilt oder bestraft wird, die zur Zeit ihrer Begehung nach den allgemeinen, von der Gesamtheit der Nationen anerkannten Grundsätzen strafbar war.
(3) Das Strafmaß darf zur Straftat nicht unverhältnismäßig sein.
Artikel 50 - Recht, wegen derselben Straftat nicht zweimal strafrechtlich verfolgt oder bestraft zu werden: Niemand darf wegen einer Straftat, derentwegen er bereits in der Union nach dem Gesetz rechtskräftig verurteilt oder freigesprochen worden ist, in einem Strafverfahren erneut verfolgt oder bestraft werden.

- Verfahrensgrundrechte

  faires Verfahren
  effektiver Rechtsschutz
- Verbot des Zwangs zur Selbstbezichtigung

6.11.1.15 Brief- und Fernmeldegeheimnis

Schutz des Briefgeheimnisses
(Art. 10 StGG; Art. 8 EMRK) und des Fernmeldegeheimnisses (Art. 10a StGG; Art. 8 EMRK)
Vgl. auch **Art 10a StGG (Staatsgrundgesetz)**:
(1) Das Fernmeldegeheimnis darf nicht verletzt werden.
(2) Ausnahmen von der Bestimmung des vorstehenden Absatzes sind nur auf Grund eines richterlichen Befehles in Gemäßheit bestehender Gesetze zulässig.

6.11.1.16 weitere Bürgerrechte

EU-Charta:
Artikel 39 - Aktives und passives Wahlrecht bei den Wahlen zum Europäischen Parlament
(1) Die Unionsbürgerinnen und Unionsbürger besitzen in dem Mitgliedstaat, in dem sie ihren Wohnsitz haben, das aktive und passive Wahlrecht bei den Wahlen zum Europäischen Parlament unter denselben Bedingungen wie die Angehörigen des betreffenden Mitgliedstaats.
(2) Die Mitglieder des Europäischen Parlaments werden in allgemeiner, unmittelbarer, freier und geheimer Wahl gewählt.
Artikel 40 - Aktives und passives Wahlrecht bei den Kommunalwahlen Die Unionsbürgerinnen und Unionsbürger besitzen in dem Mitgliedstaat, in dem sie ihren Wohnsitz haben, das aktive und passive Wahlrecht bei Kommunalwahlen unter denselben Bedingungen wie die Angehörigen des betreffenden Mitgliedstaats.
Artikel 43 - Der Europäische Bürgerbeauftragte Die Unionsbürgerinnen und Unionsbürger sowie jede natürliche oder juristische Person mit Wohnsitz oder

satzungsmäßigem Sitz in einem Mitgliedstaat haben das Recht, den Europäischen Bürgerbeauftragten im Falle von Missständen bei der Tätigkeit der Organe, Einrichtungen und sonstigen Stellen der Union, mit Ausnahme des Gerichtshofs der Europäischen Union in Ausübung seiner Rechtsprechungsbefugnisse, zu befassen.

Artikel 44 - Petitionsrecht Die Unionsbürgerinnen und Unionsbürger sowie jede natürliche oder juristische Person mit Wohnsitz oder satzungsmäßigem Sitz in einem Mitgliedstaat haben das Recht, eine Petition an das Europäische Parlament zu richten.
Artikel 45 - Freizügigkeit und Aufenthaltsfreiheit
(1) Die Unionsbürgerinnen und Unionsbürger haben das Recht, sich im Hoheitsgebiet der Mitgliedstaaten frei zu bewegen und aufzuhalten.
(2) Staatsangehörigen von Drittländern, die sich rechtmäßig im Hoheitsgebiet eines Mitgliedstaats aufhalten, kann nach Maßgabe der Verträge Freizügigkeit und Aufenthaltsfreiheit gewährt werden.
Artikel 46 - Diplomatischer und konsularischer Schutz Die Unionsbürgerinnen und Unionsbürger genießen im Hoheitsgebiet eines Drittlands, in dem der Mitgliedstaat, dessen Staatsangehörigkeit sie besitzen, nicht vertreten ist, den Schutz durch die diplomatischen und konsularischen Behörden eines jeden Mitgliedstaats unter denselben Bedingungen wie Staatsangehörige dieses Staates.

6.11.1.17 weitere Grundrechte

- **Österreich:**

Zu den verfassungsgesetzlich geschützten Rechten der Minderheiten zählen zum einen solche, die die Gleichbehandlung der Minderheitsangehörigen gebieten und Diskriminierungen untersagen (Art. 62 ff. Staatsvertrag von Saint-Germain-en-Laye), und zum anderen spezifische Sonderrechte des Gebrauchs der eigenen Sprache vor Behörden sowie im Bereich des Unterrichts- und Erziehungswesens und des Kulturlebens (Art. 7 Staatsvertrag von Wien)).

- **EU-Charta:**

Artikel 9 - Recht, eine Ehe einzugehen und eine Familie zu gründen Das Recht, eine Ehe einzugehen, und das Recht, eine Familie zu gründen, werden nach den einzelstaatlichen Gesetzen gewährleistet, welche die Ausübung dieser Rechte regeln.
Artikel 13 - **Freiheit der Kunst und der Wissenschaft**
Kunst und Forschung sind frei. Die akademische Freiheit wird geachtet.
Artikel 14 - Recht auf Bildung
Jede Person hat das Recht auf Bildung sowie auf Zugang zur beruflichen Ausbildung und Weiterbildung. Dieses Recht umfasst die Möglichkeit, unentgeltlich am Pflichtschulunterricht teilzunehmen. Die Freiheit zur Gründung von Lehranstalten unter Achtung der demokratischen Grundsätze sowie das Recht der Eltern, die Erziehung und den Unterricht ihrer Kinder entsprechend ihren eigenen religiösen, weltanschaulichen

und erzieherischen Überzeugungen sicherzustellen, werden nach den einzelstaatlichen Gesetzen geachtet, welche ihre Ausübung regeln.

Artikel 15 - Berufsfreiheit und Recht zu arbeiten

Jede Person hat das Recht, zu arbeiten und einen frei gewählten oder angenommenen Beruf auszuüben. Alle Unionsbürgerinnen und Unionsbürger haben die Freiheit, in jedem Mitgliedstaat Arbeit zu suchen, zu arbeiten, sich niederzulassen oder Dienstleistungen zu erbringen. Die Staatsangehörigen dritter Länder, die im Hoheitsgebiet der Mitgliedstaaten arbeiten dürfen, haben Anspruch auf Arbeitsbedingungen, die denen der Unionsbürgerinnen und Unionsbürger entsprechen.

Artikel 16 - Unternehmerische Freiheit

Die unternehmerische Freiheit wird nach dem Unionsrecht und den einzelstaatlichen Rechtsvorschriften und Gepflogenheiten anerkannt.

Artikel 17 - Eigentumsrecht

Jede Person hat das Recht, ihr rechtmäßig erworbenes Eigentum zu besitzen, zu nutzen, darüber zu verfügen und es zu vererben. Niemandem darf sein Eigentum entzogen werden, es sei denn aus Gründen des öffentlichen Interesses in den Fällen und unter den Bedingungen, die in einem Gesetz vorgesehen sind, sowie gegen eine rechtzeitige angemessene Entschädigung für den Verlust des Eigentums. Die Nutzung des Eigentums kann gesetzlich geregelt werden, soweit dies für das Wohl der Allgemeinheit erforderlich ist. Geistiges Eigentum wird geschützt.

6.11.2 Teilung der Verantwortung

Aus rechtspolitischen Grundsatzüberlegungen sollten bei Verfahren mit Grundrechtseingriffen die unterschiedlichen Rollen berücksichtigt werden:

- Antragstellende Behörde
- Bewilligende Behörde
- Ausführende Behörde
- Verfahrensbegleitende Kontrolle
- Nachkontrolle und Evaluierung

Um Verfahren transparent und nachvollziehbar zu gestalten, sind die Verantwortlichen für die einzelnen Verfahrensschritte organisatorisch zu trennen und möglichst unabhängig voneinander zu verankern.

Dieserart kann das Herausbilden von eigenen "Schallräumen", informellen Strukturen die nur sich selbst bestätigen und dabei eine eigenständige, unkontrollierte Entwicklung nehmen, eingeschränkt werden.

6.11.2.1 Verantwortung für Einleiten und Beantragen einer Maßnahme

6.11.2.2 Verantwortung für die Bewilligung einer Maßnahme

Die Bewilligung hat durch eine unabhängige, qualifizierte und sachlich kompetente Instanz, idealerweise einem unabhängigen Richtersenat, zu erfolgen. Bewilligungen bedürfen einer dokumentierten, im weiteren Verfahren anfechtbaren Dokumentation.

6.11.2.3 Verantwortung für die Durchführung der Maßnahme

6.11.2.4 Verantwortung für begleitende Kontrolle

Eine begleitende Verfahrenskontrolle, ausgestaltet als unabhängige, qualifizierte und kompetente Instanz könnte - mit entsprechenden Rechten ausgestattet, auch den kommissarischen Rechtsschutz für Betroffene wahrnehmen.

6.11.2.5 Verantwortung für Nachkontrolle und Evaluierung der Maßnahme

Nach Abschluss von Maßnahmen ist eine sinnvolle Nachkontrolle vorzunehmen, die Ordnungsmäßigkeit des Verfahrens zu prüfen. Bei eventuellen Verfahrensfehlern oder Abweichungen sind entsprechende Verbesserungsvorschläge zu erarbeiten und gegebenenfalls der ordentliche Rechtsweg zu beschreiten.
Vom Ergebnis dieser Maßnahmenkontrolle sind Betroffene zeitnah zu informieren.
Bei länger dauernden Maßnahmen sollte diese unabhängige Verfahrenskontrolle spätestens sechs Monate nach Bewilligung eingreifen.
Diese unabhängige Nachkontrolle hat Daten quantitativer und qualitativer Art für die Evaluierung und Abschätzung der Zielerreichung aufzubereiten und regelmäßig zu veröffentlichen.

6.11.2.6 Verantwortung für den Rechtschutz von durch die Maßnahme Betroffenen

Betroffene sind von sie betreffenden Maßnahmen so früh wie möglich zu informieren. Diese Information muss auch Informationen über mögliche Rechtsmittel enthalten.
Im Falle von Beschwerden sind Betroffene von Amts wegen mit qualifizierter juristischer Beratung und Verfahrenshilfe zu unterstützen.
Sollte die frühzeitige Information Betroffener das Erreichen des vorgesehenen und bewilligten Zieles verhindern, ist dies im Rahmen des Verfahrens zu dokumentieren und jene Instanz zu informieren, die mit dem kommissarischen Rechtschutz beauftragt ist.

6.11.3 Grundrechtskatalog

6.11.3.1 Freiheitsrechte

6.11.3.2 Verfahrensrechte

6.11.3.3 soziale Rechte

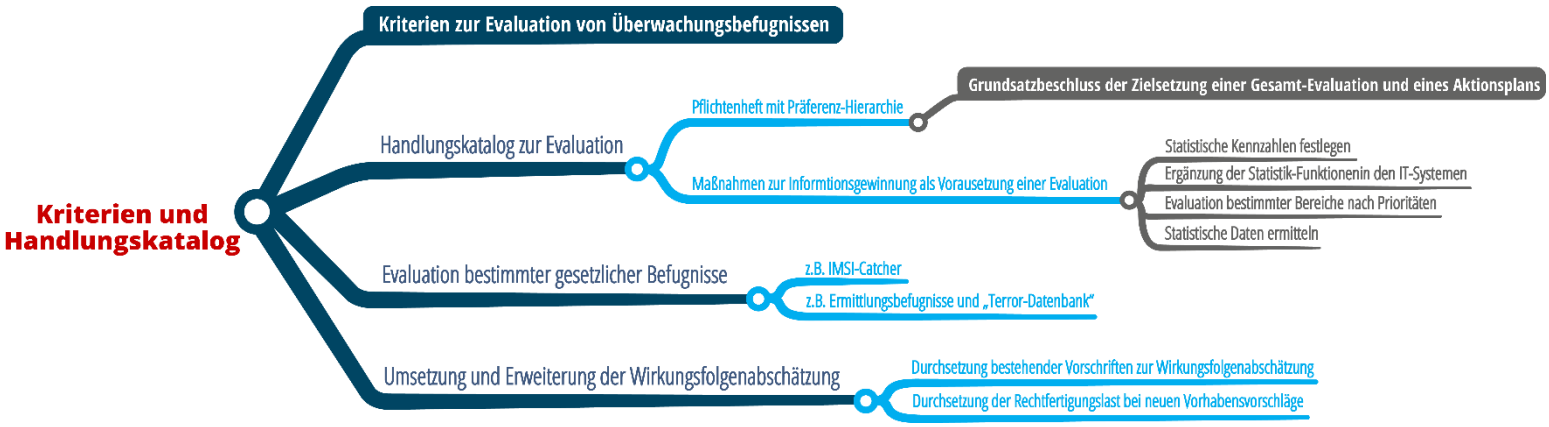
6.11.3.4 politische Rechte

6.11.3.5 Gleichheitsrechte

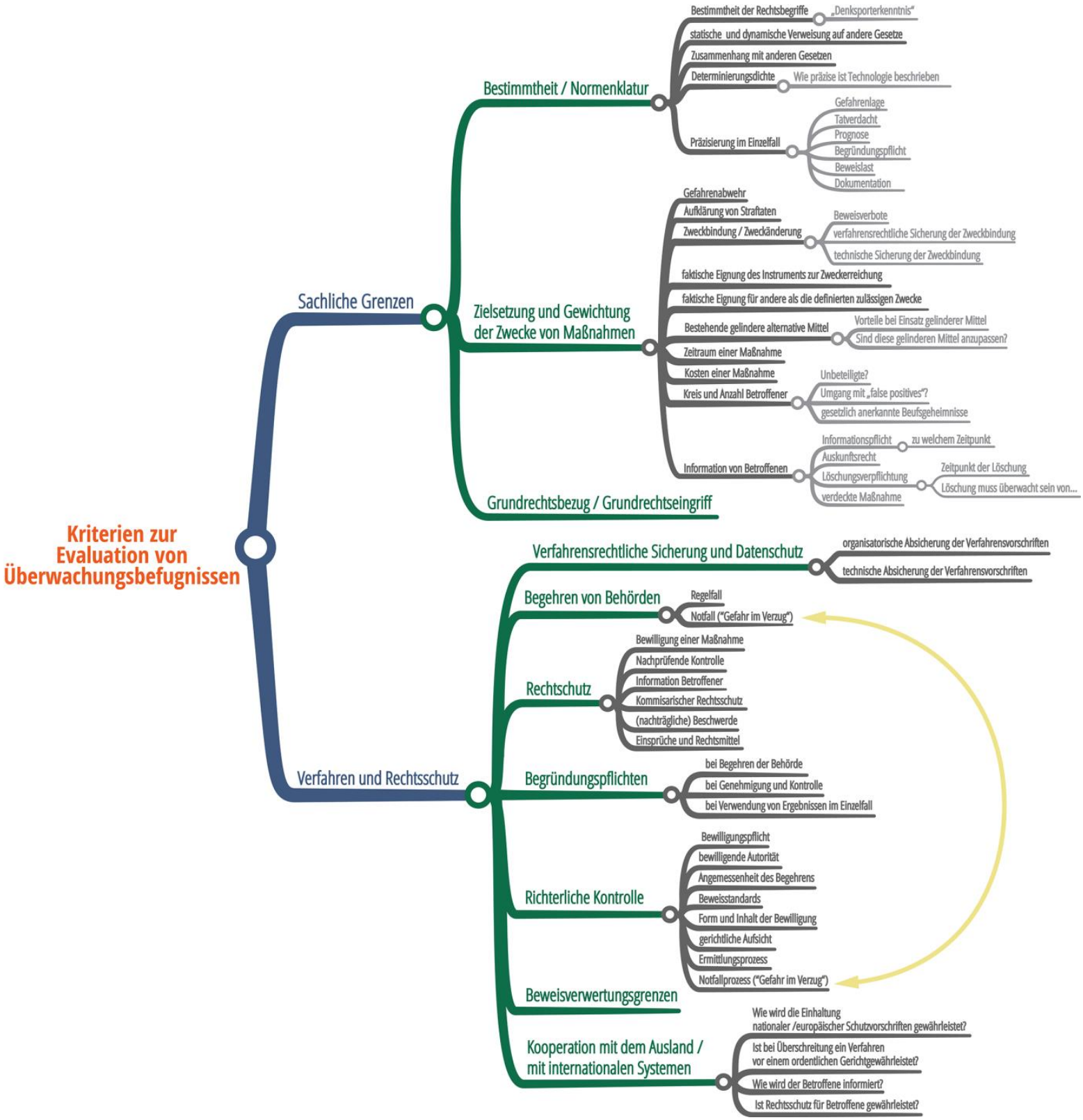
7 Kriterien und Handlungskatalog

Dieses Kapitel stellt die Conclusio von HEAT dar. Die Zusammenführung aller interdisziplinären Teile aus Technologie, Recht und Sozialwissenschaften mündet in einer Mindmap, die wiederum in verschiedene abgrenzbare Bestandteile zerlegt wird. Die Mindmap „Kriterien und Handlungsempfehlungen zur Evaluation" zeigt zuerst den Überblick, in der Folge werden die einzelnen Bestandteile jeweils separat dargestellt. Während die Mindmap mit allen Informationen auch online unter www.epicenter.works/HEAT zu finden ist, werden die darin enthaltenen Informationen im vorliegenden Handbuch auch als Text dargestellt, bei dem die Gliederungsstruktur der Mindmap folgt.

Aus der vorangehenden Analyse werden zunächst die Kriterien zur Evaluation der Anti-Terror Gesetze herausgearbeitet und dargestellt. Darauffolgend und aufbauend werden die Empfehlungen für die verschiedenen Arten der Evaluation jeweils in einem abgrenzbaren Teil der Mindmap und wieder zugleich in Textform dargestellt.



8 Kriterien zur Evaluation von Überwachungsbefugnissen



8.1 Sachliche Grenzen

8.1.1 Bestimmtheit / Normenklarheit

8.1.1.1 Bestimmtheit der Rechtsbegriffe

- **Deskriptive Begriffe:**

Begriffe, deren Bedeutungsgehalt (Begriffskern und Begriffshof) im Zusammenhang der Norm aus dem allgemeinen Sprachgebrauch im Wesentlichen erschließbar ist, ohne dass es besonderer juristischer Auslegungskunst bedarf: z.B.: Handlung, Hilfe, Abwehr, Leben, Gesundheit, etc.

- **Normative Begriffe:**

Begriffe, deren Bedeutungsgehalt (Begriffskern und Begriffshof) im Zusammenhang der Norm nur durch juristische Auslegung erschließbar ist und daher eine entsprechende Legaldefinition erfordert.
z.B. Terrorismus, Sicherheit, Gruppierung, verfassungsgefährdender Angriff, etc.

Bei der Verwendung normativer Begriffe ist darauf Bedacht zu nehmen, dass die Norm verständlich bleibt und der Bedeutungsgehalt nicht nur im Sinne des "Denksporterkenntnis" des VfGH erschließbar ist.

- "Denksporterkenntnis"

  siehe VfGH Sammlung VfSlg. 12420/1990:
  Aus dem rechtsstaatlichen Gedanken der Publizität des Gesetzesinhaltes kann die Schlussfolgerung gezogen werden, dass der Gesetzgeber der betroffenen Öffentlichkeit den Inhalt seines Gesetzesbeschlusses in klarer und erschöpfender Weise zur Kenntnis bringen muss, weil andernfalls der Normunterworfene nicht die Möglichkeit hat, sich der Norm gemäß zu verhalten.[1] Daraus lässt sich ableiten, dass Gesetze, welche auch tiefgreifende Grundrechtseingriffe beinhalten, verständlich und klar formuliert werden müssen, dass der einzelne Bürger erkennen kann wann er von dieser Norm betroffen ist und diese auch versteht, ohne eine „subtile Sachkenntnis, außerordentlichen methodischen Fähigkeiten und einer gewissen Lust zum Lösen von Denksportaufgaben“[2] zu besitzen. Dabei bedürfen Ermächtigungen zu Grundrechtseingriffen einer gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenbestimmtheit und Normenklarheit entspricht.[3]
  [1] So auch der VfGH in seiner E VfSlg 3130/1956.
  [2] VfSlg 12420/1990.
  [3] BvR 518/02, 150.

8.1.1.2 Statische und dynamische Verweisungen auf andere Gesetze

Statische und dynamische Verweisungen in Rechtsnormen können notwendig sein, um bei gesetzesübergreifenden Zusammenhängen möglichst auf eine systematische Einheit der Rechtsordnung hinzuwirken und unnötige Redundanzen in den Rechtstexten zu vermeiden. Die Verweisungstechnik darf aber nicht dazu führen, dass eine Rechtsnorm nur noch für Spezialisten der jeweiligen Materie verständlich ist. Die Regelungstechnik der Normenverweise sollte daher zurückhaltend und mit Bedacht auf die Normenklarheit zum Einsatz kommen.

8.1.1.3 Zusammenhang mit anderen Gesetzen

Häufig bestehen bei Gesetzen mit Eingriffsbefugnissen in Grundrechte auch immanente Zusammenhänge mit anderen Gesetzen, die nicht an jeder Stelle explizit gemacht sind. Ein Beispiel ist die Definition des "gefährlichen Angriffs" in § 16 SPG, der an die Strafbarkeit nach dem StGB oder dem Nebenstrafrecht anknüpft und dabei auf bestimmte Begehungsformen (nur Vorsatzdelikte) abstellt. Jede Ermittlungs- und Eingriffsbefugnis nach dem SPG muss in der Folge in diesem Zusammenhang gesehen und beurteilt werden, wenngleich die Eingriffsnormen des SPG dann regelmäßig selbst nicht mehr unmittelbar auf das materielle Strafrecht verweisen.
Ein anderes Beispiel ist das Datenschutzgesetz 2000, das im Stufenbau der Rechtsordnung durch § 1 DSG im Verfassungsrang steht und der einfachgesetzlichen Umsetzung in den weiteren Bestimmungen des DSG zugleich die besondere Norm (lex specialis) zur Verarbeitung personenbezogener Daten darstellt. Das DSG ist auch dann beachtlich, wenn ein Gesetz in einer bestimmten Materie, z.B.: die Bundesabgabenordnung, keinen ausdrücklichen Verweis auf das DSG oder einzelne Bestimmungen enthält - die Schranken des DSG sind trotzdem beachtlich.
Optimal ist in komplexen Fällen, wenn zumindest die Erläuternden Bemerkungen auf systematische Zusammenhänge eingehen und allfällige Unklarheiten so gut wie möglich auflösen.

8.1.1.4 Determinierungsdichte

- **Wie präzise ist Technologie beschrieben?**

Rechtsgrundlagen für Überwachungsbefugnisse stehen typischerweise im Zusammenhang mit Technologie, mit der die entsprechende Maßnahme auch umgesetzt werden kann. Die besondere legistische Herausforderung besteht darin, dass die normativen Grenzen (Sollen) und die faktischen technischen Möglichkeiten (Sein) in der Praxis möglichst nahe beieinander liegen sollten. Dementsprechend wichtig ist die rechtliche Determinierung der eingesetzten Technologie. Diese erfolgt aber nach der bisherigen Erfahrung häufig gar nicht explizit oder nur sehr oberflächlich und so bleibt der Exekutive meistens sehr viel Spielraum, welche technischen Mittel konkret zum Einsatz gelangen. Ein Beispiel hierfür ist der IMSI Catcher. Die Rechtsgrundlage des § 53 Abs. 3b SPG erlaubt, "technische Mittel zur Lokalisierung der Endeinrichtung" einer Person zum Einsatz zu bringen. Aus der Norm geht nicht hervor, dass damit die

Rechtsgrundlage für den Einsatz von IMS Catchern geschaffen wurde. Diese Technologie existierte bereits zum Zeitpunkt der Entstehung der Norm und schon bei der Ausarbeitung der SPG Novelle 2007 war klar, dass ein IMSI Catcher nicht nur Endgeräte lokalisieren kann, sondern vor allem dazu dient, Gespräche inhaltlich ohne Beteiligung des Telekommunikationsanbieters eines bestimmten, durch die IMSI gefilterten Teilnehmers zu überwachen. Hier besteht eine große Kluft zwischen dem rechtlich Zulässigen und dem technisch Möglichen.

    - Wird die Technologie bereits eingesetzt?
    - Existiert dafür eine ausdrückliche Rechtsgrundlage?
    - Existiert dafür eine implizite Rechtsgrundlage?
    - Sind alle möglichen Funktionen der Technologie rechtlich eindeutig gedeckt?
    - Erfordert die Rechtsgrundlage funktionelle Einschränkungen der Technologie? sind allfällige Einschränkungen technisch abgesichert / befördert?
    - Ist eine technische oder organisatorische Einschränkung überhaupt möglich? Sind allfällige Einschränkungen nur organisatorisch möglich?
    - Wie wird dies abgesichert?
    - Gibt es nachvollziehbare, dokumentierte Safeguards?
- Wie wird die Rechtsgrundlage angepasst bei technologischen Erweiterungen / Weiterentwicklungen?

8.1.1.5 Präzisierung im Einzelfall

- **Gefahrenlage**
- Welche Konkretisierung ist im Einzelfall vorgeschrieben?
- Wo und von wem ist dies konkret zu begründen?
- Auf welche bestimmten Tatsachen bezieht sich die Annahme einer Gefahrenlage?
- **Tatverdacht**
- Ist bereits ein konkreter Tatverdacht als Eingriffsvoraussetzung erforderlich (wie z.B.: bei Festnahmen nach der StPO)?
- Auf welche Delikte bezieht sich der Tatverdacht und in welchem Zusammenhang steht dieser mit der begehrten Maßnahme?
- Gibt es Abstufungen zum Tatverdacht (z.B.: "dringender Tatverdacht" als Voraussetzung für die U-Haft nach der StPO)?
- Geht es um eine versuchte oder um eine bereits ausgeführte Tat?
- **Prognose**
- Auf welche konkrete(n) Gefahr(en) bezieht sich die Prognose?
- Auf welche Fakten stützt sich die Prognose?
- Bezieht sich die Prognose auf eine bestimmte Person und deren Verhalten?

- Wird die Prognose mit technologischen Hilfsmittel erstellt? Welchen Einfluss haben dann die menschlichen Akteure (Thema automatisierte Einzelentscheidung)?
- Was passiert, wenn sich zu einem späteren Zeitpunkt die Prognose als unrichtig erweist? Wie sind die Auswirkungen auf ein laufendes Ermittlungsverfahren geregelt?
- Welche konkreten Rechtsgüter sind von der Gefahrenprognose betroffen und in welchem Verhältnis stehen die Maßnahmen dazu?

- **Begründungspflicht**

- Ist konkretisiert, welches Organ an welcher Stelle welche Begründungspflichten hat?
- Welche Begründungen hat das Ersuchen um eine Maßnahme zu enthalten? Welche Begründungen sind vom genehmigenden Organ (z.B.: Richter, Rechtsschutzbeauftragter) auszuführen?
- Gibt es Begründungspflichten nur in bestimmten Konstellationen? (z.B.: Begründungspflicht nur bei Ablehnung der Maßnahme, ansonsten "Stampiglien-Bewilligung" in der Praxis der österreichischen Gerichte, die Bewilligung erfolgt also ohne Begründung nur mit Stempel) - gibt es dafür sachliche Argumente abseits der Kostenersparnis durch Aufwandsreduktion?

- **Beweislast:** Grundsätzlich gelten im Strafverfahren die Garantien eines fairen Verfahrens nach Artikel 6 EMRK und damit insbesondere die Unschuldsvermutung. Das bedeutet, dass den Ankläger die Last trifft, seine Anschuldigungen zu beweisen, während der Angeklagte bei Zweifeln an dessen Schuld freizusprechen ist. Diese Garantie greift nach Artikel 6 Absatz 1 EMRK aber erst in einem Verfahren vor einem Gericht, das "über die Stichhaltigkeit der gegen ihn erhobenen strafrechtlichen Anklage zu entscheiden hat". Wenn zur Aufklärung einer konkreten strafbaren Handlung ermittelt wird, ist die Strafprozessordnung anwendbar und die Garantien des Art 6 EMRK gelten für jeden konkreten Beschuldigten. Personen die zwar in den Ermittlungen ausgeforscht, befragt und möglicherweise durchleuchtet werden, jedoch nicht selbst als Beschuldigte adressiert werden, können sich "nur" auf die Grundrechte auf Privatsphäre (Art 8 EMRK) und Datenschutz (§ 1 DSG) berufen, von Art 6 EMRK sind sie aber nicht geschützt. Ebenso wenig greift dieser Schutz im Bereich der präventiven Gefahrenabwehr, wo definitionsgemäß noch gar keine Straftat begangen wurde, deretwegen eine bestimmte Person beschuldigt werden könnte, also ist auch die Unschuldsvermutung des Art 6 EMRK als Beweislastregel nicht anwendbar, während Eingriffe in andere Grundrechte durch die Ermittlungshandlungen gesetzlich zulässig sind.

Bei diesem Kriterium geht es darum, in wie weit sich eine Person im Rahmen von polizeilichen Ermittlungen Rechtfertigen oder "freibeweisen" muss, um weitere Grundrechtseingriffe im Rahmen weiterer Ermittlungen zu verhindern. Im Bereich der "digitalen Forensik" besteht hierzu vor allem die Zusatzfrage, welche Aussagekraft bzw. welchen "Beweiswert" einer ermittelten Information beizumessen ist. Dies betrifft z.B.: die Ausforschung eines Anschlussinhabers anhand einer IP-Adresse oder die Auskunft über historische Standortdaten zu einer bestimmten Endeinrichtung. In beiden Fällen lässt die Information keinen zwingenden Schluss zum tatsächlichen Nutzer des Anschlusses bzw. des Endgeräts zu. Dennoch besteht im Rahmen von Ermittlungshandlungen typischerweise die (widerlegbare) Vermutung, dass der Anschlussinhaber auch der Nutzer zum fraglichen Zeitpunkt war oder über diesen zumindest weitere Auskünfte geben kann. Die Frage ist, welche Konsequenzen es für den Betroffenen hat, wenn er diese Erwartungshaltung enttäuscht und keine weitere Aufklärung bringt. In der Praxis muss dann z.B.: der Anschlussinhaber zu einer IP-Adresse unter Umständen damit rechnen, dass sein gesamter Rechnerbestand innerhalb des allenfalls dahinterstehenden Netzwerks zur Beweissicherung beschlagnahmt wird, weil die IP-Adresse der einzige Ermittlungshinweis ist. Wenn in einem solchen Sachverhalt ein Unternehmen betroffen ist, könnte mit einer solchen Maßnahme der wirtschaftliche Niedergang verbunden sein.

Da es im IT-Bereich noch keine gesetzlichen verschuldensunabhängigen Haftungsregeln gibt wie etwa nach dem Eisenbahn- und Kraftfahrzeug Haftpflicht-Gesetz (EKHG), ist im Zusammenhang mit Ergebnissen digitaler Beweissicherung wichtig, dass sich der Gesetzgeber schon bei der Einführung neuer Ermittlungsbefugnisse damit auseinandersetzt, welche Risiken damit verbunden sind und ob allenfalls mit Beweislastregeln oder auch nur Überlegungen dazu eine möglichst faire Risikoverteilung erreicht werden kann.

- **Dokumentation:** Die Beachtung der vorangehend aufgestellten Kriterien zur Präzisierung im Anwendungsfall kann nur sichergestellt werden, wenn es entsprechende Dokumentationspflichten in jedem Abschnitt eines Verfahrens gibt, die den Hergang einer nachträglichen Prüfung zugänglich machen.

8.1.2 Zielsetzung und Gewichtung der Zwecke von Maßnahmen

8.1.2.1 Gefahrenabwehr

Gerade im Bereich polizeilicher Eingriffsbefugnisse ist der Unterschied rechtlich bedeutsam, ob eine Maßnahme der Gefahrenabwehr oder der Strafverfolgung (oder beiden Zwecken) dient. Die Gefahrenabwehr oder die noch weiter ins Vorfeld verlagerte "erweiterte Gefahrenerforschung" basiert notwendigerweise weitgehend auf Prognosen über zukünftiges Verhalten. Das Risiko, dass unbeteiligte Personen nur zufällig ins Netz der Ermittlungen geraten und dabei Grundrechtseingriffe hinnehmen müssen (Streubreite des Eingriffs), ist typischerweise im Hinblick auf Prognosen deutlich größer

als bei Ermittlungen zu einer bestimmten bereits verwirklichten Tat. Entlang der Zieldefinitionen im Rahmen eines Vorhabens sollte danach getrachtet werden, auch in der Umsetzung eine möglichst saubere Trennung zwischen Prävention und Strafverfolgung zu erreichen.

8.1.2.2 Aufklärung von Straftaten

8.1.2.3 Zweckbindung / Zweckänderung

- Beweisverbote
- verfahrensrechtliche Sicherung der Zweckbindung
- technische Sicherung der Zweckbindung

8.1.2.4 Faktische Eignung des Instruments zur Zweckerreichung

8.1.2.5 Faktische Eignung für andere als die definierten zulässigen Zwecke

8.1.2.6 Bestehende gelindere alternative Mittel?

- Vorteile bei Einsatz gelinderer Mittel
- Nachteile bei Einsatz gelinderer Mittel
- sind diese gelinderen Mittel anzupassen?

8.1.2.7 Zeitraum einer Maßnahme

8.1.2.8 Kosten einer Maßnahme

Es ist zu prüfen, ob die Kosten eines Vorhabens in einem angemessenen Verhältnis zum wahrscheinlich zu erwartenden Erfolg stehen. Die zu erwartenden Kosten eines Vorhabens sind in der Vorlage anzuführen, wesentliche Abweichungen vom Kostenrahmen sind in einem angemessenen Zeitraum nach der Umsetzung des Vorhabens zu dokumentieren und zu begründen. Wesentliche Abweichungen vom vorgegebenen Kostenrahmen bedürfen einer zusätzlichen Rechtfertigung.
Neben den Kosten zur Umsetzung und zum Betrieb des Vorhabens ist auch zu fragen, ob gesellschaftliche (Folge-)Kosten in relevantem Ausmaß entstehen und wie allenfalls eine faire Verteilung erreicht wird.
Wichtig erscheint aber im Hinblick auf die bisherige Praxis im Rahmen der gesetzlichen Einführung von Überwachungsbefugnissen, dass die "Wirkungsorientierte Folgenabschätzung" (WFA) nicht auf die Kostenfrage reduziert wird. Vielmehr ist zu fragen, ob sich aus anderen Kriterien im Rahmen der Folgenabschätzung weitere Kosten ergeben, beispielsweise für begleitende Aus- und Fortbildungsmaßnahmen oder für effektive Kontrollinstanzen.

8.1.2.9 Kreis und Anzahl Betroffener

- Unbeteiligte?
- Umgang mit "false positives"?
- gesetzlich anerkannte Berufsgeheimnisse

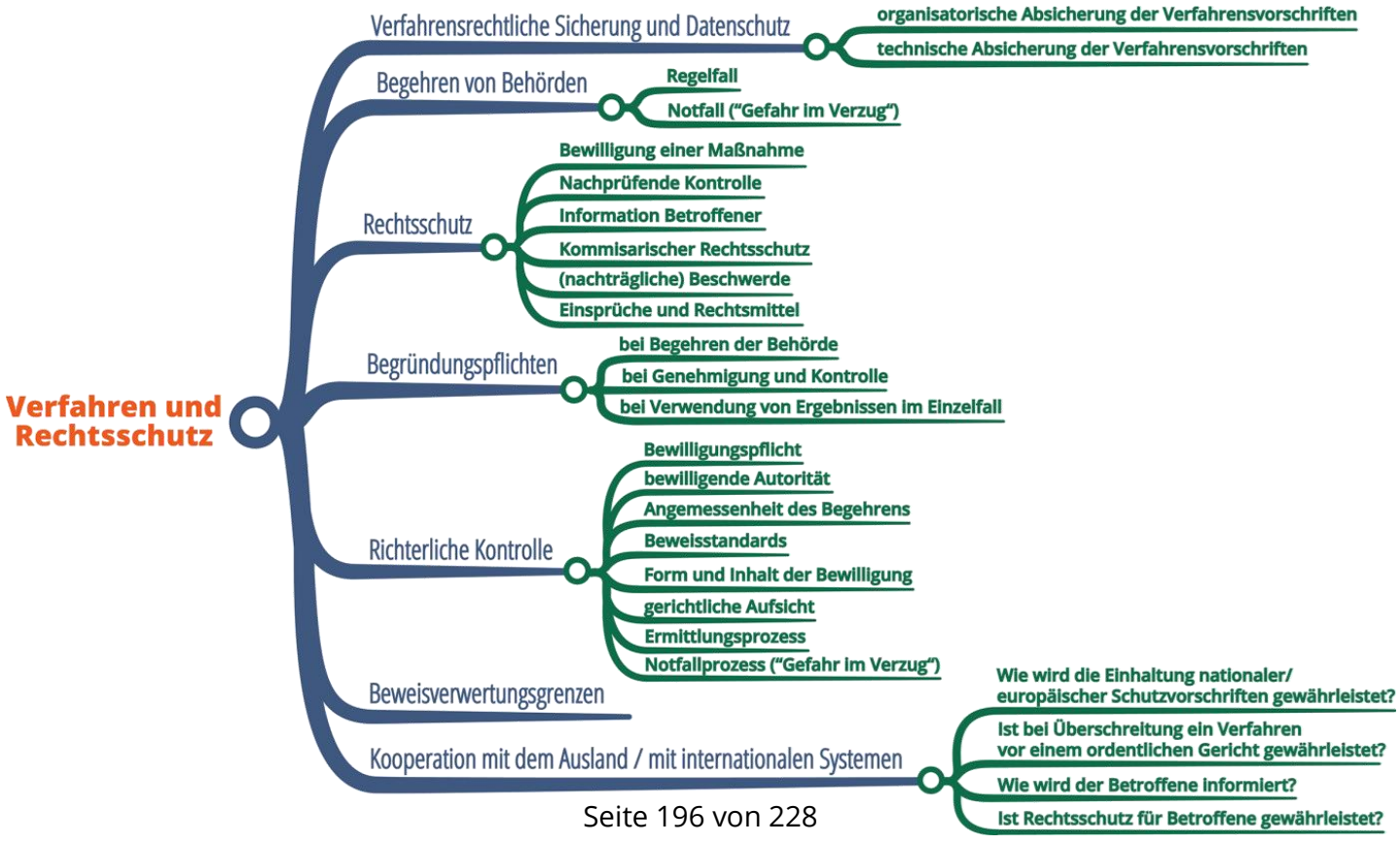
8.1.2.10 Information von Betroffenen

- Informationspflicht
  - zu welchem Zeitpunkt
- Auskunftsrecht
- Löschungsverpflichtung
  - Zeitpunkt der Löschung
  - Löschung wird überwacht von …
- verdeckte Maßnahme

8.1.3 Grundrechtsbezug / Grundrechtseingriffe

- Welche Grundrechte sind betroffen?
- besteht ein formeller Eingriffsvorbehalt?
- besteht ein materieller Eingriffsvorbehalt?
- Ist die konkrete Zielsetzung vom Eingriffsvorbehalt gedeckt?
- Grundrechtsprüfung nach Schema des VfGH / EGMR / EuGH

8.2 Verfahren und Rechtsschutz



Der Normalfall muss richterliche Kontrolle sein.
Sonderregelungen (Senatsähnliche Strukturen, …) müssen mindestens den Anforderungen für Tribunale nach der Rechtsprechung des EGMR genügen

Gerichtliche Bewilligung
Die Bewilligung zur Datenauskunft muss durch ein unabhängiges, unparteiliches und kompetentes Gericht erfolgen. Die Richter müssen genügend Kurse in dieser Materie absolviert haben um eine informierte Entscheidung treffen zu können und über technische, prozessrechtliche und andere notwendige Expertise verfügen. Oftmals sind die Genehmigungsprozesse nicht öffentlich, daher sollen diese transparent gestaltet werden und mittels einer Durchlaufstelle überwacht und festgehalten werden. Das Gericht darf nur die Auskunft bewilligen, wenn das Begehren alle oben genannten Anforderungen auch tatsächlich erfüllt und wenn die Maßnahme das gelindeste Mittel darstellt. Dabei obliegt der ansuchenden Stelle die Beweislast. Das Gericht steht in der Pflicht die genehmigte Maßnahme zu überwachen und muss sicherstellen, dass der Staat über die durchgeführte Maßnahme berichtet.
Die Bewilligung ist schriftlich zu erteilen und hat zu enthalten:

- Name des Gerichts, Richters und Datum
- Gesetzliche Grundlage
- Geltungsbereich und Dauer der bewilligten Maßnahme
- Bezeichnung des zugrundeliegenden Begehrens
- Schriftliche Stellungnahme

Der genehmigende Richter soll die Ermittlungsergebnisse sichern. Ein anderer Richter soll ernannt werden um die Ergebnisse zu verwalten. Sobald die Ermittlungen abgeschlossen sind, müssen die Informationen vernichtet werden. Damit wird der Vorratsdatenspeicherung entgegengewirkt, wo eine Speicherung der Daten auf einen langen Zeitraum vorgesehen war. Ermittlungen sollen öffentlich geführt werden. Auch dies hilft dabei, den Prozess transparenter zu gestalten. Sollten bei dem Ermittlungsprozess Unregelmäßigkeiten/ Verstöße gegen die Bewilligung oder Gesetze vorkommen, hat der Richter die Autorität, ermittelnde Behörden zu suspendieren oder sonst zu bestrafen.

8.2.1 Verfahrensrechtliche Sicherung und Rechtsschutz

- organisatorische Absicherung der Verfahrensvorschriften
- technische Absicherung der Verfahrensvorschriften

8.2.2 Begehren von Behörden

Behördliches Begehren
Wenn die Behörde ein Begehren zur Auskunft über Daten stellt, muss dieses im Einklang mit der bestehenden Rechtslage erfolgen. Die Befugnis zur Stellung des Begehrens muss

mit den internationalen Grundrechten vereinbar sein und die Rechtsgrundlage muss hinreichend bestimmt sein.

Das Begehren muss sich auf die notwendigsten Daten beschränken, so dass keine bzw. kaum Daten von unbeteiligten Dritten oder zu viele Daten von Verdächtigten gesammelt werden. Dabei ist es wichtig, dass das Auskunftsbegehren das gelindeste Mittel darstellt, um an notwendige Informationen zu gelangen. Des Weiteren muss der Rahmen der notwendigen Informationen im Vorhinein von den Behörden bestimmt werden. Das Ansammeln von Daten auf "Vorrat" für mögliche spätere Entwicklungen ist ohne konkreten Bezug zum gegenwärtigen Ermittlungsstand unzulässig.

Das Begehren muss schriftlich an das Gericht gestellt werden und die Behörde muss die Richtigkeit und Stichhaltigkeit der Informationen in dem Begehren bestätigen. Das Begehren muss den Namen der Behörde, der Position des Stellers, die Ermächtigung zur Stellung des Begehrens und eine Signatur enthalten. Der Prozess muss rechtlich genau beschrieben sein. Dabei ist der Steller des Begehrens für die Informationen in dem Begehren verantwortlich.
Für jede Auskunft und jede Überwachungsmaßnahme muss ein neues Begehren gestellt werden. Dieses hat das legitime Ziel der Maßnahme und die notwendigen Informationen zur Erreichung desselben zu enthalten. Weiters muss es die Rechtsgrundlage enthalten, sowie eine genaue Beschreibung von den betroffenen Datenbanken, Geräten, Accounts und Informationen. Außerdem muss dargelegt werden, warum die Maßnahme die notwendigen Informationen erwarten lässt, auf welchen Tatsachen die Annahme basiert, dass sich die Informationen in dem Account oder Gerät befinden und schließlich, dass die Maßnahme nicht mehr Daten als unbedingt erforderlich umfassen darf.

8.2.2.1 Regelfall

Behörde stellt das Begehren

- Das Begehren muss im Einklang mit dem Gesetz erfolgen
- Die Befugnis der Behörde muss im Einklang mit den internationalen Grundrechten stehen
- Das Gesetz muss Gegenstand eines öffentlichen Diskurses gewesen sein

Die Notwendigkeit des Begehrens

- Gelindestes Mittel, um an notwendige Information zu gelangen, um ein legitimes Ziel zu verfolgen
- Die Behörde muss den Rahmen der notwendigen Informationen bestimmen
- Dieser Rahmen muss zugeschnitten werden auf den geringstmöglichen Einfluss auf andere geschützte Informationen

Form des Begehrens

- Das Begehren muss schriftlich an das Gericht gestellt werden und die Behörde, sowie die Richtigkeit und Genauigkeit der Informationen in dem Begehren bestätigen
- Das Begehren muss den Namen der Behörde, der Position des Stellers, die Ermächtigung zur Stellung des Begehrens und eine Signatur enthalten
- Der Prozess muss rechtlich genau beschrieben sein
- Der Steller des Begehrens ist für die Informationen in dem Begehren verantwortlich

Inhalt des Begehrens

- Das legitime Ziel der Maßnahme und die notwendigen Informationen zur Erreichung
- Die relevante Rechtsgrundlage
- Der präzise Anwendungsbereich der Maßnahme
- Für jede Maßnahme soll ein neues Begehren gestellt werden
- Genau Beschreibung von betroffenen Datenbanken, Geräte, Accounts, Informationen

Beweislast – Das Begehren soll enthalten:

- Die bestimmten Tatsachen zur Annahme, dass die Maßnahme die notwendigen Informationen liefern wird
- Die bestimmten Tatsachen zur Annahme, dass sich die notwendigen Informationen in dem Account, Gerät etc. befinden
- Die Begründung zur notwendigen Einschränkung, dass die Maßnahme nicht mehr Informationen als unbedingt erforderlich betrifft

8.2.2.2 Notfall ("Gefahr im Verzug")

Bei Fällen der "Gefahr im Verzug" sind typischerweise, um Zeit zu sparen, die üblichen Formvorschriften keine Voraussetzung zur Durchführung einer konkreten Maßnahme. Die Rechtsgrundlagen sollten aber vorsehen, dass dieses zunächst bestehende Dokumentationsdefizit so rasch wie möglich behoben wird und alle Meldungen nachgeliefert werden und in den Verfahrens- und Dokumentationsprozess des Regelfalls überführt werden. Zusätzlich erforderlich ist eine Begründung, die die ex-ante Annahme einer "Gefahr im Verzug" nachträglich rechtfertigt.

8.2.3 Rechtsschutz

8.2.3.1 Bewilligung einer Maßnahme

8.2.3.2 Nachprüfende Kontrolle

8.2.3.3 Information Betroffener

8.2.3.4 kommissarischer Rechtsschutz

Sollte bei einer Maßnahme die sofortige Information Betroffener nicht möglich sein, ohne den bewilligten Zweck der Maßnahme zu gefährden, ist dies zu Begründen und zu Dokumentieren. In solchen Fällen ist ein entsprechend qualifizierter kommissarischer Rechtsschutz, unabhängig von beantragender und bewilligender Instanz zu informieren und mit der Vertretung der Interessen der Betroffenen zu betrauen. Ein solcher kommissarischer Rechtsschutz muss die Kompetenz haben, in allen Stufen des Verfahrens, bereits ab der Bewilligung von Maßnahmen, wirksame Rechtsmittel zu ergreifen.
Für eine ausreichende personelle und sachliche Ausstattung des kommissarischen Rechtsschutzes ist unter Wahrung der Unabhängigkeit zu sorgen.

8.2.3.5 (nachträgliche) Beschwerde

Ungeachtet dessen, ob im Zuge der Maßnahme kommissarischer Rechtsschutz aktiviert wurde, müssen Betroffene die Möglichkeit haben, innerhalb angemessener Frist nach einer notwendigen Information über die Maßnahme selbst effektive Rechtsmittel ergreifen zu können.

8.2.3.6 Einsprüche und Rechtsmittel

Dem Nutzer, auf dessen Daten oder Kommunikation zugegriffen wird, muss ein Mechanismus zur Verfügung stehen, um Einsprüche und Rechtsmittel gegen Verletzungen zu erheben. Gesetzwidrig erlangte geschützte Informationen dürfen in keinem Verfahren verwendet werden (Beweisverwertungsverbote). Der Staat soll regelmäßig Statistiken über angefragte, bewilligte und durchgeführte Maßnahmen publizieren sowie darstellen, in welchen (und wie vielen) Fällen durchgeführte Maßnahmen im Zuge weiterer gerichtlicher Verfolgung maßgeblich waren und zu welchen Strafen diese Verfahren geführt haben. Diese Darstellungen sollen sowohl quantitativ wie auch qualitativ erfolgen.

8.2.4 Begründungspflichten

- bei Begehren der Behörde
- bei Genehmigung und Kontrolle
- bei Verwendung von Ergebnissen im Einzelfall
- Richterliche Kontrolle
- Bewilligungspflichten
- Bewilligende Autorität

- Bewilligung durch ein Gericht
- Vermeidung von Rollen- und Interessenskonflikten (z.B.: soll der Rechtsschutzbeauftragte beim BM.I die Maßnahmen nach dem PStSG genehmigen und gleichzeitig die Interessen des Betroffenen kommissarisch Vertreten)
- Unabhängig, unparteilich, kompetent
- Richter müssen ausgebildet und fachlich qualifiziert sein, um eine informierte Entscheidung treffen zu können und über technische, prozessrechtliche und andere notwendige Expertise verfügen

8.2.4.1 Angemessenheit des Begehrens

- Das Gericht soll nur bewilligen, wenn das Begehren alle genannten Anforderungen und Begründungspflichten erfüllt

8.2.4.2 Beweisstandards

- Das Gericht soll nur bewilligen, wenn die Maßnahme notwendig ist und wenn genügend sachliche Verbindungen zu den betroffenen Geräten, Datenbanken bestehen
- Es muss sich dabei um das gelindeste Mittel handeln
- Die Beweislast liegt bei der ansuchenden Stelle

8.2.4.3 Form und Inhalt der Bewilligung

Anträge und Bewilligungen bedürfen der Schriftform. Die Bewilligung enthält:

- Name des Gerichts, Richters und Datum
- Gesetzliche Grundlage
- Geltungsbereich und Dauer der bewilligten Maßnahme
- Bezeichnung des zugrundeliegenden Begehrens
- Schriftliche Stellungnahme

8.2.4.4 Gerichtliche Aufsicht

- Es ist die Pflicht des Gerichts, die bewilligte Maßnahme zu überwachen
- Der Genehmigende muss sicherstellen, dass die ausführenden Organe über die durchgeführte Maßnahme berichten

8.2.4.5 Ermittlungsprozess

- Der genehmigende Richter soll die Ermittlungsergebnisse und die begleitende Dokumentation sichern
- Der Richter hat die Autorität, ermittelnde Behörden zu beschränken und im Falle eines Missbrauchs auch entsprechende Konsequenzen einzuleiten
- Wenn Ermittlungen nicht innerhalb einer angemessenen Zeit in ein Verfahren münden, ist eine Prüfung der bisherigen Ermittlungsarbeit in einem eigenständigen Verfahren durchzuführen

8.2.4.6 Notfallprozess ("Gefahr im Verzug")

- Das Gericht entscheidet darüber, ob aus Sicht ex ante zulässigerweise ein Notfall angenommen werden durfte
- Das Gericht stellt sicher, dass innerhalb einer angemessenen Frist das schriftliche Begehren nachträglich gestellt wird
- Das Gericht prüft die Benachrichtigung und das Begehren auf ihre Gültigkeit, Notwendigkeit und Angemessenheit

8.2.5 Beweisverwertungsgrenzen

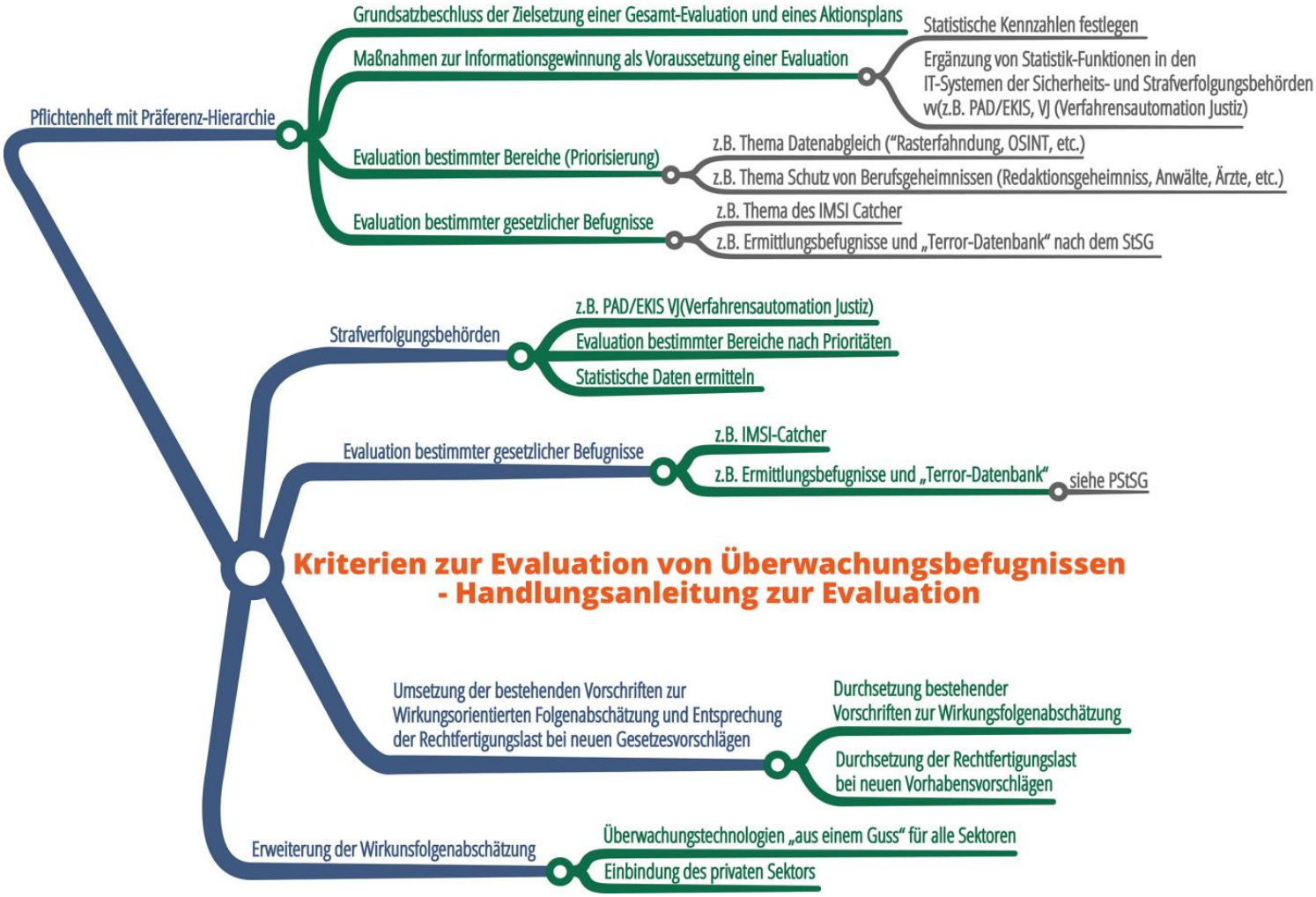
Bei Ermittlungen, die Grundrechtseingriffe erfordern, sollte aus rechtspolitischen Überlegungen ein Beweisverwertungsverbot für Zufallsfunde ("Beifang") zumindest ab einer gewissen Schwelle vorgesehen werden. Dadurch wird die Verwendung von Ermittlungsergebnissen für Zwecke, die im Sinne der Verhältnismäßigkeit den Grundrechtseingriff für sich genommen nicht rechtfertigen, zumindest erschwert.
Besonderes Augenmerk bedarf die Frage der Verwertung rechtswidrig erlangter Beweismittel, vor allem im Zusammenhang mit der Umgehung gesetzlich anerkannter Verschwiegenheitspflichten. Bestehende Verwertungsverbote im Rahmen der Nichtigkeitsbeschwerde nach § 281 StPO gehen in der Praxis häufig ins Leere, weil es sich nur um "relative Nichtigkeitsgründe" handelt, das heißt eine Nichtigkeit liegt nur dann vor, wenn ohne das Beweismittel das Verfahren zu einem anderen Ergebnis gelangen würde. Das ist jedoch nicht der Fall, wenn die rechtswidrig erlangten Beweise nur ein Anstoß für weitere Ermittlungen waren, am Ende jedoch nicht direkt Eingang in die Urteilsbegründung gefunden haben. In dieser Konstellation würde sogar das rechtswidrige Abhören des Rechtsanwalts des Angeklagten ohne Konsequenzen bleiben.

Die Problemstellungen im Zusammenhang mit Beweiserhebungs- und Beweisverwertungsverboten sind aber insgesamt äußerst komplex und nicht trivial aus einzelnen Grundrechten ableitbar. In dieser Hinsicht wäre ein offener rechtspolitischer Diskurs zu diesem Thema äußerst wünschenswert.

8.2.6 Kooperation mit dem Ausland / mit internationalen Systemen

- Wie wird die Einhaltung nationaler / europäischer Schutzvorschriften gewährleistet
- Ist bei Überschreitung ein Verfahren vor einem ordentlichen Gericht gewährleistet?
- Wie wird der Betroffene informiert?
- Ist Rechtsschutz für Betroffene gewährleistet?

9 Handlungsanleitung zur Evaluation



9.1 Pflichtenheft mit Präferenz-Hierarchie

9.1.1 Grundsatzbeschluss der Zielsetzung einer Gesamt-Evaluation und eines Aktionsplans

EU Policy Brief aus dem Projekt RESPECT:
"To select which type of surveillance system to set up, it is recommended to have the surveillance objectives more specifically determined via a mandatory security analysis which would also include a zero-point evaluation. The zero-point evaluation will provide baseline data for future evaluations." Danach wird ein verpflichtendes Privacy Impact Assessment (PIA) des ausgewählten Überwachungssystems vorgeschlagen. Um die dabei identifizierten Risiken zu entschärfen wird der Einsatz von Privacy-enhancing Technologies (PETs) empfohlen.

9.1.2 Maßnahmen zur Informationsgewinnung als Voraussetzung einer Evaluation

Vor allem die Beantwortung der im Rahmen des Projekts ausgearbeiteten parlamentarischen Anfragen zeigt, dass die Bundesregierung an vielen wichtigen Stellen offenbar nicht über die Informationen verfügt, welche die Voraussetzung für eine ordentliche Evaluation eines bestimmten Bereichs sind. Beispielsweise kann das Justizministerium nicht unterscheiden, welche der verschiedenen Ermittlungsmaßnahmen im Rahmen des § 135 StPO (Funkzellenabfrage, Inhaltsüberwachung, Verkehrsdatenauskunft) wie oft zur Anwendung gelangt ist, sondern nur wie oft insgesamt eine Maßnahme angeordnet wurde. Die Unterscheidung ist insofern wichtig, als es sich um völlig unterschiedliche Ermittlungsmaßnahmen mit unterschiedlichem Informationsgehalt und auch unterschiedlichen Risiken handelt.

HEAT bietet hierzu nachfolgend einige Vorschläge ohne Anspruch auf Vollständigkeit.

9.1.3 Statistische Kennzahlen festlegen

- Festlegung von Prioritäten
  - z.B. "Datenabgleich" (Rasterfahndung, OSINT, ...)
  - z.B. Schutz von Berufsgeheimnisträgern (Redaktionsgeheimnis, Anwälte, Ärzte, Seelsorge, ...)
  - z.B. Umsetzung der Statistik-Funktion in der Durchlaufstelle gemäß der Datensicherheitsverordnung zum TKG

9.1.4 Evaluation bestimmter Bereiche (Priorisierung)

Unabhängig von einer Gesamtevaluation bestehen bestimmte Themenfelder, die aufgrund besonderer Umstände und Entwicklungen dringend evaluiert werden sollten.

9.1.4.1 Telekommunikationsgesetz (TKG 2003) und Durchlaufstelle (DLS:):

Unabhängig von einer Gesamtevaluation bestehen bestimmte Themenfelder, die aufgrund besonderer Umstände und Entwicklungen dringend evaluiert werden sollten.

1. Telekommunikationsgesetz (TKG) und Durchlaufstelle (DLS) – Auskunftspflichten der TK-Anbieter

Eine Evaluation des Bereichs Telekommunikation im Hinblick auf Auskunftspflichten gegenüber Sicherheits- und Strafverfolgungsbehörden ist indiziert, seit der Verfassungsgerichtshof im Juni 2014 die Vorratsdatenspeicherung (VDS) aufgehoben hat. Mit dieser Entscheidung wurden grundsätzlich alle Bestimmungen aus dem TKG entfernt, die auf die VDS bezogen waren, allerdings hatte der VfGH bewusst die Bestimmungen zur Datensicherheit in § 102c TKG nicht aufgehoben, obwohl sich dort noch immer der Terminus „Vorratsdaten“ befindet, der aber ansonsten keine Bedeutung mehr hat.

Konsequent dazu ist auch die Datensicherheitsverordnung zum TKG (TKG-DSVO)[251] weiterhin unverändert in Kraft, deren Rechtsgrundlagen in § 102c TKG sowie § 94 TKG sind. Die DSVO und die dadurch eingerichtete Durchlaufstelle (DLS) zur sicheren Abwicklung der Auskunftsvorgänge wurden zwar ausdrücklich auch für den Bereich der Betriebsdaten geschaffen, aber die Vorschriften im Zusammenhang mit Vorratsdaten bestehen auch dort unverändert weiter.

Die Evaluation dieses Bereichs ist aber nicht nur aufgrund der überfälligen Rechtsbereinigung nach Aufhebung der VDS indiziert. Ein zentraler Bestandteil des TKG Datenschutzkonzepts liegt im Anspruch auf Rechtssicherheit und Transparenz. Genau deshalb enthält § 99 Abs. 1 TKG die Formulierung, dass Verkehrsdaten „außer in den **in diesem Gesetz** geregelten Fällen nicht gespeichert oder übermittelt werden“ dürfen. Dem entsprechend enthält § 99 Abs. 5 TKG in der Folge eine abschließende Aufzählung der korrespondierenden Rechtsnormen in der StPO und im SPG sowie neuerdings auch im PStSG, die dem Anbieter eine Auskunftspflicht auferlegen. Dieser **abschließende Katalog zulässiger Fälle der Datenverwendung** wurde – im Zuge der nationalen VDS-Umsetzung – mit der TKG Novelle 2011[252] eingeführt, begleitet durch die Einführung TKG-DSVO und die Einrichtung der DLS als exklusivem Kanal zur Abwicklung der Auskünfte. Die Erläuterungen zu § 99 Abs. 1 TKG weisen ausdrücklich darauf hin, dass hier dem datenschutzrechtlichen Transparenzgebot Rechnung getragen wird. „Eine Nachschau im TKG muss dem Anbieter Rechtsklarheit bieten, welche Datenverwendungen zulässig sind.“[253] Der Oberste Gerichtshof[254] hat schon 2012 unter Berufung auf diese Rechtslage solche Auskunftsansprüche abgelehnt, die in § 99 Abs. 5 nicht ausdrücklich aufgezählt sind, selbst wenn ein anderes Gesetz einen Auskunftsanspruch normiert wie z.B.: in § 87b Urheberrechtsgesetz.[255]

Nun hat der Gesetzgeber allein in den Jahren 2015 und 2016 zwei neue Rechtsgrundlagen zur Auskunftserteilung über Verkehrsdaten außerhalb der StPO oder des SPG geschaffen, dabei aber die Systematik des § 99 TKG ignoriert und dort keine entsprechende Ergänzung normiert. Der mit dem Steuerreformgesetz 2015/2016[256] neu eingeführte § 99 Abs. 3a FinStrG enthält einen Auskunftsanspruch zu Verkehrsdaten und einen Verweis auf § 99 Abs. 5 TKG, im TKG selbst wurde aber keine korrespondierende Norm geschaffen.

---

[251] Verordnung der Bundesministerin für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO) StF: BGBl. II Nr. 402/2011

[252] Kundgemacht am 18. Mai 2011 durch BGBl. I Nr. 27/2011.

[253] Erläuterungen zu § 99 Abs. 1 TKG, 1074 der Beilagen, XXIV. GP.

[254] OGH 6 Ob 119/11k auch mit Verweis auf die Materialien zur TKG Novelle.

[255] Vgl. dazu OGH 4 Ob 41/09x, wo der OGH schon vor der Novellierung mit guten Gründen den zivilrechtlichen Auskunftsanspruch wegen Urheberrechtsverletzungen ablehnt. Die Entscheidung 6 Ob 119/11k schließt sich dieser Entscheidung ausdrücklich an und argumentiert die neue Rechtslage.

[256] Steuerreformgesetz 2015/2016, BGBl. I Nr. 118/2015.

Weiters ist am 1.8.2016 § 48b BörseG neu in Kraft getreten[257]. Die Bestimmung gewährt der Finanzmarktaufsicht (FMA) eine Auskunft über Daten einer Nachrichtenübermittlung (§ 134 Z2 StPO einschließlich der in § 76a StPO genannten Daten, also Verkehrs-, Zugangs-, Standort- und Stammdaten), wenn der begründete Verdacht einer Zuwiderhandlung gegen § 48c BörseG (Missbrauchs von Insiderinformationen und Marktmanipulation) oder § 48d Abs. 1 Z2 BörseG (Verstoß gegen die Verpflichtungen zur Veröffentlichung von Insiderinformationen und daran anknüpfende Verpflichtungen) besteht. Das Landesgericht für Strafsachen Wien entscheidet als Einzelrichter mit Beschluss über einen entsprechenden Antrag der FMA. **Das Börsegesetz enthält weder einen Verweis auf das TKG noch wurde eine Anpassung im TKG selbst vorgenommen**. Anders als § 99 Abs. 3b FinStrG ist im Börsegesetz auch **keine Regelung enthalten, wonach die DLS als Kommunikationskanal für Auskünfte exklusiv vorzusehen ist**. Neben diesen Unterlassungen ist diese neue gesetzliche Grundlage auch sonst vielfach kritikwürdig. Die Finanzmarkaufsicht soll unter sinngemäßer Anwendung der Bestimmungen der StPO den Anspruch durchsetzen und es ist völlig unklar, welches Verfahrensrecht gelten soll, wenn der Anbieter die Auskunft verweigert oder nicht erteilen kann. Die FMA ist eine Verwaltungsbehörde und § 48b BörseG normiert einen Verwaltungsstraftatbestand und keine gerichtliche Strafnorm. Gerichtliche Beugemaßnahmen nach der StPO zu verhängen wäre daher eine klare Verletzung der Gewaltenteilung.

An dieser Stelle schließlich noch eine Bemerkung zur Verhältnismäßigkeit: Der Strafverfolgung stehen Auskünfte über Daten einer Nachrichtenübermittlung erst ab einer Mindeststrafdrohung von einem Jahr Freiheitsstrafe zu. Die Ausweitung dieser Ermittlungsbefugnisse auf das Verwaltungsstrafrecht, wo höchstens Geldstrafen drohen, stellt einen Dammbruch dar und setzt die bisherige Schwelle empfindlich herab.

Kommunikationssysteme nach dem TKG betreffen praktisch die gesamte Bevölkerung unmittelbar und Eingriffe in das Kommunikationsgeheimnis haben die denkbar größte Streubreite. Allein die hier bereits sichtbar gemachten Beispiele zeigen, dass eine Evaluation dieses Bereichs von höchster Dringlichkeit ist.

9.1.4.2 Schutz von Berufsgeheimnisträgern (Redaktionsgeheimnis, Anwälte, Ärzte etc.)

Besondere Bedeutung kommt dem Schutz gesetzlicher Verschwiegenheitsverpflichtungen bzw. gesetzlich anerkannter Berufsgeheimnisse zu. Viele der beschriebenen Überwachungsbefugnisse, insbesondere im Zusammenhang mit elektronischer Kommunikation, sind potentiell geeignet, den grundsätzlich in der

[257] Bundesgesetz über die Wertpapier- und allgemeinen Warenbörsen und über die Abänderung des Börsesensale-Gesetzes 1949 und der Börsegesetz-Novelle 1903 (Börsegesetz 1989 - BörseG) BGBl. I. Nr. 555/1989 idF BGBl. I Nr. 76/2016.

Rechtsordnung verankerten Schutz dieser Geheimnissphären zu umgehen. Dieses Problem ist nicht neu, wird aber mit jeder Erweiterung der Überwachungsbefugnisse – z.B.: dem Polizeilichen Staatsschutzgesetz – potenziert. Es ist daher dringend geboten, diesen Bereich gezielt zu evaluieren und neue Ansätze zu finden, die das Vertrauen der Menschen in solche gesellschaftlich bedeutsamen Geheimnissphären rechtfertigen bzw. wiederherstellen können. Siehe dazu im Detail insbesondere Kapitel 5.1.6.1.

9.1.4.3 Automatisierter Datenabgleich („Rasterfahndung", OSINT, etc.)

Als dritte Priorität für dringend notwendige Bereichsevaluationen wurde im Rahmen von HEAT der Themenkreis „Automatisierter Datenabgleich" identifiziert. Hierzu ist vor allem zu berücksichtigen, dass sich die technologischen Möglichkeiten seit der Einführung der „Rasterfahndung" (siehe insbesondere § 141 StPO) Ende der 1990er Jahre enorm weiterentwickelt haben. Aus damaliger Sicht wären wohl allein die Möglichkeiten, die ein Dienst wie die „Google Suche" heute bietet, eine nahezu übermächtige „Super-Rasterfahndung" gewesen. Heute wird nicht einmal entfernt daran gedacht, eine Google Suche im Rahmen von Ermittlungsmaßnahmen als automatisierten Datenabgleich im gesetzlich geregelten Sinne zu verstehen. Weit darüber hinaus gehen dem gegenüber die Möglichkeiten, welche die Technologien rund um die sog. „Open Source Intelligence" (OSINT) eröffnen – siehe dazu im Detail Kapitel 4.2. Es ist daher dringend nach dem aktuellen Stand der Technik zu evaluieren, was heutzutage alles unter den Begriff des „automatisierten Datenabgleichs" fällt und wo die Grenzen verlaufen.

9.1.5 Evaluation bestimmter gesetzlicher Befugnisse

Nach der Festlegung des sachlichen Bereichs für eine Evaluation ist zu identifizieren, welche Rechtsnormen für den jeweiligen Bereich relevant sind und welche Rechtsgrundlagen konkret in die Evaluation einzubeziehen sind.

9.2 Strafverfolgungsbehörden

9.2.1 z.B. PAD[258]/EKIS[259], VJ (Verfahrensautomation Justiz)

Ergänzung von Statistik-Funktionen in den IT-Systemen der Sicherheits- und Strafverfolgungsbehörden.

9.2.2 Evaluation bestimmter Bereiche nach Prioritäten

9.2.3 Statistische Daten ermitteln

9.3 Evaluation bestimmter gesetzlicher Befugnisse

z.B. Rechtsgrundlage zum Einsatz des IMSI Catchers (§ 53 Abs. 3b SPG)

[258] IT-Anwendung „Protokollieren-Anzeigen-Daten".
[259] Elektronisches Kriminalpolizeiliches Informationssystem.

z.B. Ermittlungsbefugnisse und "Terror-Datenbank"[260] nach dem PStSG

9.4 Umsetzung der bestehenden Vorschriften zur Wirkungsorientierten Folgenabschätzung und Entsprechung der Rechtfertigungslast bei neuen Gesetzesvorschlägen

RESPECT: Zur Erhöhung der Transparenz und Verantwortlichkeit sollen Überwachungssysteme – vor ihrer Entwicklung sowie nach Inbetriebnahme regelmäßig – von unabhängigen Dritten evaluiert werden. Diese Evaluationen sollten wiederum von einer staatlichen Datenschutz- oder Überwachungsbehörde evaluiert werden. Die Evaluation soll

- operationale
- organisatorische
- technische

Aspekte umfassen. Auf EU-Ebene sollten klare Leitlinien und Methoden für solche Evaluationen entwickelt und umgesetzt werden, insbesondere zur Bewertung der sozialen und wirtschaftlichen Kosten der Überwachungsmaßnahmen und -systeme.

9.4.1 Durchsetzung bestehender Vorschriften zur Wirkungsfolgenabschätzung

Ein rechtlicher Rahmen für den Einsatz von Überwachungstechnologien „aus einem Guss“ für alle Sektoren wird gefordert.

9.4.2 Durchsetzung der Rechtfertigungslast bei neuen Vorhabensvorschlägen

9.5 Erweiterung der Wirkungsfolgenabschätzung

9.5.1 Überwachungstechnologien „aus einem Guss“ für alle Sektoren

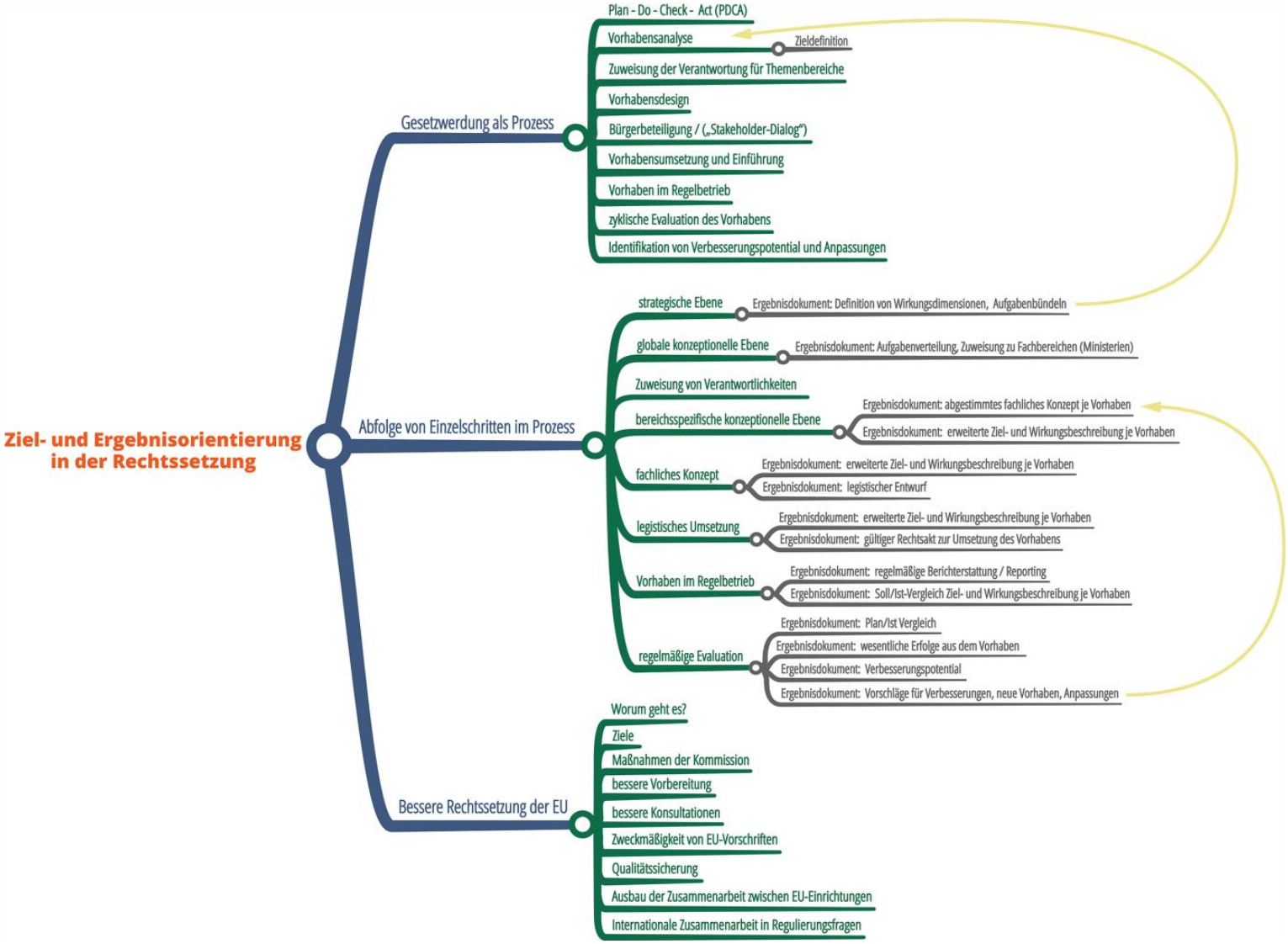
Ein rechtlicher Rahmen für den Einsatz von Überwachungstechnologien „aus einem Guss“ für alle Sektoren wird gefordert.

9.5.2 Einbindung des privaten Sektors

Der private Sektor soll ermutigt werden, Systeme zu entwickeln, die Individuen [Ergänzung: ihre Privatsphäre] und ihre personenbezogenen Daten schützen. Datenschutzbehörden sollen die Schaffung eines effektiven Verfahrens für ein PIA unterstützen, das während der Entwicklungsphase angewandt wird.

[260] § 12 PStSG.

10 Ziel- und Ergebnisorientierung in der Rechtssetzung



Rechtsetzung ist kein Selbstzweck

Jedes einzelne Vorhaben ist (sollte sein) Teil einer politischen Strategie zur Weiterentwicklung eines gedeihlichen Zusammenwirkens aller Kräfte der Republik.
Vorhaben und Maßnahmen dienen der Weiterentwicklung der Gesellschaft.
Jedes einzelne Vorhaben und jede einzelne Maßnahme muss daher einem gesamtgesellschaftlichen Wertekatalog zugeordnet werden können.
So wie das menschliche Leben nicht konfliktfrei sein kann, sind auch gesellschaftliche Werte nicht frei von Widersprüchen und notwendigen Abwägungen.
Im praktischen Leben finden sich diese strategischen Vorgaben für Österreich in Regierungsübereinkommen und Regierungserklärungen.
Aus österreichischer Sicht werden (sollten?) beabsichtigte Weiterentwicklungen in den jährlichen "aktuellen Wirkungszielen" in überschaubare Einzelschritte heruntergebrochen.

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 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 Umsetzung, Anwendung, Evaluierung und Anpassung durchgängig zu gestalten ist (Plan - Do- Check - Act, PDCA, siehe dort).
Zahlreiche Ansätze und Einzelmaßnahmen wurden in den letzten Jahren gesetzt, um den Gesetzwerdungsprozess qualitativ zu verbessern, methodische und technologische Unterstützung zu bieten. Hier ist insbesondere auf die Wirkungsfolgen-Grundsatzverordnung oder e-Recht verwiesen, die dabei wichtige Beiträge liefern. Diese beiden Initiativen setzen im Gesamtprozess jedoch sehr spät auf. Versäumnisse aus frühen Phasen der einzelnen Vorhaben können hierbei nur in geringem Umfang und mit unnötig großem Aufwand ausgeglichen werden.

Ein Beispiel:

Wenn die Anforderungen der WFA-GV nach Zieldefinition und Problembeschreibung erst im Rahmen der legistischen Umsetzung, als Vorbereitung des Begutachtungsprozesses, erarbeitet werden, sind zahlreiche Informationen aus Vorphasen nicht verfügbar. 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 in diesem Abschnitt einen möglichen, groben Rahmen für die Gestaltung von Vorhaben zur Gesetzwerdung vor.
- Begleitend zur Anregung geben wir einen Überblick über die Maßnahmen für "Bessere Rechtssetzung der EU"

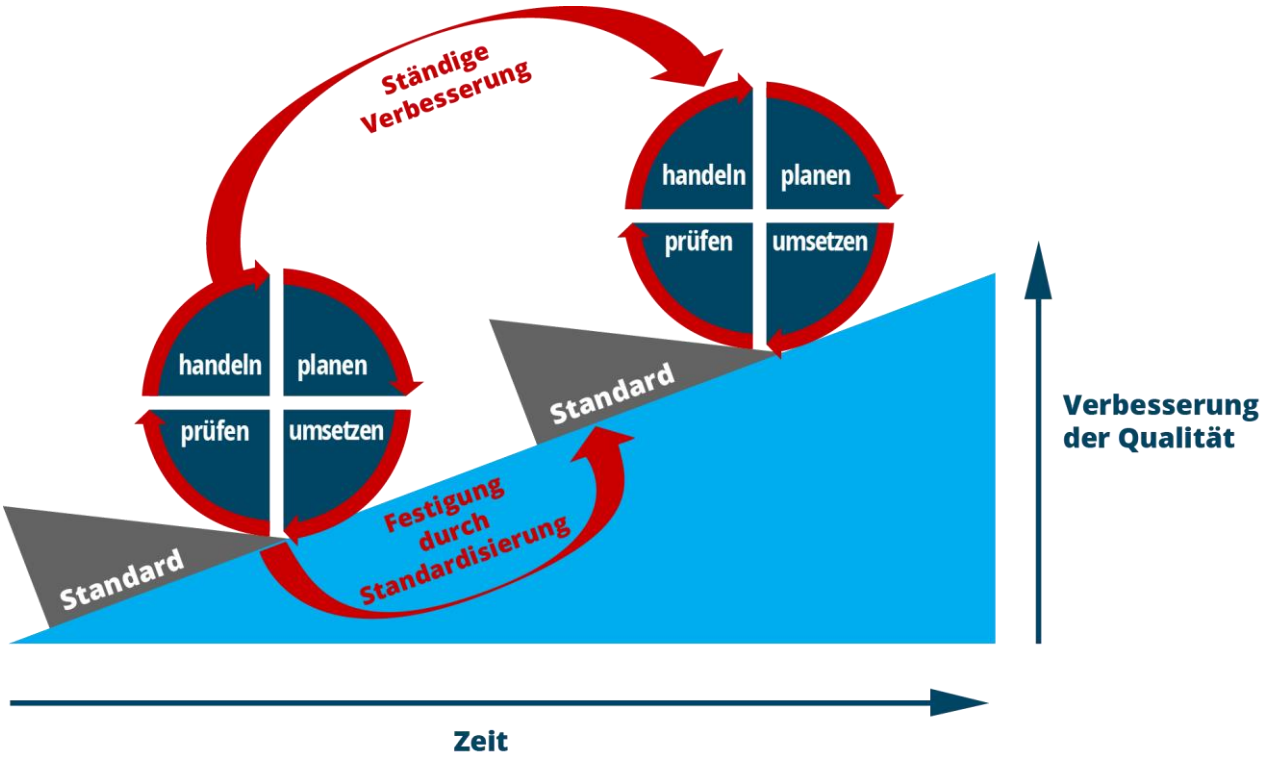
10.1 Gesetzwerdung als Prozess

Abgeleitet aus politischer Gesamtstrategie und den eingemeldeten Anforderungen von Interessensträgern ("stake-holder") 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 (zumeist Verantwortliche in Ministerien) zu übergeben.

10.1.1 Plan - Do -Check - Act (PDCA)

PDCA ist eine Sichtweise auf kontinuierliche Weiterentwicklung, die die zyklische Abfolge von einzelnen Entwicklungsvorhaben zeigt.
Diese Sichtweise, ursprünglich aus der Qualitätssicherung, wird heute allgemein auf Entwicklungs- und Verbesserungsprozesse angewandt.
Diese prozesshafte Weiterentwicklung gilt – unabhängig ob sie als solche wahrgenommen und angewandt wird – für jede Art der Weiterentwicklung, die nicht zu einem Stillstand führt.

Daher ist es sinnvoll, dieses zyklische Vorgehen jedem Entwicklungsprozess zu Grunde zu legen.



[261]

[261] Die englischsprachige Vorlage für diese Grafik ist auf Wikimedia zu finden: https://upload.wikimedia.org/wikipedia/commons/a/a8/PDCA_Process.png .

10.1.2 Vorhabensanalyse

Jedes Vorhaben ist mit Problembeschreibung, Zielsetzung, Priorität, Grobschätzung des erwartetet Umsetzungs- und Betriebsaufwandes als Teil des Gesamtportfolios zu dokumentieren.

10.1.3 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 keine konkrete Zielvorgabe oder –Vorstellung 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.

Beispiel SMART-Analyse:
Eine praxisbewährte Methode zur Zielfindung ist die SMART-Analyse. Die Reduktion auf fünf wesentliche Kriterien trägt dazu bei, überschaubare und dennoch hinreichend genaue Zieldefinitionen zu erstellen. Diese Methode kann auch als Controlling-tool eingesetzt werden, um die Zieldefinition abschließend zu überdenken: Sind die Zielangaben…

S= spezifisch (eindeutig und konkret)
M= messbar
A= angemessen (Erreichbarkeit /Ressourcen)
R= realistisch und relevant (und ergeben daher einen Mehrwert?)
T= terminierbar (gibt es einen Start- und einen End-Termin?)

Ist die Zieldefinition gefunden, formuliert und dokumentiert sollte sie final an die Entscheidungsträger kommuniziert werden. Alle Informationen sollten detailliert abgestimmt werden, so dass die Freigabe gesetzt und der Startschuss für das Vorhaben erfolgen kann.[262]

[262] Siehe z.B. 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/ .

10.1.4 Zuweisung der Verantwortung für Themenbereiche

Aus dem Gesamtportfolio werden Vorhabensbündel und Einzelvorhaben den adäquaten Verantwortungsträgern (zumeist innerhalb der Hierarchie der jeweiligen Fachministerien) zugewiesen.

10.1.5 Vorhabensdesign

Im Rahmen der Themenverantwortlichkeit wird ein Verantwortlicher je einzelnem Vorhaben festgelegt.
Dieser Vorhabensverantwortliche ist mit der nötigen sachlichen und fachlichen Kompetenz zur Umsetzung des Vorhabens auszustatten.
Diese Vorhabensverantwortlichen begleiten die ihnen zugewiesenen Vorhaben bis zur Umsetzung und sichern dabei Kontinuität und Vollständigkeit der Dokumentation für den gesamten Vorhabensablauf.
Im Rahmen der zugewiesenen Verantwortung entwickelt der Vorhabensverantwortliche 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.

10.1.6 Bürgerbeteiligung / ("Stakeholder-Dialog")

Möglichst frühzeitig, jedenfalls unmittelbar nach Vorliegen eines ersten Konzepts zur Vorhabensumsetzung, sind alle beteiligten oder möglicherweise betroffenen Interessensträger zu identifizieren und zur Abstimmung der weiteren Umsetzungsschritte beizuziehen.
Das Ergebnis dieser Abstimmung - inklusive von nicht ausgeräumten Bedenken von Interessensträgern ist zu dokumentieren.
Dieses Dokument ist nach Qualitätssicherung durch die zuständige vorgesetzte Instanz freizugeben und gilt als Basis für die nächsten Vorhabensschritte.

10.1.7 Vorhabensumsetzung und Einführung

Aus dem Vorhabensdesign und dem Ergebnis der Abstimmung mit den Interessensträgern werden das Vorhaben und die notwendigen Elemente weiterentwickelt und umgesetzt.
Hierzu gehören die notwendigen Schritte im parlamentarischen Verfahren - Begutachtung, Nachbesserung, Abstimmung.

10.1.8 Vorhaben im 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.

10.1.9 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.

10.1.10 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 Auswirkungen des Vorhabens außerhalb des ursprünglichen Zielbereichs einzufließen.
Aus dieser Beurteilung sind mögliche Verbesserungsvorschläge, sinnvolle Änderungen oder der Bedarf von zusätzlichen Vorhaben abzuleiten und in das Portfolio einzumelden.

10.2 Abfolge von Einzelschritten im Prozess

10.2.1 strategische Ebene

Aus der Gesamtstrategie sind einzelne umsetzungsrelevante Themen- und Vorhabensbündel abzuleiten, grob inhaltlich zu beschreiben, gegeneinander abzugrenzen und zu dokumentieren.

10.2.1.1 Ergebnisdokument: Definition von Wirkungsdimensionen Aufgabenbündeln

10.2.2 global konzeptionelle Ebene

Aus dem Aufgabenportfolio sind themen- und fachspezifische Zuordnungen entsprechend der allgemeinen Aufgabenzuordnung (Bundesministeriengesetz) von Verantwortung für die Umsetzung abzuleiten.

10.2.2.1 Ergebnisdokument: Aufgabenverteilung, Zuweisung zu Fachbereichen (Ministerien)

10.2.3 Zuweisung von Verantwortlichkeiten

Aus dem daraus entstehenden Portfolio sind Vorhabensbündel entsprechend der Aufgabenverteilung den Verantwortlichen zuzuweisen.

Ergebnisdokument: Katalog von Vorhaben und verantwortlichen Personen: Die Verantwortung von Aufgaben und Aufgabenbündel sind innerhalb der Verantwortungsbereiche (zumeist Ministerien) konkreten Personen für die weitere Gestaltung der Vorhaben zuzuweisen.

10.2.4 bereichsspezifische konzeptionelle Ebene

In der bereichsspezifisch zugeordneten Verantwortung sind die Vorhaben konzeptuell auszuarbeiten und mit den beteiligten oder betroffenen Interessensträgern ("stake-holder") abzustimmen.

10.2.4.1 Ergebnisdokument: abgestimmtes fachliches Konzept je Vorhaben

10.2.4.2 Ergebnisdokument: erweiterte Ziel- und Wirkungsbeschreibung je Vorhaben

In diesem Bearbeitungsschritt wird die Ziel- und Wirkungsbeschreibung erweitert und mit den Interessensträgern abgestimmt.
Kriterien für die Evaluation werden überprüft, erweitert und mit den Interessensträgern abgestimmt.

10.2.5 fachliches Konzept

Das fachliche Konzept wird bis zur Umsetzungsreife (Vorlage an die für die Freigabe zur weiteren Bearbeitung zuständige Instanz, z.B. Ministerrat) weiterentwickelt.

10.2.5.1 Ergebnisdokument: erweiterte Ziel- und Wirkungsbeschreibung je Vorhaben

In diesem Bearbeitungsschritt wird die Ziel- und Wirkungsbeschreibung erweitert und mit den Interessensträgern abgestimmt.
Die Kriterien für die Evaluation werden ergänzt.

10.2.5.2 Ergebnisdokument: legistischer Entwurf

10.2.6 legistische Umsetzung

Hier findet die tatsächliche Freigabe zur Umsetzung statt: Begutachtung, parlamentarische Diskussion, Gesetzesbeschluss; Ausfertigung einer Verordnung; Kundmachung, Dienstanweisung ...).

10.2.7 Ergebnisdokument: erweiterte Ziel- und Wirkungsbeschreibung je Vorhaben

In diesem Bearbeitungsschritt wird die Ziel- und Wirkungsbeschreibung erweitert und mit den Interessensträgern abgestimmt.
Die Kriterien für die Evaluation werden ergänzt.

10.2.7.1 Ergebnisdokument: gültiger Rechtsakt zur Umsetzung des Vorhabens

Gesetzesbeschluss; Verordnung; Kundmachung, Dienstanweisung …

10.2.8 Vorhaben im Regelbetrieb

10.2.8.1 Ergebnisdokument: regelmäßige Berichterstattung / Reporting

10.2.8.2 Ergebnisdokument: Soll/Ist-Vergleich Ziel- und Wirkungsbeschreibung je Vorhaben

Informationen entsprechend der Ziel- und Wirkungsbeschreibung und den Vorgaben zur Evaluation sind aufzubereiten und zu veröffentlichen.

10.2.9 regelmäßige Evaluation

10.2.9.1 Ergebnisdokument: Plan/Ist Vergleich

10.2.9.2 Ergebnisdokument: wesentliche Erfolge aus dem Vorhaben

Abweichungen von den erwarteten / geplanten Ergebnissen sind zu erklären.
Dieses Ergebnisdokument muss gegebenenfalls positive und negative Auswirkung außerhalb des ursprünglichen Zielbereichs dokumentieren.

10.2.9.3 Ergebnisdokument: Verbesserungspotential

Aus Plan/Ist-Vergleich und Erfolgsdokumentation sind mögliche Verbesserungen abzuleiten und zu dokumentieren.

10.2.9.4 Ergebnisdokument: Vorschläge für Verbesserungen, neue Vorhaben, Anpassungen

Diese Ergebnisse sind in die strategische Portfolioverwaltung einzumelden.

10.3 Bessere Rechtssetzung der EU

Im Rahmen der Agenda für bessere Rechtsetzung wird bei der Erarbeitung und Bewertung von Rechtsvorschriften und Strategien der EU Wert auf Transparenz, solide Fakten und die Meinung von Öffentlichkeit und Interessenträgern gelegt. Die Agenda erstreckt sich auf alle Politikbereiche und soll für eine gezielte Regulierung sorgen, die nicht weiter geht als erforderlich und bei möglichst geringem Kostenaufwand die gewünschten Ziele erreicht.
Better regulation for better results - an EU Agenda Proposal for an inter-institutional agreement on better regulation

10.3.1 Worum geht es?

Um bessere Ergebnisse zu erzielen, öffnet die Kommission Politikgestaltung und Rechtsetzung und verschafft den Menschen, die davon betroffen sind, mehr Gehör. Bessere Rechtsetzung stützt sich auf Fakten und einen transparenten Prozess, der

Bürger/-innen und Interessenträger (z. B. Unternehmen, öffentliche Verwaltungen und Wissenschaftskreise) im gesamten Verlauf einbezieht.
Die Kommission ermittelt die Bereiche, in denen bestehende EU-Rechtsvorschriften verbessert werden können. Wenn sie neue Strategien und Rechtsvorschriften vorschlägt, konzentriert sie sich auf die Dinge, die tatsächlich auf EU-Ebene angegangen werden müssen, und sorgt für eine gute Umsetzung.
Diese Grundsätze sollen der Kommission helfen, ihre Ziele bei möglichst geringem Kosten- und Verwaltungsaufwand zu erreichen. Außerdem trägt sie damit Bedenken der EU-Bürger/-innen Rechnung.

10.3.2 Ziele

- offene und transparente Entscheidungsfindung
- Einbeziehung von Öffentlichkeit und Interessenträgern in den gesamten Prozess der Politikgestaltung und Rechtsetzung
- EU-Maßnahmen, die sich auf Fakten und eine Analyse der Auswirkungen stützen
- Minimierung des Verwaltungsaufwands für Unternehmen, Bürger/-innen oder öffentliche Verwaltungen

10.3.3 Maßnahmen der Kommission

10.3.4 bessere Vorbereitung

10.3.5 bessere Konsultationen

Die Kommission verbessert und erweitert die Möglichkeiten für Öffentlichkeit und Interessenträger, sich in den gesamten Prozess der Politikgestaltung und Rechtsetzung einzubringen. Interessierte Bürger/-innen und Interessenträger können sich äußern zu

- Fahrplänen und Folgenabschätzungen in der Anfangsphase, in denen die Kommission neue Ideen für Strategien und Rechtsvorschriften oder Bewertungen bestehender Strategien vorstellt,
- Elementen von Folgenabschätzungen, wenn die Kommission die möglichen wirtschaftlichen, sozialen und ökologischen Auswirkungen eines Vorschlags untersucht,
- Legislativvorschlägen, sobald sich die Kommission darauf geeinigt hat,
- Entwürfen von Rechtsakten, die Elemente bestehender Rechtsvorschriften ergänzen oder ändern (delegierte Rechtsakte) oder die Bedingungen für eine EU-weite einheitliche Anwendung von Rechtsvorschriften festlegen (Durchführungsrechtsakte) – Anmerkungen zu Durchführungs- oder delegierten Rechtsakten
- Elementen von Bewertungen und Eignungsprüfungen bestehender Strategien und Rechtsvorschriften,
- Ideen zur Verbesserung bestehender EU-Rechtsvorschriften.

10.3.6 Zweckmäßigkeit von EU-Vorschriften

Die Kommission bewertet die Leistung des bestehenden EU-Rechts und nimmt gegebenenfalls Änderungen vor, um Rechtsvorschriften auf den neuesten Stand zu bringen.

- Das Programm zur Gewährleistung der Effizienz und Leistungsfähigkeit der Rechtsetzung (REFIT) wurde 2012 ins Leben gerufen, um das EU-Recht zu vereinfachen und Regulierungskosten zu verringern, ohne den Nutzen zu beeinträchtigen. Die Kommission baut das REFIT-Programm aus, indem sie Interessenträgern und EU-Ländern mehr Möglichkeiten gibt, sich einzubringen.
- Die REFIT-Plattform, unter dem Vorsitz des Ersten Vizepräsidenten Frans Timmermans, sammelt Vorschläge und legt Empfehlungen zur Vereinfachung von Rechtsvorschriften vor.
- Informationen über den Stand von REFIT-Initiativen zur Vereinfachung und Reduzierung des Verwaltungsaufwands werden im REFIT-Anzeiger veröffentlicht.
- Mittels Bewertungen und Eignungsprüfungen wird überprüft, ob Rechtsvorschriften, Strategien und Förderprogramme der EU die erwarteten Ergebnisse bei möglichst geringem Kostenaufwand erzielen.

10.3.7 Qualitätssicherung

Für die Sicherung der Qualität hat die Kommission den Ausschuss für Regulierungskontrolle eingerichtet, eine unabhängige Gruppe von Kommissionsbeamten und externen Sachverständigen. Der Ausschuss überprüft die Qualität aller Folgenabschätzungen und umfangreichen Bewertungen, die in die Entscheidungsfindung der EU einfließen.
Für eine wirksame Umsetzung gemeinsamer Rechtsetzungsstandards orientieren sich die Kommissionsdienststellen im gesamten Prozess der Politikgestaltung und Rechtsetzung an den Leitlinien und dem Instrumentarium für eine bessere Rechtsetzung.

10.3.8 Ausbau der Zusammenarbeit zwischen EU-Einrichtungen

Der politische Wille zur Verbesserung der Qualität der Rechtsetzung sowie zur Überprüfung bestehender Rechtsvorschriften und, falls erforderlich deren Aktualisierung, wird von den drei wichtigsten EU-Organen geteilt: Parlament, Rat und Kommission. Eine entsprechende interinstitutionelle Vereinbarung über bessere Rechtsetzung ist im April 2016 in Kraft getreten.
Interinstitutionelle Vereinbarung über bessere Rechtsetzung

10.3.9 Internationale Zusammenarbeit in Regulierungsfragen

Durch Informationsaustausch und frühzeitige Zusammenarbeit können Regulierungsbehörden und zuständige Stellen Lösungen für ähnliche Probleme finden, unter Beibehaltung ihrer jeweiligen politischen Ziele und Standards. Dies verringert die Geschäftskosten und führt länderübergreifend zu mehr und fairerem Wettbewerb.
In Regulierungsfragen arbeitet die Kommission eng mit ihren Handelspartnern zusammen, sowohl im Rahmen multilateraler Dialoge (z. B. mit den **Vereinten Nationen**, der **OECD** und der **Weltbank**) als auch in bilateralen Gesprächen.
Die Zusammenarbeit in Regulierungsfragen ist inzwischen auch integraler Bestandteil bilateraler Freihandelsabkommen wie dem umfassenden Wirtschafts- und Handelsabkommen EU-Kanada (CETA) und Teil der laufenden Verhandlungen über die Transatlantische Handels- und Investitionspartnerschaft zwischen der EU und den USA (TTIP).

11 Abbildungsverzeichnis

12 Literaturverzeichnis

12.1 Publikationen

Albrecht, P. A. (2007). Das nach-präventive Strafrecht: Abschied vom Recht. Institut für Kriminalwissenschaften Frankfurt aM (ed.) Jenseits des rechtsstaatlichen Strafrechts. Frankfurt aM: Lang, 3-26.

Arendt, H. (2003). Was ist Politik? Piper.

Beckett, K. (1999). Making crime pay: Law and order in contemporary American politics. Oxford University Press.

Berka, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT, 2012, Band I/1.

Berka, Grundrechte, Rz 400 f.

BMJ/BMI Interministerielle Arbeitsgruppe „Online-Durchsuchung" Bericht, Endfassung vom 09.04.2008.

Böszörmenyi Janos/Schweighofer Erich, Tracking of Financial Movements, in: Erich Schweighofer/Franz Kummer/Walter Hötzendorfer (Hrsg.), Transparenz. Tagungsband des 17. Internationalen Rechtsinformatik Symposions IRIS 2014, books@ocg.at, Wien 2014, S. 617-624.

Damjanovic (u.a.), Handbuch des Telekommunikationsrechts (2006).

Depenheuer, Selbstbehauptung des Rechtsstaates, Schöningh, 2. Auflage (2008)

Dohr (u.a.), Art 1 § 1, DSG Kommentar, 20082,8.Er.-Lfg.

Edthaler/Schmid, Auskunft über IP-Adressen im Strafverfahren, MR 2008.

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.

Erläuterungen zum DSG 2000, EBRV 1613 BlgNR XX. GP, 35.

ErlRV 128 der Beilagen XXII. GP 17.

Eser/Hassemer (Hg.), Die deutsche Strafrechtswissenschaft vor der Jahrtausendwende, 2000.

EuGH C-293/12 und C-594/12, RN 42.

EuGH Rs C-314/12.

Europäische Kommission, Overview of information management in the area of freedom, security and justice, COM(2010)385 final.

European Data Protection Supervisor, Opinion 15/2015.

Fuchs, Verdeckte Ermittler – anonyme Zeugen, ÖJZ 2001, 495 [496 ff.].

Furedi, F. (2005). Politics of fear. A&C Black.

Gandy, O. H. (2012). a. Statistical surveillance. Remote sensing in the digital age. In: Ball, K. et al. (eds.): Routledge Handbook of Surveillance Studies. Routledge: London, New York.

BMI, Verfassung – Reform – Rechtsschutz.

Giddens, A. (2013). The consequences of modernity. John Wiley & Sons.

Grabenwarter, EMRK³, 161, Rz 3.

Grabenwarter, EMRK4, § 18 Rz 14, S. 116.

Grabenwarter, Europäische Menschenrechtskonvention, 4. Auflage.

Hasberger, Die providerinterne Auswertung von Verkehrsdaten und Datenschutz, MR 2010.

Hayes, B., Rowlands, M., & Buxton, N. (2009). Neoconopticon: The EU security-industrial complex (p. 5). Transnational institute.

Hegemann, H.; Kahl, M. (2016): Konstruktionen und Vorstellungen von Wirklichkeit in der Antiterror-Politik: Eine kritische Betrachtung In: Fischer, S.

Heißl, Recht auf Privatleben, in: Heißl (Hrsg.), Handbuch Menschenrechte.

Hiesel, Die Rechtsstaatsjudikatur des Verfassungsgerichtshofes, ÖJZ 1999,522 (Heft 14-15).

Holoubek, Grundrechtliche Gewährleistungspflichten.

HRRS (Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht), Ausgabe 3/2004.

IdF BGBl I 2013/195.

Jakobs, Kriminalisierung im Vorfeld einer Rechtsgutverletzung, ZStW 97,1985.

Kirchbacher, WK-StPO § 252 Rz 66 f.

Kopetzki, in Korinek/Holoubek (Hrsg), Art 1 PersFrG, Rz 17.

Kotschy, Datenschutzrechtliche Fragen im Zusammenhang mit dem neuen Verbraucherkreditrecht, ÖBA 2011.

Kreissl, R. (ed.): Surveillance in Europe., Routledge: London, New York.

Kreissl, R. et al. (2015): Surveillance. Preventing and detecting crime and terrorism. in: Wright, D.

Kunnert, "Tausche Visafreiheit gegen Datenschutz" - Die neue Polizeikooperation auf Basis des US-Österreichischen "Prüm-like"-Abkommens, Jahrbuch Datenschutzrecht und E-Government 2012.

Lachmayer, Die Wirkung von “Schengen“ nach innen – Polizeiliche Informationsnetzwerke ohne Grenzen? Juridikum 2009.

Lachmayer, Transnationales Polizeihandeln – Demokratische und rechtsstaatliche Herausforderungen der europäischen Polizeikooperation, JBl 2011.

Ladeur, Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?, DÖV 2009, Jg 62.

Lasch, C. (1995). Das Zeitalter des Narzißmus.

Laurer, Verfassungsänderungen 1988 (1989).

Lehner, Recht auf Datenschutz, in: Heißl (Hrsg.), Handbuch Menschenrechte.

Lyon, D. (2007): Surveillance Studies: An overview., Polity Press: Cambridge.

Marcel Alexander NIGGLI/Stefan MAEDER, Was schützt eigentlich Strafrecht (und schützt es überhaupt etwas, in: Mantscher/Pernthaler/Raffeiner (Hrsg.), Ein Leben für Recht und Gerechtigkeit, Festschrift für Hans R. Klecatsky zum 90. Geburtstag, nwV, 2010.

Masala, C. (Hg.): Innere Sicherheit nach 9/11. Sicherheitsbedrohungen und (immer) neue Sicherheitsmaßnahmen? Springer: Wiesbaden.

Mueller, J. E., & Stewart, M. G. (2015). Chasing ghosts: The policing of terrorism. Oxford University Press.

O'connor, J. (1979). The fiscal crisis of the state. Transaction Publishers.

ÖJZ 1999.

Peukert, in Frohwein/Peukert, EMRK.

Pinker, S. (2011). The better angels of our nature: The decline of violence in history and its causes. Penguin UK.

Probst, Bericht des Rechtsschutzbeauftragten nach § 57 MBG, in: BMI, Der Rechtsschutzbeauftragte.

Probst, Bericht über den Rechtsschutz nach §§ 22 und 57 MBG nach der Änderung des MBG 2004, in: BMI, Terror – Prävention – Rechtsschutz.

Probst, Die rechtlichen Positionen der Rechtsschutzbeauftragten.

Probst, Kompetenzen des Rechtsschutzbeauftragten nach MBG und Rechtsprobleme, in: Vogl/Wenda, Grundrechte – Rechtsschutz – Datenschutz.

Probst, Menschenwürde, Personenwürde – Datenschutz nach MBG, Amtshilfe, FS Machacek-Matscher (2008).

Probst/Markel, Die Auswirkungen der MBG-Novelle 2006 auf die Stellung des Rechtsschutzbeauftragten, in: BMI, Integration – Sicherheit – Rechtsschutz.

Pühringer, Vorratsdatenspeicherung, JAP 2012/2013/10 (80).

Raschhofer/Feiler, Die Online-Durchsuchung, in: Zankl, Auf dem Weg zum Überwachungsstaat?

Rede am 30.01.2009 anlässlich des Europäischen Datenschutztags in Wien.

Rieser-Angulo García/Bauer, Polizeiliche und justizielle Zusammenarbeit in der EU (Teil II) - Polizeilicher Informationsaustausch und Datenschutz, SIAK-Journal 2013 H 3.

S. bspw. 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).

Schanda, Auskunftspflicht über Inhaber dynamischer IP-Adressen contra Verpflichtung zur Löschung von Verkehrsdaten, MR 2007.

Scheucher, Dissertation Universität Liechtenstein, Feindrechtsstaat und Feindstrafrecht, Arbeitsversion, Fertigstellung Oktober 2016.

Schmoller, Geändertes Erscheinungsbild staatlicher Verbrechensbekämpfung?, ÖJZ 1996.

Schwaighofer, Der Unmittelbarkeitsgrundsatz beim Zeugenbeweis und seine Ausnahmen, ÖJZ 1996, 124 (134) mit Berufung auf (die mittlerweile überholte Entscheidung) 14 Os 40/95.

Sennett, R. (1992). The fall of public man. WW Norton & Company.

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, 7.

Simmel, G. (1987). Der Fremde. Das individuelle Gesetz–Philosophische Exkurse, Suhrkamp Taschenbuch Wissenschaft, Frankfurt am Main (originally published in 1908).

Sommer, Geldwäschemeldungen und Strafprozess, in. StraFo 2005.

Stephanie Öner/Valerie Walcher, Zum Einspruch nach § 106 StPO, ÖJZ 2014/150.

Stratil (Hrsg), TKG 20034 (2013).

Studie: Clickonomics: Determining the Effect of Anti-Piracy Measures for One-Click Hosting (2013).

Studie: Online Copyright Enforcement, Consumer Behavior, and Market Structure (2015).

Suhr, Freiheit durch Geselligkeit, EuGRZ 1984, Jg 11, 529.

Tschohl 14.06.2011, Studie: Datensicherheit in der TKG Novelle zur Umsetzung der Vorratsdatenspeicherung in Österreich.

Tschohl, Die Anonymität im Internet – Umsetzung der Vorratsdaten-RL im österreichischen Telekom, Strafprozess- und Sicherheitspolizeirecht, in: Jaksch-Ratajczak/Stadler, Aktuelle Rechtsfragen der Internetnutzung, Band 2, 341 ff.

Tschohl, Vorratsdatenspeicherung - Aufstieg und Fall in Österreich, in: Jahrbuch Datenschutzrecht (2014), 31 ff.

Uwer / Organisationsbüro (Hrsg.), Bitte bewahren Sie Ruhe, Leben im Feindrechtsstaat, Vereinigung Berliner Strafverteidiger, 1. Auflage (2006)

Vorwort von Dr. Josef Ostermayer, Bundesminister für Kunst und Kultur, Verfassung und öffentlichen Dienst, Bundeskanzleramt, Bericht über die wirkungsorientierte Folgenabschätzung 2014.

Zerbes, Spitzeln, Spähen, Spionieren (2010).

12.2 Relevante Judikatur

BVerfG 27.02.2008, 1BvR 370/07.

BVerfG 27.02.2008, 1BvR 370/07.

BVerfGE 100, 313 (375 f).

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

EGMR 01.6.2004, Altun, 24.561/94.

EGMR 02.08.1984 Malone gg. das Vereinigte Königreich, RN. 83 f.= EuGRZ 1985.

EGMR 03.07.2007 Copland gg. das Vereinigte Königreich = EuGRZ 2007.

EGMR 04.05.2000 Rotaru gg. Rumänien = ÖJZ 2001.

EGMR 05.02.2008, Ramanauskas gg. Litauen, NL 2008, 21 und 4.11.2010, Bannikova gg. Russland.

EGMR 05.11.2002, 48539/99, Allan v. UK.

EGMR 05.11.2002, Allan v. United-Kingdom.

EGMR 09.06.1998, Teixeira de Castro gg. Portugal, EuGRZ 1999.

EGMR 16.10.2007, Wieser und Bicos Beteiligungen GmbH vs. Österreich, Newsletter Menschenrechte 2007.

EGMR 16.12.1992 Niemietz gg. Deutschland = NJW 1993.

EGMR 22.10.2002 Taylor–Sabori gg. das Vereinigte Königreich.

EGMR 23.04.1997, Van Mechelen und andere gg. die Niederlande, NL 1997, 91.

EGMR 23.10.2014, 54648/09, Furcht v. Deutschland.

EGMR 25.03.1983 Silver gg. das Vereinigte Königreich = EuGRZ 1984.

EGMR 26.03.1987 Leander gg. Schweden.

EGMR 31.05.2007, NL 2007, 133 Kontrová gg. die Slowakei.

EGMR Roman Zakharov v. Russland.

EGMR Rotaru gg. Rumänien, Urteil 4.5.2000, Bsw. Nr. 28341/95.

EGMR Szabó und Vissy v. Ungarn.

EGMR Teixera de Castro v. Portugal, 25829/94, Ramanauskas v. Litauen, 74420/01 und Allan v. UK, 48539/99.

EGMR Urteil Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien.

EGMR, Wille v. Litauen, Urteil 28.10.1999, Bsw. Nr. 28396/95.

EuGH 18.07.2013, C-584/10 P, C-593/10 P und C-595/10 P, Kadi.

OGH 13 Os 127/15y.

OGH 13 Os 153/03.

OGH 15 Os 63/04.

OGH 14.08.2008, 2Ob178/07a.

OGH 19.05.2015, 4Ob22/15m.

OGH 21.10.2014, 4 Ob 140/14p.

OGH 24.06.2014, 4Ob71/14s.

OGH, JBl 1995, 332.

VfGH 16. 12. 2010, G 259/09.

VfGH 27.06.2014, G47/2012, kundgemacht in BGBl I 2014/44.

VfGH 29.06.2012, B 1031/11-20.

VfSlg 1804/1949

VfSlg 2455/1952

VwGH 24.04.2013, 2011/17/0293.

VwGH 27.05.2009, 2007/05/0280.

12.3 Sonstiges

Begutachtungsprozess 192/ME XXV. GP Erläuterungen.

BGBl. I Nr. 165/1999 idF BGBl. I Nr. 2/2008 (1. BVRBG).

EB RV 1613 BlgNR XX. GP, 35.

EuGH Opinion 1/15 des Generalanwalts Mengozzi vom 08.09.2016 zum Gutachten PNR EU-Kanada.

Richtlinie 2005/60/EG des europäischen Parlaments und des Rates vom 26.10.2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, ABl. L 309/15 vom 25.11.2005.

RL 2001/29/EG.

RL 2002/58/EG DatenschutzRL für elektr. Kommunikation

RL EU/2016/681.

RL EU/2016/681.

RV zu BGBl. I 158/2005.