



universität
wien

Masterarbeit

Titel:

**Die Verfassung im Spannungsfeld zwischen
Freiheit und Sicherheit:
Eine Analyse der Problematik der liberalen Grundrechte in Österreich anhand des
Beispiels „Vorratsdatenspeicherung“**

Verfasserin:

Mag. iur Alexandra Stoffl, BA

angestrebter akademischer Grad

Master of Art (MA)

Wien, 2013

Studienkennzahl lt. Studienblatt:	066/824
Studienrichtung lt. Studienblatt:	Politikwissenschaft
Betreuer:	Univ.-Prof. Dr. Karl Ucakar

INHALTSVERZEICHNIS

1. Einleitung.....	3
a) Eine Verfassungsdiskussion aus aktuellem Anlass.....	4
b) Methode	5
c) Die Rolle der Verfassung und das Zusammenspiel zwischen Politik und Recht.....	6
d) Begrifflichkeiten	10
2. Freiheit und Staat.....	12
a) Entwicklung der liberalen Grundrechte.....	12
b) Der Stellenwert (liberaler) Grundrechte	14
c) Grundvoraussetzung - Beschränkung von verfassungsmäßig gewährleisteten Rechten.....	16
a) Einzelne liberale Grundrechte – EMRK und StGG	18
3. Sicherheit und Staat.....	23
a) Der hohe Preis für mehr Sicherheit	25
b) Ein Einblick in die Strafrechtstheorie	26
c) Die absoluten Straftheorien	28
d) Die relativen Straftheorien.....	29
e) Das Zusammenwirken von Polizei und Gericht	30
4. Beschränkung des liberalen Prinzips – Beispiel Vorratsdatenspeicherung	33
a) Was ist Vorratsdatenspeicherung	34
b) Die Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten	36
c) Die Umsetzung der Vorratsdatenspeicher-Richtlinie in Österreich.....	41
5. Der öffentliche Diskurs zur Vorratsdatenspeicherung	49
a) Offizielle Stellungnahmen aus der Politik.....	51
b) Medien und Öffentlichkeit – Reaktionen.....	52
c) Wissenschaftliches Interesse am Thema Vorratsdaten	56
d) Verfassungsrechtliche Prüfung.....	57

6. Abwägung der Interessen.....	59
a) Argumente von Befürwortern der Vorratsdatenspeicherung.....	59
b) Argumente der Gegner der Vorratsdatenspeicherung.....	64
7. Zusammenfassung.....	79
a) Entfernen wir uns immer weiter von einer liberalen Verfassung?	79
b) Werden Sicherheit und Prävention in unserer Gesellschaft höher eingestuft als Privatsphäre und freie Meinungsäußerung?	81
c) Wie drastisch sind die Auswirkungen der Gesetzgebung zur Vorratsdatenspeicherung wirklich?	82
d) Abschließende Gedanken.....	83
8. Nachwort.....	90
9. Anhang	94
Zusammenfassung:	94
Abstract:	95

1. Einleitung

Das Spektrum der Aufgaben, die „*dem Staat*“ zugewiesen sind, ist so breit und vielfältig, dass es nur schwer erfassbar ist. Wohl jede Politikwissenschaftlerin und jeder Politikwissenschaftler beschäftigt sich im Laufe ihres/seines Studiums mehr oder weniger intensiv mit diversen Staatstheorien. Dies mag auch ein Grund dafür sein, dass es unzählige Arbeiten gibt, die sich mit dem Staat und dessen Aufgaben auseinandersetzen.

Dass staatswissenschaftliche Analysen dennoch niemals obsolet sind, lässt sich durch die Komplexität des Staatsbegriffes und den teilweise widersprüchlichen Charakter der Aufgaben „*des Staates*“ begründen.

Obwohl einige Staatstheorien Jahrhunderte überdauern und noch heute von Politikwissenschaftlerinnen und Politikwissenschaftlern für Analysen herangezogen werden, oder als Referenzen für das „ideale Staatsgerüst“ dienen, sind der Staatsbegriff und die Anforderungen, die an den abstrakten Staat gestellt werden, dynamisch und befinden sich in einem permanenten Wandel. Es scheint, als hätte jede Zeit ihre ganz eigenen Prioritäten und Probleme, auf die der Staat reagieren muss.

Es gibt kaum zwei Begriffe in der Politikwissenschaft, die so eng miteinander verbunden sind wie „Staat“ und „Verfassung“. Wie die Schwerpunkte in einem Staat gesetzt sind, wie Wertigkeiten verteilt sind, lässt sich zu einem gewissen Teil aus der Verfassung ablesen: Der Zeitgeist spiegelt sich in der Verfassung wider. Durch die wissenschaftliche Auseinandersetzung mit der Verfassung in Verbindung mit Gesetzen, welche die Verfassung berühren, lassen sich Tendenzen feststellen und sogar vorsichtige Zukunftsprognosen wagen.

Auch wenn die grundsätzlichen Regelungen, die in der Verfassung getroffen werden, auf den ersten Blick fast zeitlos erscheinen, ergibt sich durch bestimmte Ereignisse und eine nach und nach stattfindende Veränderung der Gesellschaft eine neue Rolle des Staates: Dies kann dazu führen, dass gewisse Anforderungen, welche die politische und soziale Wirklichkeit an den Gesetzgeber stellt, eine Bedrohung oder Beschränkung der durch die Verfassung garantierten Rechte des Einzelnen darstellen.

Daraus resultieren Widersprüche, die nicht vollständig gelöst werden können und immer wieder dazu führen, dass Kompromisse eingegangen werden müssen, die nur mäßig zufriedenstellend sind und von vielen als Nicht-Lösung wahrgenommen werden.

Der Gesetzgeber soll dafür sorgen, dass der/die Einzelne vor Willkür geschützt wird, und möglichst detaillierte Regelungen getroffen werden, die zu mehr Rechtssicherheit führen. Gleichzeitig wird jedoch mehr Flexibilität von den Verwaltungsbehörden gefordert, die sich mit den Umständen des Einzelfalls befassen sollen, und oftmals wird dadurch verkannt, dass auch ihnen durch eine sehr große Regelungsdichte die Hände gebunden sind. Dies ist nur eines von vielen Beispielen.

Spannungsverhältnisse dieser Art lassen sich auf so gut wie allen Ebenen finden, und man kommt zu dem Ergebnis, dass keine Regelung perfekt sein kann. Doch sich mit dieser Erkenntnis zufrieden zu geben, reicht nicht aus. Vielmehr muss untersucht werden, worin Kompromisslösungen bestehen können, die zumindest nicht als grob ungerecht wahrgenommen werden, und wie diese argumentierbar und nachvollziehbar sind.

Diese Arbeit konzentriert sich auf ein bestimmtes Spannungsverhältnis: jenes zwischen dem liberalen Grundprinzip der Verfassung (sowie der Idee, die hinter diesem Prinzip steht), der Freiheit der/des Einzelnen, die durch die staatsbegrenzenden Grundrechte garantiert werden soll – und der Sicherheit im weitesten Sinne. In diesem Zusammenhang möchte ich mich vor allem mit dem Grundrecht auf Datenschutz (Stichwort: Vorratsdatenspeicherung) sowie im Zusammenhang damit, mit dem Sicherheitspolizeirecht befassen.

a) Eine Verfassungsdiskussion aus aktuellem Anlass

Die vorliegende Arbeit versucht, eine Verschiebung von Wertigkeiten im Staat hinsichtlich der Problematik von *Freiheit* und *Sicherheit* nachzuzeichnen: Den Anlass für diese Analyse stellt die Gesetzgebung zur Vorratsdatenspeicherung dar, die in den letzten Monaten vermehrt für ausgeprägte Diskussionen gesorgt hat, wobei immer wieder auch von einer Gefährdung der Grundrechte der/des Einzelnen, ja sogar von einem Verstoß gegen das liberale Prinzip der österreichischen Bundesverfassung gesprochen wurde – im Namen der Sicherheit?

Bedenklich daran ist jedoch vor allem, dass kaum jemand weiß, was es mit der

Vorratsdatenspeicherung tatsächlich auf sich hat. Die Tatsache, dass die Implementierung der Vorratsdatenspeicherungsrichtlinie in Österreich durch unterschiedliche – an sich bereits höchst komplexe – Gesetze stattgefunden hat, trägt noch zusätzlich zu Unsicherheiten bei. Dies sei an dieser Stelle vorerst nur am Rande erwähnt.

b) Methode

Um den Kern des Problems der Vorratsdatenspeicherung überhaupt verstehen zu können, bedarf es zunächst einer **theoretischen Auseinandersetzung mit der Verfassung**, ihrem Aufbau, ihrer Bedeutung und ihrem grundsätzlichen Charakter.

Diese theoretische Auseinandersetzung befasst sich vor allem auch mit dem Zusammenspiel zwischen Politik und Recht; in diesem Zusammenhang kommt der Verfassung eine besondere Bedeutung zu. Um den herausragenden Charakter der Verfassung besser zu verstehen, wird auch kurz auf die Systematik österreichischer Rechtsordnung eingegangen.

Um die tatsächliche Tragweite der Vorratsdatenspeicherung beurteilen zu können ist eube Auseinandersetzung mit einzelnen betroffenen **Grundrechten** notwendig.

Diese finden sich teilweise im Staatsgrundgesetz, teilweise zusätzlich auch in der EMRK. Es wird fast ausschließlich auf die liberalen Grundrechte eingegangen, da diese im Zentrum der Arbeit stehen und auch diejenigen sind, die am ehesten von der Vorratsdatenspeicherung betroffen sein könnten. Im Zuge dessen wird die Entstehungsgeschichte dieser Grundrechte kurz skizziert, da diese für die gegenwärtige Bedeutung derselben immens wichtig war.

Schließlich ist es auch unumgänglich, den Aufbau und Inhalt der von der Vorratsdatenspeicherung (mittelbar oder unmittelbar) betroffenen Gesetze zu skizzieren, wobei versucht wird, diesen Teil möglichst kurz und prägnant zu halten. Konkret muss aber insbesondere auf das **Telekommunikationsgesetz** und die darin enthaltenen neuen Bestimmungen eingegangen werden.

Erst in weiterer Folge wird auf den **Hintergrund der Vorratsdatenspeicherungsrichtlinie**, ihre **Umsetzung in Österreich**, ihre Entstehungsgeschichte und die Reaktionen darauf eingegangen. In diesem Zusammenhang soll auch dargestellt werden, wie die Vorratsdatenspeicherung der Öffentlichkeit bislang präsentiert wurde, und welches Bild sich

daraus ergibt.

Im Anschluss daran sollen die **positiven** und **negativen Aspekte** der Vorratsdatenspeicherung diskutiert werden. Hier werden vor allem die in der öffentlichen Diskussion immer wieder auftauchenden Argumente genauer betrachtet, und zunächst ohne eine Bewertung dieser Argumente vorzunehmen, wiedergegeben.

Abschließend soll auf die Stichhaltigkeit dieser Argumente in einer Zusammenfassung und Conclusio eingegangen und auch eine vorsichtige Zukunftsprognose angestellt werden.

Im Schlussteil sollen schließlich auch **folgende Forschungsfragen** nochmals ausdrücklich beantwortet werden:

1. Entfernen wir uns schrittweise von einer – lange Zeit als Ideal betrachteten – liberalen Verfassung?
2. Werden Sicherheit und Prävention in unserer Gesellschaft höher eingestuft als Privatsphäre und freie Meinungsäußerung?
3. Wie drastisch sind die Auswirkungen der Gesetzgebung zur Vorratsdatenspeicherung wirklich?

Am Ende dieser Arbeit sollte die Leserin/ der Leser selbst Schlüsse darüber ziehen können, wie das Spannungsverhältnis zwischen Freiheit und Sicherheit im Staat aufzulösen ist, oder ihrer/ seiner Meinung nach aufzulösen sein sollte und worin nun tatsächlich die wichtigste Aufgabe von Recht und Politik, und im diesem Zusammenhang natürlich der Verfassung, besteht.

c) Die Rolle der Verfassung und das Zusammenspiel zwischen Politik und Recht

Recht und Politik sind untrennbar miteinander verbunden. Damit politische Maßnahmen umgesetzt werden können, bedarf es, ganz allgemein und praktisch gesprochen, immer eines rechtlichen Rahmens. Sollen also staatliche Maßnahmen gesetzt werden, sei es in der Wirtschaftspolitik, Sozialpolitik, Umweltpolitik oder Bildungspolitik, so muss zunächst auch

stets ein Regelwerk geschaffen werden, das die Umsetzung der betroffenen Maßnahmen sicherstellt und lenkt. Die wichtige Rolle, die dem Recht für die politische Gestaltung eines Landes zukommt, wird oftmals von Politologinnen und Politologen vernachlässigt und das Recht als etwas von der Politik völlig Losgelöstes angesehen.

Ebenso ignorant stehen viele Juristinnen und Juristen der Politologie oder gar der Politik im Allgemeinen gegenüber. Dabei wird gänzlich außer Acht gelassen, dass Rechtskonstrukte und Gesetze nicht einfach vom Himmel fallen, sondern in einem legislativen Prozess entstehen. Dieser legislative Prozess wird vor allem durch eines gesteuert – politische Interessen.

Recht ist nicht unpolitisch, sondern könnte kaum politischer sein.

Durch die Analyse diverser Trends in der Gesetzgebung kann ungemein viel darüber ausgesagt werden, wohin ein Staat sich bewegt, welche Entwicklungen in Gange sind, wo Prioritäten gesetzt werden, worin die Sorgen und Nöte eines bestimmten Jahrzehntes liegen. Kaum etwas eignet sich also besser für die staatswissenschaftliche Analyse als Gesetze.

Eine ganz besondere Rolle kommt in diesem Zusammenhang zweifelsohne der Verfassung zu: Die Verfassung „bildet den rechtsstaatlichen Rahmen der Politik“.¹ Änderungen der Verfassung oder bestimmter Verfassungsgesetze oder der Beschränkung oder Erweiterung bestimmter verfassungsmäßig gewährleisteter Rechte sind daher naturgemäß als ganz besonders bedeutsam anzusehen und bedürfen wohl auch eines besonders breiten politischen Konsenses.

Damit bestimmte Gesetze also überhaupt entstehen können, ist zunächst politisches Handeln und das Treffen von Entscheidungen auf politischer Ebene unabdingbar, „(d)enn einerseits ist die Politik durch die rechtlich vorskizzierten Handlungsspielräume determiniert, andererseits übernimmt sie im demokratischen Verfassungsstaat die Rolle der zentralen Schöpferin von Recht. Ziel des politischen Prozesses ist, die Auffassungen der politischen Majorität (natürlich mit grundrechtlichen Einschränkungen) in verbindliche Rechtsnormen zu gießen.“² Der politische Gestaltungsspielraum ist grundsätzlich groß. Politische Parteien können – theoretisch – wenn sie einmal gewählt sind, im Staat signifikante Veränderungen durchsetzen. Dies geschieht vor allem durch Gesetzgebung.

Das Recht kennt jedoch zuverlässige Mechanismen, durch die auch die politische Macht

¹ Öhlinger, Verfassung und Verfassungsrecht zwischen Politik und Recht, 2012, S. 51.

² Ehs/Gschiegl/Ucakar/Welan (Hg.), Politik und Recht. Spannungsfelder der Gesellschaft, 2012, S. 21.

eingeschränkt wird. Das österreichische Rechtssystem ist so aufgebaut, dass nicht alle Gesetze beliebig verändert werden können.

Der so genannte „Stufenbau der Rechtsordnung“³ ist ein solcher Mechanismus, den es zu verstehen gilt, um die dieser Arbeit zu Grunde liegende *rechtliche* Problematik nachvollziehen zu können. Recht ist nicht gleich Recht, Gesetz ist nicht gleich Gesetz. Im österreichischen Rechtssystem gibt es Gesetze unterschiedlicher Bedeutung und unterschiedlicher rechtlicher Qualität.

Innerhalb des staatlichen Rechts kommt dem Verfassungsrecht die höchste Bedeutung beziehungsweise der höchste Rang zu. Alle anderen Gesetze, bei denen es sich nicht um Verfassungsrecht handelt, sind an das Verfassungsrecht gebunden, das heißt, sie dürfen dem Verfassungsrecht nicht widersprechen. Verfassungswidrige Gesetze sind nicht per se nichtig, sondern so lange anwendbar, bis der Verfassungsgerichtshof ihre Verfassungswidrigkeit feststellt und diese aufhebt.

Auch das Verfassungsrecht selbst lässt sich nochmals untergliedern. Die so genannten Verfassungsprinzipien sind die leitenden Grundsätze der Verfassung und genießen einen höheren Bestandsschutz als das übrige Verfassungsrecht.

Wird ein solcher Grundsatz durch eine Gesetzesänderung berührt, ist immer zu prüfen, ob sich daraus eine „Gesamtänderung“ der Verfassung ergibt. Ist dies der Fall, so ist eine Volksabstimmung notwendig. Dies ist deshalb der Fall, weil eine solche Gesamtänderung als so drastisch angesehen wird, dass dem Volk auch auf direktem Wege die Möglichkeit gegeben werden muss, über sie zu entscheiden. Ganz allgemein kommt auch dem „einfachen Verfassungsrecht“ eine höhere Bestandskraft zu als den einfachen Gesetzen. Man spricht daher auch nach dem Stufenbau der Rechtsordnung nach derogatorischen Kraft, nach der Möglichkeit der Abänderlichkeit.⁴

Für das österreichische Recht ergibt sich daher eine klare Rangordnung. Das Recht einer niedrigeren Stufe ist immer durch das Recht einer höheren Stufe bedingt und kann durch dieses abgeändert werden. Gleichzeitig ist Konsequenz daraus, dass es höherrangigem Recht nicht widersprechen darf. An der Spitze dieses Stufenbaus steht die so genannte „Grundnorm“. Worum es sich bei dieser Grundnorm genau handelt, ist schwer zu erklären

³ Dieser Begriff wurde vom österreichischen Juristen Hans Kelsen geprägt und von Adolf Julius Merkl weiterentwickelt.

⁴ Zum Stufenbau der Rechtsordnung vgl. zB: Öhlinger, Verfassungsrecht8, 2009, S.27 ff.

und zutiefst rechtsphilosophisch.

Die Existenz einer solchen Grundnorm muss vorausgesetzt werden, um den restlichen Stufenbau auf sie zu stützen. Auf der nächst höheren Stufe befinden sich die Grundprinzipien der Bundesverfassung. Dabei handelt es sich um das demokratische Prinzip, das republikanische Prinzip, das bundesstaatliche Prinzip, das rechtsstaatliche Prinzip, das gewaltenteilende und das liberale Prinzip.

Unter diesen Grundprinzipien ist das Bundesverfassungsrecht einzuordnen, darunter das Landesverfassungsrecht. Die einfachen Bundesgesetze und Landesgesetze stehen schließlich auf derselben Stufe. Verordnungen sind unter den Gesetzen einzustufen.

Dem Europarecht kommt eine Sonderstellung zu. Es ist grundsätzlich höherrangig als sämtliches nationalstaatliches Recht, sollte jedoch – da es auf den Verfassungstraditionen der Mitgliedstaaten aufbaut – eigentlich nicht mit nationalstaatlichem Verfassungsrecht kollidieren.

Anhand dieses Grundgerüsts lässt sich bereits erahnen, dass Rechten, denen ein höherer gesellschaftlicher Stellenwert zukommt, wohl auch eine erhöhte Bestandskraft zukommen muss und sie daher in Verfassungsgesetze gegossen werden. Dies trifft vor allem auf die Grundrechte zu. Die Idee der Grundrechte basiert auf Vorstellung, „dass der Mensch mit seiner Person verbundene und daher unabdingbare Rechte habe. (...) Die eigentliche Idee der Grund- und Freiheitsrechte nach unserem heutigen Verständnis wurde aber erst geboren, als man diese natürlichen Rechte des Menschen ausdrücklich und bewusst als einen gegen Eingriffe der staatlichen Autorität gerichteten Anspruch zu verstehen begann.“⁵

Wenn bereits Recht stets etwas höchst Politisches ist, und als Spiegel unserer Gesellschaft verstanden werden kann, so trifft dies ganz besonders auf die Grund-, Menschen- und Verfassungsrechte zu: „Bei den Grund- und Menschenrechten ist die Dynamik im Verhältnis von rechtlicher Reglementierung und gesellschaftlicher Veränderung besonders signifikant ausgeprägt: Geänderte gesellschaftliche Verhältnisse erfordern neue grund- und menschenrechtliche Regulative, die ihrerseits Bewährung an den Sachverhalten sichern.“⁶

⁵ Adamovich/Funk/Holzinger, Österreichisches Staatsrecht³ – Grundrechte, Wien 2003, S.3 ff.

⁶ Funk, Grund- und Menschenrechte im Spannungsfeld zwischen Politik und Recht, 2012, S.71.

d) Begrifflichkeiten

Liberales Prinzip der Verfassung, die liberalen Grundrechte, Freiheit

In Österreich spiegeln sich die wichtigsten Anforderungen an den Staat in den Grundprinzipien der Österreichischen Bundesverfassung wider. Das liberale Prinzip ist nicht als solches in der österreichischen Bundesverfassung festgeschrieben, sondern ergibt sich vielmehr aus deren Systematik. Das liberale Prinzip soll die Freiheit (im weitesten Sinne) aller Menschen, die im Staat leben, sichern.

Der Freiheitsbegriff lässt sich nicht abschließend definieren. Die Verfassung und diverse andere Gesetze haben die Aufgabe, unterschiedlichste Freiheiten von Menschen zu schützen und die Macht des Staates insofern teilweise zu begrenzen. Die Freiheit der Einzelnen/des Einzelnen ist durch Grundrechte geschützt, die eine erhöhte Bestandsgarantie aufweisen⁷ und Abwehrrechte gegenüber dem Staat darstellen.

Die Grenze, durch die Staat und Gesellschaft getrennt werden und die die Freiheit des Individuums sichern soll, wird durch die Grundrechte normiert, denen somit eine essentielle Schlüsselrolle zukommt: „In diesem Sinn ist die Existenz eines Katalogs staatsbegrenzender („liberaler“) Grundrechte ein Verfassungsprinzip. Die Beseitigung dieses Katalogs – nicht jedoch seine Modifikation – wäre ebenfalls eine Gesamtänderung der Bundesverfassung.“⁸

In dieser Arbeit sind vor allem das Grundrecht auf Privatsphäre, sowie das Recht auf freie Meinungsäußerung von zentraler Bedeutung. Diese Grundrechte basieren auf der Annahme, dass die/der Einzelne in bestimmten Bereichen ihres/seines Lebens von Eingriffen und Einmischungen von Seiten des Staates geschützt sein soll, stellen also liberale Grundrechte dar.

Wenn in weiterer Folge davon gesprochen wird, dass die Vorratsdatenspeicherung bestimmte oder damit im Zusammenhang stehende Gesetze das liberale Prinzip der Bundesverfassung berühren, so ist damit vor allem gemeint, dass in einzelne Grundrechte eingegriffen wird, beziehungsweise, dass einzelne Normen im Spannungsverhältnis zu den Grundrechten stehen.

⁷ Adamovich/Funk/Holzinger, Österreichisches Staatsrecht³ – Grundrechte, Wien 2003, S.24.

⁸ Öhlinger, Verfassungsrecht⁸, Wien 2009, S. 60.

Sicherheit

Sicherheit ist der zweite zentrale Begriff dieser Arbeit. Sicherheit umfasst im Konkreten die *Gefahrenabwehr* und ihre *Aufklärung* durch den Staat. Gemeint sind einerseits terroristische Vereinigungen als Gefahr für den Staat als Gesamtheit, andererseits aber auch die Sicherheit der/des Einzelnen, die einer der wichtigen genannten Gründe sind, weshalb der Staat unter Umständen in Privatsphäre seiner Staatsbürger eingreifen darf. Sicherheit meint demnach die präventive Abwehr von Straftaten, andererseits aber auch die Aufklärung von Straftaten. Unter Einschränkungen unter dem Aspekt der *Sicherheit* als Gegenpol zur *Freiheit* wird also in Folge alles verstanden, was einen Eingriff in die Freiheit des Einzelnen zur Verhinderung oder Aufklärung von Straftaten darstellt.

Damit verbunden ist auch die Problematik des „präventiven Strafrechts“ und – hier vor allem relevant – die Thematik des Datenschutzes, die eng mit dem Begriff der Privatsphäre verknüpft ist.

2. Freiheit und Staat

Unser Staats- und Rechtsverständnis ist weithin von der Annahme geprägt, dass der Mensch unabdingbare Rechte habe. Dabei handelt es sich um Grund- und Freiheitsrechte, deren Tradition noch gar nicht so weit zurückreicht, wie manchmal angenommen wird. In Zeiten des Mittelalters gab es schlichtweg keine Grundrechte, die den Menschen zugesichert worden wären.⁹

Neben den liberalen Grundrechten (oder Freiheitsrechten) gibt es Gleichheitsrechte, demokratische/politische Grundrechte, Verfahrensgrundrechte, soziale Grundrechte, und andere Grundrechte¹⁰, wobei die Einteilung der Grundrechte auf unterschiedliche Art und Weise vorgenommen werden kann. Teilweise wird einfach nur danach unterschieden, ob dem Staat eine aktive Rolle zukommt, um der/dem Einzelnen zu ihren/seinen Rechten zu verhelfen, oder ob er lediglich Unterlassungspflichten hat.

Unter liberalen Grundrechten versteht man all jene Grundrechte, die eine Begrenzung der Staatsmacht garantieren und den Menschen *Freiheit vom Staat* sichern.

Die Grundrechte werden zwar in der Verfassung als solche nicht ausdrücklich proklamiert, dennoch sind sie eine Voraussetzung dafür, dass man überhaupt von einer rechtsstaatlichen Verfassung sprechen kann.¹¹

Die Sicherstellung der Grundrechte – einschließlich der liberalen Grundrechte – kann somit als durchaus als Bedingung dafür bezeichnet werden, dass überhaupt eine Verfassung vorliegt.

a) Entwicklung der liberalen Grundrechte

Die Wurzeln unseres heutigen Grundrechtsverständnisses begannen sich nach und nach im England des 17. Jahrhunderts zu entwickeln. Zu dieser Zeit begann man damit, den Menschen nicht mehr bloß als Bestandteil einer Gemeinschaft zu sehen, sondern auch als Individuum. Abwehrrechte gegenüber dem Staat bildeten vor allem in der frühen Phase der

⁹ Adamovich/Funk/Holzinger, Österreichisches Staatsrecht³ – Grundrechte, Wien 2003, S.3.

¹⁰ Vgl. Hengstschläger/Leeb, Grundrechte, Wien 2012, S. 17 ff.

¹¹ Vgl. Öhlinger, Verfassungsrecht⁸, Wien 2009, S. 60 f.

Grundrechtsentwicklung einen substantiellen Bestandteil der Grundrechte. Vor allem der Schutz des Individuums vor staatlichen Eingriffen stand im Vordergrund. Solche Abwehrrechte wurden auch als „bürgerliche Rechte“ bezeichnet.¹² Aus diesen bürgerlichen Rechten setzte sich das zusammen, was wir heute unter „liberalen Grundrechten“ verstehen.

Liberalen Grundrechte sollen – wie sich bereits allein aus der Begrifflichkeit erkennen lässt – die individuelle Freiheit der Menschen sichern, indem dem Staat gewissen Grenzen gesetzt werden, die dieser nicht überschreiten darf. Somit werden bestimmte Lebensbereiche von staatlichen Reglementierungen ausgenommen und der/dem Einzelnen die Freiheit gelassen, innerhalb gewisser Grenzen eigene Entscheidungen zu treffen, ohne dem Staat die Möglichkeit der Beeinflussung zu geben.

Im weiteren Sinne wird daher mit liberalen Grundrechten auch eine gewisse Trennung von Staat und Gesellschaft verbunden.¹³ Der klassischen Einordnung von Grundrechten folgend handelt es sich bei den liberalen Grundrechten um Abwehrrechte (status negativus) gegenüber dem Staat.¹⁴

Wie bereits kurz erwähnt, ist das liberale Prinzip als solches nicht ausdrücklich in der österreichischen Bundesverfassung bezeichnet. Ebenso vergeblich wird man in der Verfassung nach einem Grundrechtskatalog suchen. Was im allgemeinen Sprachgebrauch unter „Grundrechten“ verstanden wird, bezeichnet die österreichische Bundesverfassung als „verfassungsmäßig gewährleistete Rechte“, die jedoch auf unterschiedlichste Rechtsquellen aufgeteilt sind. Diese Verstreuung macht es mitunter schwierig festzustellen, welche Rechtsvorschriften im Verfassungsrang subjektive Rechte gewährleisten.¹⁵

Als Hauptgrund für das Fehlen eines Grundrechtskatalogs im B-VG ist der mangelnde Konsens bei der Ausarbeitung der Bundesverfassung 1919/1920 bezeichnet. Die Parteien konnten sich auf keine Neukodifikation der Grundrechte einigen¹⁶, weshalb nach wie vor dem Staatsgrundgesetz 1867 (StGG) essentielle Bedeutung zukommt, welchem durch Artikel 149 B-VG sogar ausdrücklich der Status eines Verfassungsgesetzes verliehen wurde.

¹² Vgl. Hengstschläger/Leeb, Grundrechte, Wien 2012, S. 17.

¹³ Hengstschläger/Leeb, Grundrechte, Wien 2012, S. 17.

¹⁴ Lurger, Das Europarecht aus der Perspektive des Unionsbürgers, ZfRV, Graz 2000, S. 71.

¹⁵ Vgl. Öhlinger, Verfassungsrecht⁸, Wien 2009, S. 298.

¹⁶ Vgl. Öhlinger, Verfassungsrecht⁸, Wien 2009, S. 299.

Neben dem Staatsgrundgesetz wurden auch andere Grundrechtsquellen¹⁷ als Verfassungsgesetze rezipiert.¹⁸

Nach dem Zweiten Weltkrieg fand die wohl wichtigste Erweiterung der Grundrechte statt: Der Grundrechtskatalog der Europäischen Menschenrechtskonvention (EMRK) wurde in den österreichischen Grundrechtstatbestand aufgenommen. Die durch die EMRK kodifizierten Rechte gelten in Österreich als unmittelbar anwendbare verfassungsmäßig gewährleistete Rechte. Wenn also folglich davon gesprochen wird, dass die Vorratsdatenspeicherung ein Grundrecht berührt, so sind damit sowohl die Grundrechte des Staatsgrundgesetzes, als auch jene der Europäischen Menschenrechtskonvention umfasst.

Es waren die liberalen Grundrechte, auch *klassische Grundrechte* genannt, die bei der ersten verfassungsrechtlichen Kodifikation subjektiver Rechte zentral waren, also die Abwehrrechte gegenüber dem Staat.

Diese Einordnung ist jedoch nicht bloß für Österreich typisch. So stellte beispielsweise der deutsche Bundesverfassungsgerichtshof fest, dass der Gehalt der Grundrechte als staatsgerichtete Abwehrrechte den „ursprünglichen und bleibenden Sinn der Grundrechte“ und den Kern jedes neuen Grundrechtsverständnisses bilde.¹⁹

Diese Ansicht hielt sich auch in Österreich sehr lange, wobei es nunmehr seit mehreren Jahrzehnten auch in Österreich als anerkannt gilt, dass es neben (den Staat einschränkenden) Abwehr-Grundrechten auch solche gibt, die den Staat zu einem positiven Tun verpflichten, um den Schutz des Einzelnen zu gewährleisten.

Dies ändert jedoch nichts an der wichtigen Rolle, welche den liberalen Grundrechten in der österreichischen Verfassungstradition zukommt.

b) Der Stellenwert (liberaler) Grundrechte

¹⁷ Gemeint sind hier das Gesetz zum Schutze der persönlichen Freiheit (1862), das Gesetz zum Schutze des Hausrechtes (1862) und der Beschluss der provisorischen Nationalversammlung (1919) zum Zensurverbot, der Gewährleistung der vollen Pressefreiheit und vollständigen Wiederherstellung der Vereins- und Versammlungsfreiheit.

¹⁸ Vgl. Berka, Lehrbuch Verfassungsrecht², Wien 2008, S. 321.

¹⁹ Vgl. Öhlinger, Verfassungsrecht⁸, Wien 2009, S. 305.

Grundrechte, oder „verfassungsmäßig gewährleistete Rechte“ sind subjektive Rechte Privater. Aufgrund des besonderen Stellenwertes, der den Grundrechten im Verfassungskontext zukommt, erfolgt auch die Auslegung von Grundrechten nach einem besonderen Schema: So kann durchaus gesagt werden, dass Grundrechte – insbesondere aufgrund der Annahme, dass es sich dabei um Rechte handelt, die jeder Mensch von Geburt aus hat und die ihm auch nicht aberkannt werden können – eine besondere Bestandskraft haben und ihnen insofern auch Vorrang gegenüber anderen Rechten zukommt.

Die besondere Bestandskraft der Grundrechte wird in der Lehre auch als *Unverbrüchlichkeit* bezeichnet. Damit ist gemeint, dass Grundrechte nur erschwert beziehungsweise überhaupt nicht aufgehoben oder abgeändert werden können.²⁰

Die unterschiedlichen Grundrechte ergeben ein System von Prinzipien, an dessen oberster Stelle die Achtung vor der Selbstbestimmung und Würde des Menschen steht.²¹

Dass jedoch kein Grundrecht oder keine Grundfreiheit unbeschränkt gilt, ergibt sich aus der Natur der Grundrechte selbst: Jeder Mensch kann die ihm durch den Staat beziehungsweise die Verfassung gewährleisteten Freiheiten und Rechte nur insofern ausüben, als er dadurch nicht andere Menschen in deren Freiheiten und Rechten einschränkt. Die Freiheit der/des einen ist nicht mehr wert als die Freiheit/die Rechte der/des anderen.

Dies schließt selbstverständlich auch den Fall mit ein, in dem jemand durch die Ausübung ihrer/seiner Freiheiten die Sicherheit anderer Menschen gefährdet.

An dieser Stelle sei daher festgehalten, dass auch Grundrechte nicht *per se* unbegrenzt gelten. Treffen mehrere Interessen – in Gestalt von Rechten – aufeinander, so ist eine Güterabwägung vorzunehmen.²² Was auf den ersten Blick nach einer logischen Lösung für das Problem von Grundrechtskollisionen aussieht, erweist sich jedoch bei genauerer Betrachtung als äußerst diffizil, da sich die einzelnen Güter bzw. Rechte im Einzelfall nicht immer gegeneinander abwägen lassen. Der Rechtsprechung kommt insofern eine schwierige Aufgabe zu, die zu einer dynamischen Fortentwicklung der Grundrechte bzw ihres Stellenwertes führt.

²⁰ Hengstschläger/Leeb, Grundrechte, Wien 2012, S. 1.

²¹ Adamovich/Funk/Holzinger, Österreichisches Staatsrecht 3. Grundrechte, Wien 2003, S.15.

²² Adamovich/Funk/Holzinger, Österreichisches Staatsrecht 3. Grundrechte, Wien 2003, S.16.

Eine solche Dynamik ist durchaus wünschenswert: Auch dem einfachen Gesetzgeber muss Raum für die Durchsetzung seiner rechtspolitischen Ziele zugestanden werden, und dies gilt selbst dann, wenn dadurch auch Grundrechte berührt werden.²³

Gleichzeitig darf der dem Gesetzgeber bleibende Spielraum nicht so groß sein, dass schließlich das Grundrecht als solches ausgehöhlt wird und der/dem Einzelnen von ihrem/seinem subjektiven Recht nichts weiter bleibt, als eine leere Hülle. Die Grenzziehung ist daher essentiell.

Die grundlegende Bedeutung der Grundrechte wird auch durch ihre Bindungswirkung gegenüber allen Staatsfunktionen zum Ausdruck gebracht, da die Grundrechte die Gesetzgebung, die Vollziehung und die Rechtsprechung binden.²⁴

c) Grundvoraussetzung - Beschränkung von verfassungsmäßig gewährleisteten Rechten

Wird in der gegenständlichen Arbeit von einer Begrenzung der Freiheit gesprochen, so ist damit der Überbegriff der durch die Vorratsdatenspeicherung berührten Grundrechte gemeint. Aus verfassungsrechtlicher Sicht ist dazu vorab zu sagen, dass nicht jeder Eingriff in ein verfassungsmäßig gewährleistetes Recht, nicht jede Einschränkung der durch die Verfassung gewährleisteten Freiheiten, rechts- beziehungsweise verfassungswidrig ist:

Unter Eingriff ist bereits jeder staatliche Akt zu verstehen, der in eine grundrechtlich geschützte Rechtsphäre eingreift und diese belastet. Was jeweils konkret einen Eingriff darstellt, ist bei den unterschiedlichen Grundrechten verschieden und wurde durch die Judikatur geprägt.

Teilweise stellen nur intentionale Eingriffe einen Eingriff in ein bestimmtes Grundrecht dar. Dies ist beispielsweise bei der Kunstfreiheit der Fall – ein verfassungswidriger Eingriff in das Grundrecht der Freiheit der Kunst kann demnach nur dann vorliegen, wenn eben gerade die Intention des Eingriffs die Einschränkung der Kunstfreiheit ist.

²³ Adamovich/Funk/Holzinger, Österreichisches Staatsrecht 3. Grundrechte, Wien 2003, S.16.

²⁴ Adamovich/Funk/Holzinger, Österreichisches Staatsrecht 3. Grundrechte, Wien 2003, S.17.

Bei anderen Grundrechten ist bereits jede Beschränkung als Eingriff zu bewerten. Ein Beispiel dafür ist die Eigentums- oder Meinungsfreiheit.

Selbst wenn ein Eingriff festgestellt wird, so bedeutet dies nicht unbedingt, dass eine verfassungswidrige Verletzung des Grundrechts erfolgt ist. Es muss daher in einem weiteren Schritt festgestellt werden, ob es sich um einen verfassungsmäßigen oder einen verfassungswidrigen Eingriff in das betreffende Grundrecht handelt.

Wird durch ein bestimmtes Gesetz in ein Grundrecht eingegriffen ist zunächst zu prüfen, ob im Rahmen des Gesetzesvorbehalts vorgegangen wurde. Ganz grundsätzlich existiert eine Bindung des Gesetzgebers an die Grundrechte. Dies bedeutet, dass dem Gesetzgeber durch die Grundrechte Schranken gesetzt sind, innerhalb derer der legislative Handlungsspielraum liegt. Für viele Grundrechte ist ein Gesetzesvorbehalt vorgesehen.

Gesetzesvorbehalte ermächtigen die Legislative dazu, bestimmte Grundrechte entweder näher auszugestalten (wie beispielsweise die Vereinsfreiheit) oder diese auch einzuschränken (wie beispielsweise die Eigentumsfreiheit). Es wird zwischen formellen und materiellen Gesetzesvorbehalten unterschieden. Formelle Gesetzesvorbehalte lassen dem Gesetzgeber einen relativ weiten Spielraum und Möglichkeiten zur Einschränkung. Materielle Gesetzesvorbehalte hingegen determinieren relativ genau, unter welchen Voraussetzungen ein bestimmtes Grundrecht beschränkt werden darf. Zum einen dürfen Grundrechte mit einem materiellen Gesetzesvorbehalt immer dann eingeschränkt werden, wenn Rechtsgüter geschützt werden müssen, die besonders wichtig für eine demokratische Gesellschaft sind.

Ein Eingriff in ein bestimmtes Grundrecht zum Zweck des Schutzes solcher hochwertiger Rechtsgüter muss notwendig sein; dies setzt auch die Verhältnismäßigkeit des Eingriffs voraus.

Bei genauerem Hinterfragen des Begriffes der Verhältnismäßigkeit ergibt sich folgendes Ergebnis: Wenn das Ziel der Regelung, die in ein Grundrecht eingreift im öffentlichen Interesse liegt und die Regelung selbst zur Erreichung des Ziels geeignet ist und auch erforderlich, um das Ziel zu erreichen, so ist unter der Voraussetzung, dass die Adäquanz oder

Güterabwägung zwischen dem Grundrecht und dem konkreten Ziel ausgeglichen ist, eine Beschränkung des Grundrechtes zulässig.²⁵

Dieses Prüfungsschema, das so auch vom Verfassungsgerichtshof angewandt wird, ist im Hinterkopf zu behalten, wenn – wie im konkreten Fall die Vorratsdatenspeicherung – ein Rechtsakt auf seine Grundrechtskonformität und Verfassungsmäßigkeit geprüft wird.

Es darf nicht vergessen werden, dass nicht jeder Eingriff, jede potentielle Beeinflussung eines Grundrechts, auch verfassungswidrig ist.

Nachstehend soll daher jeweils auch konkret auf das besprochene Grundrecht bezogen kurz dargestellt werden, unter welchen Voraussetzung eines Beschränkung dieses Grundrechts zulässig ist.

Dies soll der Leserin/ dem Leser dabei helfen, ein Gefühl dafür zu bekommen, ob die Vorratsdatenspeicherung in Bezug auf den konkreten Eingriff mit dem Verfassungsrecht in Einklang zu bringen ist, oder diesem entgegensteht.

a) Einzelne liberale Grundrechte – EMRK und StGG

Die traditionell herausragende Position der liberalen Grundrechte zeigt sich auch dadurch, dass nicht nur im StGG die Abwehrrechte gegen den Staat gegenüber anderen Grundrechten klar dominieren; auch in der EMRK sind die liberalen Grundrechte vorherrschend. Nachstehend sollen nun kurz die für diese Arbeit zentralen Grundrechte skizziert werden, um in weiterer Folge mögliche Eingriffe in diese Grundrechte durch die Vorratsdatenspeicherung identifizieren zu können.

1. Recht auf Privatleben

Der Schutz des Privatlebens ist in Artikel 8 der Europäischen Menschenrechtskonvention festgeschrieben. Das Recht auf ein geschütztes Privat- und Familienleben steht in einem engen Zusammenhang mit der *Unverletzlichkeit des Hausrechtes* gemäß Artikel 9 StGG.²⁶

²⁵ Zu der Möglichkeit der Beschränkung der Grundfreiheiten vgl. zB Öhlinger, Verfassungsrecht⁸, Wien 2009, S. 312 ff.

²⁶ Anm.: Auch dieses Grundrecht wird weiter unten noch ausführlich behandelt.

Explizit genannt werden von Artikel 8 EMRK der Anspruch jedermanns auf *Achtung seiner Wohnung und seines Briefverkehrs*.

Eine Definition dessen, was unter *Privatleben* zu verstehen ist, bietet das die EMRK jedoch nicht. Zweifelsohne bezieht sich der Begriff „Privatleben“ auf die persönliche, intime Sphäre eines Menschen.

Anders gesagt handelt es sich um jenen Lebensbereich, der nicht öffentlich stattfindet. Doch selbst diese Definition ist nicht wirklich zufriedenstellend; so können unter Umständen auch Interaktionen, die in einem öffentlichen Kontext stattfinden, Teil des Privatlebens sein.²⁷

Der Verwaltungsgerichtshof versteht unter „Privatleben“ die intime Sphäre eines Menschen, „in der er seinen spezifischen Interessen und Neigungen nachgeht, die Ausdruck seiner Persönlichkeit sind.“²⁸ Davon erfasst sind auch Beziehungen zu anderen Menschen, nicht bloß innere Vorgänge.

Das Recht auf ein geschütztes Privatleben umfasst vor allem den Anspruch der/des Einzelnen, den Staat von einzelnen Bereichen ihres/seines Lebens auszuschließen und ihm den Einblick in diese Bereiche zu verwehren.

Die Möglichkeiten, jemandes Recht auf ein geschütztes Privat- und Familienleben zu verletzen, sind ebenso vielseitig wie die einzelnen Facetten des Privatlebens.

Die Kenntnissnahme von staatlicher Seite, die Überwachung oder die Kontrolle reichen bereits aus, um die Privatsphäre einer Person zu verletzen.

Zulässigkeit von Beschränkungen des Grundrechts?

Dementsprechend behutsam muss auch vorgegangen werden, wenn in das Recht eingegriffen wird. In der EMRK ist mittels eines materiellen Gesetzesvorbehalts ausdrücklich normiert, unter welchen Umständen *eben doch* von staatlicher Seite Einfluss genommen werden darf. Hervorzuheben ist hier vor allem die *nationale Sicherheit, die öffentliche Ruhe und Ordnung*. Genannt werden weiters das *wirtschaftliche Wohl des Landes*, und die *Verhinderung von strafbaren Handlungen, der Schutz der Gesundheit und der Moral* sowie der *Schutz der Rechte und Freiheiten anderer*.²⁹

²⁷ Hengstschläger/Leeb, Grundrechte, Wien 2012, S. 157.

²⁸ Erkenntnis des Verwaltungsgerichtshofes vom 30.09.1997, VwSlg 14748 A/1997.

²⁹ Vgl. dazu Artikel 8 Absatz 2 EMRK.

2. *Hausrecht, Schutz der Wohnung*

Der Schutz des Hausrechts (Artikel 9 StGG) steht in engem Zusammenhang mit dem Recht auf Privatsphäre, wobei der allgemeine Anspruch auf Achtung der Wohnung von Artikel 8 EMRK umfasst ist.³⁰ Auch das Hausrecht soll den persönlichen Lebensraum von Personen schützen und ist demnach ein liberales Grundrecht, das den staatlichen Einfluss und auch den Einblick des Staates in den privaten Lebensbereich zurückdrängen soll. Das Hausrecht schützt mitunter vor willkürlichen Hausdurchsuchungen.

Zulässigkeit von Beschränkungen des Grundrechts?

Grundsätzlich sind Eingriffe in das Hausrecht immer dann möglich, wenn ein richterlicher Befehl für eine Hausdurchsuchung vorliegt. Doch auch, wenn ein solcher nicht vorhanden ist, kann unter Umständen eine Hausdurchsuchung zulässig sein, nämlich zum Zweck der Strafrechtspflege immer dann, wenn Gefahr im Verzug herrscht und nicht die Zeit bleibt, um einen richterlichen Befehl zu erwirken.

3. *Grundrecht auf Datenschutz*

Das Datenschutzgesetz 2000 (DSG) beinhaltet eine Verfassungsbestimmung, welche die Überschrift „Grundrecht auf Datenschutz“ trägt. Dieses Grundrecht bezieht sich auf den Schutz personenbezogener Daten, „soweit ein schutzwürdiges Interesse daran besteht“.³¹ Bereits in Absatz 2 derselben Bestimmung sind jedoch diverse Ausnahmen von dieser Grundregel normiert. Was unter einem schutzwürdigen Interesse zu verstehen ist, lässt sich nicht ganz eindeutig aus dem Gesetz herauslesen.

³⁰ Hengstschläger/Leeb, Grundrechte, Wien 2012, S. 176.

³¹ Vgl. dazu Datenschutzgesetz 2000, § 1.

Auf den ersten Blick mag die Frage, worum es sich bei *personenbezogenen* Daten handelt, unkompliziert erscheinen. Diese wird vom Gesetz jedoch nicht abschließend geklärt und muss somit Schritt für Schritt durch die Rechtsprechung bestimmt werden.

Eine weitere wichtige Unterscheidung, die das Gesetz in Hinblick auf das Grundrecht auf Datenschutz trifft, ist jene zwischen *sensiblen* und *nicht sensiblen* Daten, wobei das Gesetz hier in § 4 eine Definition anbietet:

Demnach sind *sensible Daten* (oder *besonders schutzwürdige Daten*) „Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben.“³²

Zulässigkeit von Beschränkungen des Grundrechts?

Diese Unterscheidung ist deshalb so bedeutsam, weil für die Verwendung sensibler Daten weit strengere Auflagen gelten, als für die Verwendung nicht sensibler Daten. Anders gesagt: bei der Verwendung sensibler Daten ist das schutzwürdige Geheimhaltungsinteresse einer Person ausschließlich dann nicht verletzt, wenn die betroffene Person beispielsweise die Daten selbst öffentlich macht.

Doch das Gesetz zählt durchaus auch andere Fälle auf, in denen sensible personenbezogene Daten verwendet werden dürfen, wie beispielsweise immer dann, wenn es um die Wahrung eines wichtigen öffentlichen Interesses geht, oder etwa die Verwendung der Daten zur Wahrung eines lebenswichtigen Interesses einer anderen Person notwendig ist.³³

Kein schutzwürdiges Interesse im Sinne des Grundrechts auf Datenschutz gemäß § 1 DSG besteht an Daten, wenn „Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.“

4. Kommunikationsfreiheit

³² Datenschutzgesetz 2000, § 4 Z 2.

³³ Für eine vollständige Auflistung der normierten Ausnahmen vgl. Datenschutzgesetz 2000, § 9.

Das Grundrecht auf Kommunikationsfreiheit ist sowohl in Artikel 13 StGG, als auch in Artikel 10 EMRK normiert. Nach dem Staatsgrundgesetz hat jeder das Recht, „*durch Wort, Schrift, Druck oder durch bildliche Darstellung seine Meinung innerhalb der gesetzlichen Schranken frei zu äußern.*“³⁴ Weiters ist auch die Zensur der Presse verboten.

Die EMRK formuliert die Kommunikationsfreiheit noch weiter: Gemäß Artikel 10 („*Freiheit der Meinungsäußerung*“) hat jedermann Anspruch auf freie Meinungsäußerung, wobei sowohl der Empfang, als auch die Mitteilung von Nachrichten oder Ideen ohne Eingriffe öffentlicher Behörden und ohne Rücksicht auf Landesgrenzen umfasst sind.³⁵

Zulässigkeit von Beschränkungen des Grundrechts?

In der Menschenrechtskonvention ist ausdrücklich normiert, dass das Grundrecht auf freie Meinungsäußerung eingeschränkt werden darf, sofern dies *im Interesse der nationalen Sicherheit, der territorialen Unversehrtheit oder der öffentlichen Sicherheit, der Aufrechterhaltung der Ordnung und der Verbrechensverhütung, des Schutzes der Gesundheit und der Moral, des Schutzes des guten Rufes oder der Rechte anderer unentbehrlich ist.*³⁶

³⁴ Staatsgrundgesetz 1867, Artikel 13.

³⁵ Vgl. Europäische Menschenrechtskonvention, Artikel 10 Abs 1.

³⁶ Europäische Menschenrechtskonvention, Artikel 10 Abs 2.

3. Sicherheit und Staat

Nach der Analyse der Bedeutung des Begriffes „Freiheit“ soll nunmehr der zweite Begriff erläutert werden, der das Spannungsfeld, in dem sich die Verfassung befindet, begründet: Die Sicherheit.

Die Faktoren, die ein staatliches System aus der Balance bringen können, sind vielfältig; die Vielfalt der Maßnahmen, die für den Schutz eines Staates ergriffen werden, orientiert sich daher an den Gefahren.

Im Folgenden soll ausschließlich auf jene Gefahren eingegangen werden, die durch kriminelle Aktivitäten hervorgerufen werden und somit eine strafrechtliche Relevanz aufweisen.

Hier ist zwischen der äußeren und der inneren Sicherheit eines Staates zu unterscheiden. Die „öffentliche Sicherheit“ ist diejenige, die der Staat im öffentlichen Interesse nach Maßgabe des objektiven Rechts gewährleistet.

Sie erfasst alle Angelegenheiten des Gemeinwesens. Während die „äußere Sicherheit“ als Teil der öffentlichen Sicherheit im tradierten Sinne die Landesverteidigung betrifft, umfasst die innere Sicherheit ursprünglich den gesamten Bereich der Zuständigkeiten der Polizei, des Verfassungsschutzes und des Katastrophenschutzes.³⁷

Die äußere Sicherheit:

Seit Entstehung der Nationalstaaten ist die äußere Sicherheit derselben immer wieder ein wichtiges Thema.

Im Zentrum steht die Verteidigung eines Staates gegenüber Angriffen von außen, also Angriffen von anderen Staaten, durch welche die Souveränität des Staates verletzt wird. Lange Zeit handelte es dabei um einen Bereich, der kaum strafrechtlich relevant war; abgesehen von den jüngeren Entwicklungen der (internationalen) Kriegsverbrechertribunale war der Schutz nationaler Grenzen und deren Unversehrtheit primär, und fast ausschließlich, die Aufgabe des Militärs.

³⁷ Simon, Präzeptoraler Sicherheitsstaat und Risikovorsorge. Frankfurt am Main 2008, S. 146.

Die innere Sicherheit:

Demgegenüber ist für die innere Sicherheit eines Staates traditionell die Polizei im weitesten Sinne zuständig. Der Begriff der Polizei ist differenziert zu sehen, die Organisationsstruktur ist so komplex und wird auch immer wieder verändert, sodass die Abgrenzung der Zuständigkeiten und die Unterscheidung zwischen Verwaltungs- und Sicherheitspolizei, Orts- und überörtlicher Polizei und der Spezialkommanden nicht ganz einfach ist. Eines haben jedoch alle Einheiten, die unter den Polizeibegriff fallen, gemein: Ihre Aufgabe – im weitesten Sinne – ist es, die innere Sicherheit eines Staates zu schützen.

Die ursprüngliche Zweiteilung zwischen innerer und äußerer Sicherheit verschwimmt jedoch zusehends: Angriffe von außen sind längst nicht mehr bloß durch physische Angriffe möglich, und werden oftmals nicht mehr durch Armeen ausgeführt. Neue Technologien eröffnen unzählige neue Möglichkeiten, wenn es darum geht, regen Informationsaustausch zu betreiben und Lücken in Sicherheitssystemen zu finden.

Ausdrücke wie „Cyberwar“ lassen erahnen, dass die Bedrohungsszenarien für Staaten sich längst geändert haben und dass somit auch ihre Bekämpfung nicht mehr ausschließlich mit traditionellen Mitteln stattfindet.

Die Rolle, die der Polizei in diesem Bereich zukommt, sollte nicht unterschätzt werden. Längst umfasst Polizeiarbeit die Wahrung der inneren und der äußeren Sicherheit, kurz, die Aufgabe der Polizei ist es, jegliche Gefahren für die öffentliche Sicherheit und Ordnung abzuwehren.³⁸ Allgemeiner ausgedrückt ließe sich sagen, die Grundidee ist die Wahrung des staatlichen Wohls.

Die Ordnung und Sicherheit in einem Staat zu wahren ist notwendigerweise damit verbunden, dass gewisse Kompromisse eingegangen werden, bestimmte Freiheiten beschränkt, und strenge Regeln auferlegt werden müssen:

„Innere Freiheit und der Bestand der freiheitlichen Demokratie bedingen einander; denn das eine ist ohne das andere nicht denkbar. Beides ist somit von vornherein in der Verfassung angelegt. Äußere Sicherheit und innere Freiheit stehen aber in einem natürlichen Spannungsverhältnis, als ihre Tendenzen diametral ausgerichtet sind. Das eine wird stets das Bestreben haben, das andere zurückzudrängen. Dieses Verhältnis permanenter Spannung muß im Einzelfall durch die Zuordnung

³⁸ Noll, Sicherheitsstaat Österreich? Kritik der Sicherheitsgesetzgebung. ÖVDJ, Wien 1991, S 27.

beider Größen unter Beachtung des durch die Verfassung selbst vorgezeichneten Rahmens des umfassenden Staatswohls aufgelöst werden. Das *salus rei publicae* liegt in einem freiheitlich demokratischen Rechtsstaat in der optimalen inneren Freiheit bei optimaler äußerer Sicherheit.“³⁹

Beim Versuch die Frage zu beantworten, *wie* die Sicherheit gewahrt werden soll, welche Methoden zulässig sind, und welche Funktion dabei dem Strafrecht zukommen soll, stellen sich noch mehr Fragen betreffend die wichtigste Funktion der Verfassung. Die Existenz des Staates selbst und das Vorhandensein geordneten sozialen Lebens beruht auf der Aufrechterhaltung der Rechtsordnung.⁴⁰ Um die staatliche Sicherheit zu gewährleisten kommt den strafrechtlichen Sanktionen eine wichtige Bedeutung zu.

a) Der hohe Preis für mehr Sicherheit

Das komplexe Verhältnis zwischen Freiheit und Sicherheit ist vor allem durch Widersprüchlichkeiten geprägt. Der Begriff „Sicherheit“ wird im täglichen Gebrauch zumeist als Gegenbegriff zu „Kriminalität“ gesehen. Wird im Zusammenhang mit der Vorratsdatenspeicherung von „Sicherheit“ gesprochen, so ist auch in diesem Fall das Gegenstück zu Verbrechen im weitesten Sinne – sei es organisierte Kriminalität oder Terrorismus – gemeint.

Der Gegenbegriff von Sicherheit ist jedoch nicht Kriminalität, sondern Unsicherheit.⁴¹ Die größte Ironie hinsichtlich der Vorratsdatenspeicherung besteht wohl darin, dass ihre Intention, wie auch aus der Präambel der Richtlinie zur Vorratsdatenspeicherung hervor geht, eigentlich darin besteht, für mehr Sicherheit zu sorgen, und zwar sowohl für mehr innere, als auch mehr äußere Sicherheit. Das Resultat ist jedoch vor allem die Unsicherheit der Betroffenen.

Mit mehr Sicherheit sind diverse trade-offs verbunden, da der Staat die Freiheit seiner Bürger innen und Bürger nur dann garantieren kann, wenn er in diese Freiheit auch eingreift. Es muss „zwischen Freiheit vom Staat und Freiheit durch den Staat oder, umgekehrt ausgedrückt,

³⁹ Ahrens, Der Beginn des Staatsgeheimnisses im deutschen und ausländischen Staatsschutzrecht. Hamburg 1966, S. 86.

⁴⁰ Blumenthal, Staatsidee und Strafzweck, Saalfeld 1935, S. 1.

⁴¹ Erwin Weissel, Sicherheit um jeden Preis? ZfRV 1998, S. 109 ff.

Sicherheit vor dem Staat und Sicherheit durch den Staat ein ausgewogenes Verhältnis“⁴² hergestellt werden.

Beachtlich ist auch, dass im Wirtschaftsbereich immer öfter der Ruf nach Liberalisierung laut wird. Immer mehr traditionell staatlich gelenkte Sektoren werden privatisiert, während es gleichzeitig offenbar für notwendig gehalten wird, dass der Staat zur Herstellung der inneren Sicherheit immer mehr Kompetenzen an sich zieht.

Diese Ausweitung der staatlichen Kompetenzen wird insbesondere durch eine Erweiterung polizeilicher Befugnisse zum Ausdruck gebracht. Diese führt dazu, dass Eingriffe in die Privatsphäre im Namen der Sicherheit rechtlich zulässig sind.

Es entsteht mitunter der Eindruck, das Sicherheitsargument würde des Öfteren von Seiten des Gesetzgebers dann eingesetzt, wenn es einfach keine anderen Argumente gibt, die für einen bestimmten Rechtsakt sprechen würden beziehungsweise wenn es solche Argumente zwar gibt, diese aber für die Bürgerinnen und Bürger keinen hohen Stellenwert haben.

Das Sicherheitsargument spielt vor allem mit den Ängsten der Betroffenen, und ist bereits einzig und allein aus diesem Grund bedenklich.

b) Ein Einblick in die Strafrechtstheorie

Wie eingangs bereits angesprochen, sind die Aufgaben des Staates vielfältig. Betrachtet man nun nur eine einzige Funktion, nämlich die Schutzfunktion im weitesten Sinne, so stehen die Maßnahmen des Staates in direktem Zusammenhang mit den Gefahren und Bedrohungen, mit denen er sich konfrontiert sieht. Jede Zeit weist ihre eigenen, für sie typischen Probleme auf. Die gesetzten Maßnahmen sind die Antwort auf diese Gefahren.

Um Kriminalität gezielt bekämpfen zu können, bedarf es der näheren Betrachtung der Wurzel des Problems. Es gibt Gefahren, die zu jeder Zeit existieren und existiert haben, und den inneren Systemfrieden gefährden.

Zu nennen wäre hier beispielsweise das Delikt des Diebstahls. Selbstverständlich steht auch ein solcher „Klassiker“ des Strafrechts in irgendeinem Zusammenhang mit den

⁴² Erwin Weissel, Sicherheit um jeden Preis? ZfRV 1998, S. 109 ff.

gesellschaftlichen Gegebenheiten: Wenn ein Land mit sehr ungleichmäßiger Vermögensverteilung eine sehr hohe Diebstahlsrate aufweist, wird das niemanden überraschen, da überproportional viele Diebstähle damit erklärt werden könnten, dass eben ein Fehler im System dazu führt, dass sich Menschen dazu gezwungen sehen, durch Beschaffungskriminalität ihr Leben zu sichern. Eine außergewöhnlich hohe Diebstahlsrate in einem Land mit sehr ungleicher Güterverteilung wäre ein „spezifisches“ Problem, dass es an einem spezifischen Ort zu einer spezifischen Zeit gibt, und für das eine spezifische Lösung gefunden werden muss.

Diebstähle werden jedoch nicht nur in Ländern mit außergewöhnlicher Verteilungsungerechtigkeit begangen, und vor allem nicht ausschließlich von Menschen, die von dieser Verteilungsungerechtigkeit am schlimmsten betroffen sind. Um Kriminalität effektiv bekämpfen zu können, muss zunächst hinterfragt werden, worauf sie zurückzuführen ist.

Wenn beispielsweise in Österreich ein Student, der keinen Respekt vor dem Eigentum anderer hat, ein Buch aus der Unibibliothek stiehlt, so kann die Androhung einer 6-monatigen Freiheitsstrafe für Diebstahl durchaus dazu führen, dass sich besagter Student gut überlegt, ob er sich das Buch nicht doch lieber ausleiht.

Die bloße Androhung einer solchen Sanktion hat bereits einen *präventiv* abschreckenden Effekt und wird sicherlich auch dazu betragen, dass weniger gestohlen wird, als dies wohl der Fall wäre, wenn es gar keine Sanktion geben würde.

Das Androhen einer 6-monatigen Freiheitsstrafe hält jedoch in einem Land mit tausenden hungernden Menschen wohl kaum jemanden davon ab, Lebensmittel zu stehlen, da die Risikobereitschaft dafür, beim Diebstahl erwischt zu werden und eingesperrt zu werden, verständlicherweise in einem solchen Fall eine andere ist.

Dieses – zugegebener Maßen sehr vereinfachte – Beispiel zeigt, dass ein und dasselbe Delikt unter Umständen nur durch sehr unterschiedliche Maßnahmen effektiv bekämpft werden kann. Während der Buchdieb mit einer „schädlichen Neigung“, wie dies im Strafrecht bezeichnet wird, sehr wohl durch eine Haftstrafe von seiner Tat abgehalten werden kann, können Eigentumsdelikte, deren Grund Hunger oder große Armut ist, nicht auf eine solche „schädliche Neigung“ zurückgeführt werden und können daher nicht durch Androhung einer Freiheitsstrafe verhindert werden.

Während es im ersten Fall die Aufgabe des Staates ist, dem Täter sein unrechtes Handeln durch Strafe vor Augen zu führen, so ist es im zweiten Fall die Aufgabe des Staates dafür zu sorgen, dass die Armut bekämpft wird.

Staatliche Sanktionen in der Gestalt von Strafen sind nur dann sinnvoll, wenn sie auch dazu geeignet sind, jemanden von seiner Tat abzuhalten oder ihn zumindest an der Wiederholung der Tat zu hindern. Jede Strafe braucht eine Rechtfertigung. Worin diese Rechtfertigung besteht, wird jedoch nicht überall gleich beurteilt: „Der Strafzweck und die sittliche Rechtfertigung der Strafe, die Art ihrer Ausgestaltung, alle diese Fragen sind in ihrer jeweils gültigen Lösung weltanschaulich bedingt.“⁴³

c) Die absoluten Straftheorien

Der so genannten „absoluten Straftheorie“ liegt der Vergeltungsgedanke im Zentrum, die den Sinn einer Strafe ausmache. Im deutschen Idealismus erlangte sie im 19. Jahrhundert eine besonders herausragende Bedeutung: „Die Strafe solle nicht deshalb verhängt werden, weil sie verschuldet sei, sie müsse verhängt werden, *weil der Täter verbrochen habe* – um der Gerechtigkeit willen.“⁴⁴

In vergeltungstheoretischen Überlegungen finden präventive Gedanken keinen Platz. Kant meint, die Strafe, die über einen Täter zu verhängen ist, müsse dem Leid entsprechen, das der Täter angerichtet hat. Hegel sieht den Sinn der Strafe für die Gemeinschaft darin, dass durch die Strafe das Verbrechen, welches den „allgemeinen Willen“, gemeint ist die Rechtsordnung, negierte, aufgehoben und somit gezeigt wird, dass das Verbrechen, das ansonsten gelten würde, keine Geltung hat. Es sei das „Aufheben des Verbrechens insofern Wiedervergeltung, als sie dem Begriffe nach Verletzung der Verletzung ist.“⁴⁵

Die absoluten Straftheorien und die für sie zentrale Bedeutung der Vergeltung, sind heute längst überholt. Obwohl Vergeltung sicherlich immer wieder als Begriff im Strafrecht auftaucht, ist sie nicht mehr der Grund für die Strafe. Im Zentrum steht vielmehr der Schutz der Gesellschaft, die Bewahrung einer gewissen Ordnung, der Rechtsfriede, die

⁴³ Dahm/Schaffstein, Liberales oder autoritäres Strafrecht, Saalfeld 1935, S. 2.

⁴⁴ Ebner in WK² Vor §§ 32–36, Rz 6.

⁴⁵ Hegel, Grundlinien der Philosophie des Rechts, zit. in Ebner in WK² Vor §§ 32–36 Rz 6.

Sicherheit der Personen. Bedeutsam sind die absoluten Straftheorien, wenigstens im weiteren Sinn, jedoch noch immer insofern, als sie einen Maßstab für die Höhe einer Strafe darstellen.

Wenn in Anbetracht der absoluten Straftheorien die Höhe der Strafe dem Leid entsprechen solle, welches die Täterin/der Täter verursacht hat, so wird nunmehr primär an der Schuld des Täters angeknüpft. Ist die Schuld einer Täterin/eines Täters als gering einzustufen, so ist seine Strafe auch zu mildern.

d) Die relativen Straftheorien

Die heute bedeutsamen relativen Straftheorien lassen den Vergeltungsgedanken immer mehr aus dem Fokus rücken, und konzentrieren sich dafür umso mehr auf präventive Überlegungen: Prävention ist das „Zauberwort nicht nur polizeilicher Arbeit“ sondern zunehmend auch der rechtlichen Steuerungstheorie.⁴⁶

Dies soll durch Strafen erreicht werden, die einerseits auf den Einzelnen einwirken (Spezialprävention), sowie auch auf die Allgemeinheit (Generalprävention). Es geht dabei darum, den Täter/die Täterin bzw. andere Personen durch die (Androhung einer) Strafe von der zukünftigen Begehung beziehungsweise der Wiederholung einer Straftat abzuhalten.

Auch diese Ansätze sind nicht ganz neu: Bereits Paul Anselm von Feuerbach griff den Gedanken der Generalprävention auf und entwickelte die Generalpräventionstheorie des psychologischen Zwanges. Demnach soll die Strafe so abschreckend wirken, dass sie stärker wirkt als die potentiell vorhandene Bereitschaft oder der wie auch immer geartete Wille einer Person, eine gewisse Straftat zu begehen. Bei Feuerbach liegt das fruchtbare Moment der Abschreckung in der Drohung.⁴⁷

Damit potentielle Straftäter jedoch eine Strafe ernst nehmen, ist nicht nur ihre Androhung, sondern auch die Verhängung und Vollstreckung derselben notwendig. Generalprävention bedeutet in gewisser Weise auch immer, dass die Bestrafung eines Täters mit dem Zweck verbunden ist, andere von der Begehung derselben Straftat abzuschrecken.⁴⁸ Insoweit dienen

⁴⁶ Noll, Sicherheitsstaat Österreich? Kritik der Sicherheitsgesetzgebung, OVDJ, Wien 1991, S. 11.

⁴⁷ Blumenthal, Staatsidee und Strafzweck, Saalfeld 1935, S. 19.

⁴⁸ Ebner in WK² Vor §§ 32–36 Rz 12.

die generalpräventiven Überlegungen, die hinter einer Strafe stehen auch immer dazu, ein Exempel zu statuieren.

Dass der erwünschte Abschreckungseffekt auch tatsächlich eintritt ist, wie bereits oben kurz angesprochen, jedenfalls in Zweifel zu ziehen. Ein solcher Abschreckungseffekt der so genannten „negativen Generalprävention“ ist nicht empirisch nachweisbar. Dennoch wird davon ausgegangen, dass Generalprävention, und zwar die positive, einen Effekt auf die Rechtstreue der Bevölkerung hat.⁴⁹

Die generalpräventiven Überlegungen werden durch spezialpräventive komplettiert: Dadurch soll ein nicht besserungsfähiger Gelegenheitstäter abgeschreckt, der besserungsfähige Zustandsverbrecher resozialisiert, und der unverbesserliche Gewohnheitsverbrecher unschädlich gemacht werden.⁵⁰ Dabei spielt die Persönlichkeit des Täters eine zentrale Rolle. Sowohl general- als auch spezialpräventive Faktoren spielen eine Rolle für den Strafraum, der vom Gesetzgeber für die einzelnen Delikte vorgegeben wird. Dieselben Überlegungen fließen auch in die Entscheidungsfindung des Gerichtes ein.

In jedem Fall ist die Bestrafung des Bösen nicht als Selbstzweck zu sehen. Der Zweck der Strafe liegt vielmehr auf dem Nutzen derselben, das Böse abzuschrecken oder es unmittelbar daran zu hindern, den Frieden zu stören.⁵¹

e) Das Zusammenwirken von Polizei und Gericht

Die Legitimierung von Strafen, der Gedanke, der hinter dem Strafrecht steht, wäre somit in groben Zügen erklärt. Ein effektives Strafrecht und die Sanktionierung von Straftaten sind ohne ein funktionierendes Polizeisystem undenkbar.

„Die Sicherheitspolizei soll die Aufrechterhaltung der ‚öffentlichen Ordnung‘ garantieren. Mit ‚öffentlicher Ordnung‘ wird üblicherweise die Gesamtheit jener Normen umschrieben,

⁴⁹ Ebner in WK² Vor §§ 32–36 Rz 13.

⁵⁰ Ebner in WK² Vor §§ 32–36 Rz 16.

⁵¹ Larenz, Rechtsidee und Strafrechtsgedanke, Berlin 1930, S. 79.

deren Befolgung nach den jeweils herrschenden Anschauungen als unentbehrliche Voraussetzungen für ein gedeihliches Zusammenleben der Bürger angesehen wird.“⁵²

Typischerweise obliegt es der Polizei, Straftaten aufzudecken, die Verdächtigen zu verfolgen und die notwendigen Ermittlungen anzustellen. Diese werden der Staatsanwaltschaft und dem Gericht übermittelt, um diesen als solide Grundlage für die Verhängung von Strafen zu dienen. Es obliegt letztlich den Gerichten zu entscheiden, welche Strafe zu verhängen ist. Welche Mittel für das Ausforschen und Stellen von Straftätern verwendet werden dürfen, wird primär vom Gesetzgeber bestimmt, wobei auch den Strafgerichten eine nicht unwesentliche Rolle zukommt, wenn es um Eingriffe in das Privatleben von Personen geht. Um bestimmte Aktionen setzen zu dürfen, muss die Polizei zunächst eine gerichtliche Bewilligung anfordern. Doch die Befugnisse der Exekutive sind weit, vor allem, was die Sicherheitspolizei betrifft.

Präventive Eingriffe in das Privatleben und die Freiheit von Personen können mitunter bereits durch das Vorliegen bestimmter Indizien gerechtfertigt sein. Es scheint, als würde die Strafe als Reaktion auf Straftaten immer mehr von präventiver Freiheitsbeschränkung abgelöst. Es kommt zu einer Art Vorverlagerung der Verbrechensbekämpfung und zu einer Beschränkung der Bürgerfreiheit durch Polizeigewalt, die darauf abzielt, die Abwehr von Gefahren vorzubereiten.⁵³

Es scheint, als sei, wo Erziehung versagt, Sicherung als kriminalpolitisches Bekämpfungsmittel umso mehr gefragt.⁵⁴

Immer mehr wird der Täter als „Feind“ statt als „Bürger“ wahrgenommen, wodurch eine Annäherung zum so genannten „Feindstrafrecht“ als nicht unrealistisch erscheint. Im Strafrecht wird ein Täter entweder als Bürger definiert, der über eine strafrechtsfreie interne Sphäre verfügt, in welche das Recht „erst eindringen kann, wenn sich der Täter extern störend verhält“, oder der Täter gilt als Feind, als Gefahr für Rechtsgüter.

Somit wird er zu jemandem, der über keine Privatsphäre verfügt, sondern auch für seine „innigsten Gedanken zur Verantwortung gezogen werden kann“.⁵⁵ Dass jedoch bereits bestimmte Vorbereitungen oder gar Gedanken, die sich noch gar nicht in konkreten

⁵² Noll, Sicherheitsstaat Österreich? Kritik der Sicherheitsgesetzgebung, ÖVDJ, Wien 1991, S. 54.

⁵³ Noll, Sicherheitsstaat Österreich? Kritik der Sicherheitsgesetzgebung. ÖVDJ, Wien 1991, S. 30.

⁵⁴ Sauer, Allgemeine Strafrechtslehre, Berlin 1949, S. 9.

⁵⁵ Greco, Feindstrafrecht, Baden-Baden 2010, S. 13.

Vorbereitungshandlungen manifestiert haben, zur Strafbarkeit führen sollen, ist durchaus kritisch zu sehen.

Lässt sich dies durch eine bloße potentielle Gefahr rechtfertigen oder durch die Möglichkeit, dass eine konkrete Straftat in der Zukunft gesetzt werden könnte? Woran sich eine spezifische Rechtsfolge in einem solchen Fall anknüpft, ist fraglich: „Jede Rechtsverletzung ist eine unwiderrufliche Tatsache und gerade als solche die Bedingung der spezifischen Rechtsfolge.“⁵⁶ Worin die Rechtsverletzung vor Schadenseintritt begründet sein soll, ist nicht einfach zu erklären.

Während dem Gericht traditionellerweise die Funktion als Rechtsschutzinstitution zukam⁵⁷, scheint die Polizei immer mehr Befugnisse zu erhalten, immer mehr das Ermittlungsverfahren zu kontrollieren, und letztlich somit auch die Beweiswürdigung maßgeblich zu beeinflussen. Gerade dies ist für das Feindstrafrecht kennzeichnend, dessen markantestes Merkmal wohl die Vorverlagerung strafrechtlicher Verbote ist, sowie die Beschneidung rechtsstaatlicher Verfahrensgarantien.⁵⁸

Dies führt mitunter zu massiven Eingriffen in die Privatsphäre, die nur schwer rechtfertigbar sind. Dass solche Einschränkungen mitunter von den Bürgern akzeptiert werden, liegt an deren eigenem Interesse an starken öffentlichen Institutionen, welche das gesellschaftliche Normen- und Ordnungsgefüge sichern sollen.⁵⁹ Werden von den Bürgern Gefahren wahrgenommen oder gewisse Situationen als Bedrohung empfunden, so führt dies mitunter zur Bereitschaft, die Einschränkung der eigenen Freiheit in gewissem Maße hinzunehmen, um im Gegenzug ein Gefühl der Sicherheit zu erhalten.

Auch das polizeiliche Handeln ist auf konkrete Gefahren beschränkt. Je weiter also der Begriff der Gefahr bestimmt wird, desto mehr Eingriffe sind gerechtfertigt. Ein enger Begriff der Gefahr hingegen führt dazu, dass Bürger verhältnismäßig wenig in ihren Rechten beschränkt werden. Man spricht dann von einem freiheitlichen Rechtsstaat.⁶⁰

⁵⁶ Flechtheim, Hegels Strafrechtstheorie, Brunn 1936, S. 92.

⁵⁷ Noll, Sicherheitsstaat Österreich? Kritik der Sicherheitsgesetzgebung. ÖVDJ, Wien 1991, S. 37.

⁵⁸ Vgl. Greco, Feindstrafrecht, Baden-Baden 2010, S. 16.

⁵⁹ Vgl. Schönert, Literatur und Kriminalität, Tübingen 1983, S. 49.

⁶⁰ Simon, Präzeptoraler Sicherheitsstaat und Risikoversorg, Frankfurt am Main 2008, S. 148.

4. Beschränkung des liberalen Prinzips – Beispiel Vorratsdatenspeicherung

Nach der theoretischen Auseinandersetzung mit dem liberalen Prinzip der Verfassung und den liberalen Grundrechten, sowie den Grundzügen des österreichischen Strafrechtes, wird nunmehr auf die Problematik der Vorratsdatenspeicherung eingegangen.

Diese stellt, wie nachfolgend gezeigt wird, einen Eingriff und eine Beschränkung des liberalen Prinzips und der liberalen Grundrechte dar. Ein Preis, der für die „Sicherheit“ gezahlt werden muss? Sicherheit meint „(...) die Gefahrenabwehr und diese wiederum (...) die Abwesenheit von Gefahren, bewirkt durch das staatliche Instrument der Gefahrenabwehr.“

Dies zeigt, dass „(...) der Begriff der Sicherheit stark mit dem Begriff der Gefahr zusammenhängt und darin liegt das Problem zwischen wachsendem Bedürfnis nach Schutzpflicht des Staates gegenüber seinen Bürgern im Widerstreit zum Begriff der Freiheit im Verhältnis zu seinen Bürgern.“⁶¹

Um die Vorratsdatenspeicherung sinnvoll evaluieren zu können genügt es daher nicht, mögliche Eingriffe derselben aufzuzeigen, sondern diese Eingriffe müssen den potentiellen Gefahren gegenübergestellt werden, die durch die Vorratsdatenspeicherung vereitelt werden sollen.

Es zeigt sich, dass es sich als durchaus schwierig gestaltet, einen sinnvollen Ausgleich zwischen dem *Schutz vor Eingriffen des Staates* und *Schutz durch den Staat* zu finden. Dieser Konflikt wird durch Verfassungsgesetze, aber mitunter auch durch das einfache Gesetz gesteuert. Diese sind nicht ausschließlich freiheitsbeschränkend oder freiheitsschützend, sondern sollen einen Ausgleich zwischen den widerstreitenden Interessen darstellen.

Ein zentraler Gedanke dabei ist, dass Freiheit erst durch legislatives Handeln überhaupt geschaffen wird, selbst wenn damit die Beschränkung von naturrechtlicher Freiheit verstanden wird.⁶² Die Freiheit des Einzelnen findet ihre Grenze immer dort, wo die Freiheit eines anderen beschränkt wird. Ohne Gesetze gibt es also auch keine Freiheit.

Dieser komplexe Zusammenhang zwischen und Widerspruch der Begriffe „Freiheit“ und „Sicherheit“ wird auch im Zusammenhang mit der Vorratsdatenspeicherung immer wieder

⁶¹ Simon, Präzeptoraler Sicherheitsstaat und Risikovorsorge, Frankfurt am Main 2008, S. 149.

⁶² Simon, Präzeptoraler Sicherheitsstaat und Risikovorsorge, Frankfurt am Main 2008, S. 175.

thematisiert. Weshalb diese Diskussion überhaupt entbrannt ist, und was zur Gesetzgebung zur Vorratsdatenspeicherung führte, lässt sich durch Geschehnisse auf globaler Ebene erklären.

a) Was ist Vorratsdatenspeicherung

Bevor auf die Entstehungsgeschichte der Vorratsdatenspeicherung in Europa und ihrer späteren Umsetzung in Österreich eingegangen werden kann, stellt sich vorab die – dem Experten vielleicht überflüssig anmutende, für den technisch weniger versierten Laien wiederum essentielle – Frage: Was verstehen wir unter Vorratsdatenspeicherung? Und was sind überhaupt Vorratsdaten?

Es tritt hier bereits ein ganz grundlegendes Problem zu Tage, nämlich, dass die Diskussion um die Vorratsdatenspeicherung zwar von vielen Leuten geführt wird, jeder eine Meinung dazu zu haben scheint, jedoch kaum jemand weiß, was von wem und für welche Zwecke gespeichert wird.

Um allerdings fundierte Diskussionen darüber führen zu können, worin genau das Konfliktpotential der Vorratsdatenspeicherung liegt, muss man jedoch verstehen, worum es bei der Vorratsdatenspeicherung eigentlich geht.

Eine befriedigende Begriffsbestimmung, die eine griffige Definition des Wortes „Vorratsdaten“ gibt, sucht man im Telekommunikationsgesetz (TKG 2003) vergeblich. Im Telekommunikationsgesetz findet sich eine wenig aufschlussreiche juristische Definition, die zwar für rein rechtliche Überlegungen wichtig ist, sich jedoch als wenig hilfreich erweist, wenn es primär darum geht zu verstehen, was Vorratsdaten denn eigentlich genau sind: „Vorratsdaten“ sind demnach „Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a gespeichert werden.“⁶³ Diese Bestimmung erweist sich tatsächlich als relativ aufschlussreich.

Sie erlegt Anbietern von öffentlichen Kommunikationsdiensten die Pflicht auf, Daten ab dem Zeitpunkt ihrer Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern. Bereits im ersten Absatz wird klar normiert, dass diese

⁶³ Vgl. TKG 2003, § 92 Abs 3 Z 6b.

Speicherung ausschließlich zum Zwecke der Ermittlung, Feststellung und Verfolgung von besonders schweren Straftaten erfolgt.

Konkret wird Anbietern von Internetzugangsdiensten die Speicherung von Name, Anschrift, sowie Teilnehmererkennung des Teilnehmers aufgetragen. Diese wird auf Grundlage der zugehörigen IP Adresse ermittelt.

Weiters haben Internetprovider das Datum und die Uhrzeit der Zuteilung und des Entzugs einer Internet-Provider-Adresse (IP-Adresse) zu speichern, sowie die Rufnummer des anrufenden Anschlusses und die Kennung des Anschlusses, über den der Internet-Zugang erfolgt ist. Es sind jedoch nicht nur die Internetprovider, denen vom Gesetzgeber durch das Telekommunikationsgesetz gewisse Speicher- und Aufbewahrungspflichten auferlegt werden. Auch die Anbieter öffentlicher Telefondienste sind Adressaten solcher Pflichten. Ihnen obliegt es, die Teilnehmernummer beziehungsweise Kennung sowohl des Anschlusses, der angerufen wird, als auch des Anschlusses, von dem aus angerufen wird, zu speichern.

Ist beispielsweise eine Rufumleitung aktiviert, so ist auch die Nummer, auf die umgeleitet wird, abzuspeichern. Wie die Internetprovider müssen auch die Anbieter von Telekommunikationsdiensten Name und Anschrift des anrufenden und des angerufenen Kommunikationsteilnehmers aufbewahren.

Datum, Uhrzeit des Beginns und die Dauer der erfolgten Kommunikation sind ebenso zu speichern wie Aufzeichnungen über die Art des in Anspruch genommenen Dienstes.

Bei Mobilfunknetzen sind zusätzlich die so genannte IMSI (die internationale Mobilteilnehmerkennung) des anrufenden und des angerufenen Anschlusses zu speichern, die eine eindeutige Identifizierung von Netzteilnehmern mittels interner Teilnehmerkennung ermöglichen. Darüber hinaus sind die IMEI (*International Mobile Station Equipment Identity* – internationale Mobilfunkgeräteerkennung) beider Kommunikationsteilnehmer zu speichern. Dabei handelt es sich um eine 15-stellige Seriennummer, anhand derer eine eindeutige Identifizierung des Gerätes erfolgen kann. Die Standorterkennung bei Beginn einer Verbindung ist ebenfalls vom Kommunikationsdiensteanbieter zu speichern.

Bei Wertkartenhandys, die ja grundsätzlich anonym sind, muss zusätzlich gespeichert werden, wann bzw wo diese das erste Mal aktiviert wurden.

Die Anbieter von E-Mail Diensten müssen nach dem TKG 2003 die Teilnehmererkennung sowie Name und Anschrift des Teilnehmers, dem eine Mailadresse zugewiesen war oder ist,

speichern. Wird eine E-Mail versandt so ist die E-Mail-Adresse, die IP-Adresse des Absenders, sowie die Mailadresse des Empfängers zu speichern.

Wird eine E-Mail empfangen, so wird die E-Mail Adresse des Absenders, die des Empfängers und dessen IP-Adresse gespeichert. Diese ist auch bei An- und Abmeldung beim E-Mail-Dienst zu speichern, ebenso wie Datum, Zeit und Teilnehmerkennung des Teilnehmers.⁶⁴

Die Bandbreite der Daten, die verpflichtend von E-Mail Providern, Internetdienste-Anbietern und Anbietern öffentlicher Telefondiensten gespeichert werden müssen, lässt erahnen, dass die Kritik an der Vorratsdatenspeicherung und die Befürchtung, mit dieser sei ein weiterer großer Schritt in Richtung „gläserner Mensch“ gesetzt worden, möglicherweise nicht ganz unbegründet ist.

Was mit den eben genannten Daten tatsächlich gemacht werden kann, welche Informationen der Mensch einzig und allein durch das Versenden einer E-Mail oder SMS oder durch die Entgegennahme eines Anrufes von sich preisgibt, ob er will oder nicht, wird zu einem späteren Zeitpunkt noch eingehend thematisiert.

An dieser Stelle sei nur ausdrücklich auf das verwiesen, was bei den umständlichen Formulierungen und bei den sich über zahlreiche Absätze erstreckenden Aufzählungen des §102a TKG beinahe völlig in den Hintergrund tritt: nämlich ein ausdrückliches Verbot der Speicherung des Inhaltes der Kommunikation bzw. der Daten über im Internet aufgerufene Adressen auf Basis dieses Gesetzes.⁶⁵

b) Die Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten

1. Ursprung und Entstehung der Richtlinie

Die Grundlage der gesetzlichen Verankerung der Vorratsdatenspeicherung bildete die Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten (RL 2006/46/EG) der Europäischen Union.

Ein – im Zusammenhang mit der Vorratsdatenspeicherung viel diskutiertes Thema – war die angeblich bereits vor Erlass der Richtlinie oftmals erfolgte Speicherung von Daten durch

⁶⁴ Vgl. TKG 2003, § 102a.

⁶⁵ Vgl. hierzu TKG 2003, § 102a Abs 7.

Provider. Bemerkenswert ist allerdings, dass eine solche auf Basis einer vorangegangenen Regelung aus dem Telekommunikationsbereich, nämlich der Richtlinie 2002/58/EG grundsätzlich keine gesetzliche Grundlage hatte. Vielmehr sah die besagte Richtlinie vor, dass Providern eine Speicherung von Daten nur erlaubt werden dürfe, soweit sie notwendig für die Erbringung des Dienstes oder der Gebührenabrechnung sei.

Dies hätte theoretisch auch bedeutet, dass selbst jene Informationen, die automatisch bei der Kommunikation erzeugt werden, umgehend vom Provider hätten gelöscht werden müssen.⁶⁶ Es herrschte demnach ein Speicherverbot, für das lediglich zu Gunsten der nationalen Sicherheit, der Landesverteidigung, der öffentlichen Sicherheit und zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten Ausnahmen gemacht wurden.⁶⁷ Auf Basis dieser Erlaubnisnorm erließen einige Mitgliedstaaten eigene Speicheranordnungen, die jedoch teils maßgeblich voneinander abwichen.

Den Anstoß für die nunmehrige, umstrittene Richtlinie gaben – wie so oft in derart rasch abgewickelten Gesetzgebungsverfahren – tagespolitische Geschehnisse.

Der Auslöser einer neuen Sicherheitsdiskussion waren die Terroranschläge von London⁶⁸, die sich im Jahr 2005 ereigneten. Obwohl auch vor diesem Zeitpunkt Terrorismus in Europa kein Fremdwort mehr war, schien der moderne Terrorismus dennoch in Anbetracht der Terroranschläge von New York im Jahr 2001 eher mit etwas Fernem assoziiert.

Als sich im Jahr 2004 die Madrider Zuganschläge ereigneten, die an die 200 Todesopfer und mehrere hundert Verletzte zur Folge hatten, wurde bereits ein Rahmenbeschluss für eine solche Richtlinie entworfen. Dieser stieß jedoch auf wenig positive Resonanz, insbesondere auch, was die Rückmeldungen aus dem Europäischen Parlament betraf.⁶⁹

Die systematischen, minutiös geplanten Anschläge in London, die sich zu Zeiten der britischen Ratspräsidentschaft unter dem damaligen Regierungschef Tony Blair ereigneten, zeigten erneut in brutaler Klarheit auf, welche reale Bedrohung der Terrorismus oder allgemeiner gesagt, die organisierte Kriminalität, auch für die Staaten der Europäischen Union ist.

⁶⁶ Vgl. Felsner, Juridikum 2011, 31, S. 1.

⁶⁷ Vgl. RL 2002/58/EG, Art. 15.

⁶⁸ Vgl. hierzu Abs 10 der Präambel der Richtlinie des Europäischen Parlaments und des Rates, RL 2006/24/EG.

⁶⁹ Westphal, Die Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten. Neues aus Brüssel zum Verhältnis von Sicherheit und Datenschutz in der Informationsgesellschaft, Juridikum 2006, 34, S. 1.

Aufgrund der verheerenden Ausmaße des Anschlages, und nicht zuletzt wohl auch aufgrund der geographischen Gegebenheiten, begann ein argumentativer Rekurs auf die Gefahren durch Terrorismus und organisierter Kriminalität.⁷⁰

Unter der österreichischen Ratspräsidentschaft mit Wolfgang Schüssel an der Spitze wurden die Ambitionen, eine Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten zu verabschieden, weiterhin schnell vorangetrieben.

Die Kritik gegenüber einer diesbezüglichen Richtlinie war jedoch dementsprechend groß, wobei die größten Kritikpunkte sich auf die Zahl der zu speichernden Datentypen, sowie die Speicherungszwecke bezogen. Noch unter der britischen Ratspräsidentschaft erreichte man einen Kompromiss und nahm bereits 2005 den vom Rat vorgelegten Richtlinienvorschlag mit deutlicher Mehrheit im Parlament an.⁷¹

Unter der österreichischen Ratspräsidentschaft wurde dieser Richtlinienvorschlag schließlich per Mehrheitsbeschluss durch den Ministerrat der Justiz- und Innenminister im Jahr 2006 angenommen – trotz der umfassenden Kritik, die aus den zahlreichen Mitgliedstaaten zu vernehmen war.

Diese Skepsis bezog sich einerseits auf die Kosten und andererseits darauf, dass durch eine solche Richtlinie alle Unionsbürger pauschal verdächtigt würden. Insbesondere dieses letzte Argument spielt auch in den nationalen Diskussionen rund um die Vorratsdatenspeicherung eine ganz zentrale Rolle.

2. Aufbau und Inhalt der Richtlinie

Wie jede Richtlinie der Europäischen Union beginnt die Richtlinie zur Vorratsdatenspeicherung mit den Beweggründen, die zu der entsprechenden Richtlinie geführt haben. Interessanterweise wird in dieser Präambel vor allem die Bedeutung einer Harmonisierung der Vorratsdatenspeicherung innerhalb der Europäischen Union für den

⁷⁰ Vgl. Westphal, Die Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten. Neues aus Brüssel zum Verhältnis von Sicherheit und Datenschutz in der Informationsgesellschaft. Juridikum 2006, 34. S. 1.

⁷¹ Vgl. Spiegel Online, Verbindungsdaten: EU-Parlament billigt Speicherung, 14.12.2005, verfügbar unter: <http://www.spiegel.de/netzwelt/web/verbindungsdaten-eu-parlament-billigt-speicherung-a-390358.html> (zuletzt abgerufen am: 13.11.2012)

Binnenmarkt hervorgehoben.⁷² Dies sei nur deshalb am Rande erwähnt, da vermutlich in Anbetracht der Diskussionen wohl kaum jemand einen Regelungsbedarf hinsichtlich der Vorratsdatenspeicherung aufgrund des einheitlichen Binnenmarktes vermuten würde.

Die Argumentation basiert vielmehr auf rechtlichen Überlegungen, die mit der damaligen Säulenstruktur der Europäischen Union und die Notwendigkeit einer solchen Richtlinie in Zusammenhang stehen: Es wurde angezweifelt, ob die rechtliche Grundlage für die Richtlinie, und zwar Artikel 95 EG-V (alt) tatsächlich als solche zulässig sei, da diese nur als Basis für Rechtsakte zulässig ist, die tatsächlich die Bedingungen für die Errichtung und das Funktionieren des Binnenmarktes verbessern sollen.⁷³

Dies wiederum ist als Indikator dafür zu sehen, welche politische Bedeutung diesem Thema zu der Zeit nach den Anschlägen in Madrid und London zukam. Aufgrund dieser Überlegungen liegt auch der Schluss nahe, dass der zweite wohl sehr viel schlüssigere Beweggrund, der in der Präambel genannt wird, und der auch Gegenstand dieser Evaluierung ist, in Wahrheit bei Weitem der bedeutsamere war. Dieser geht explizit auf das Thema „Sicherheit“ ein:

„In seinen Schlussfolgerungen vom 19. Dezember 2002 betont der Rat 'Justiz und Inneres', dass die beträchtliche Zunahme der Möglichkeiten bei der elektronischen Kommunikation dazu geführt hat, dass Daten über die Nutzung elektronischer Kommunikation besonders wichtig sind und daher ein wertvolles Mittel bei der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten und insbesondere der organisierten Kriminalität darstellen.“⁷⁴

Weiters heißt es:

„In der vom Europäischen Rat am 25. März 2004 angenommenen Erklärung zum Kampf gegen den Terrorismus wurde der Rat aufgefordert, Vorschläge für Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter zu prüfen.“⁷⁵

Insbesondere in Absatz 9 der Präambel der betreffenden Richtlinie wird nochmals explizit auf die Bedeutung der Vorratsdatenspeicherung für die Zwecke der Strafverfolgung in Fällen

⁷² Vgl. hierzu Abs 5 und Abs 6 der Präambel der Richtlinie des Europäischen Parlaments und des Rates, RL 2006/24/EG.

⁷³ Vgl. Westphal, Dietrich: Die Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten. Neues aus Brüssel zum Verhältnis von Sicherheit und Datenschutz in der Informationsgesellschaft. Juridikum 2006, 34. S. 6.

⁷⁴ Präambel der Richtlinie des Europäischen Parlaments und des Rates, RL 2006/24/EG, Abs 7.

⁷⁵ Präambel der Richtlinie des Europäischen Parlaments und des Rates, RL 2006/24/EG, Abs 8.

organisierter Kriminalität und Terrorismus, jedoch gleichzeitig auch die Grenzen der Vorratsdatenspeicherung zum Ausdruck gebracht:

„(...) Eine Behörde darf in die Ausübung dieses Rechts [Recht auf Achtung des Privatlebens, Anm.] nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist, unter anderem für die nationale oder öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten oder zum Schutz der Rechte und Freiheiten anderer. Da sich die Vorratsspeicherung von Daten in mehreren Mitgliedstaaten als derart notwendiges und wirksames Ermittlungswerkzeug für die Strafverfolgung, insbesondere in schweren Fällen wie organisierter Kriminalität und Terrorismus, erwiesen hat, muss gewährleistet werden, dass die auf Vorrat gespeicherten Daten den Strafverfolgungsbehörden für einen bestimmten Zeitraum unter den in dieser Richtlinie festgelegten Bedingungen zur Verfügung stehen. (...)“⁷⁶

Bereits in dieser Passage lassen sich im Kern die wichtigsten Gründe für, als auch gegen die Vorratsdatenspeicherung herauslesen: Einerseits wird kurz der wertvolle Beitrag, der durch die Speicherung von Vorratsdaten in der Strafverfolgung geleistet werden kann. Andererseits wird der Anwendungsbereich der Vorratsdatenspeicherung implizit auf solche Fälle reduziert, wo dies tatsächlich notwendig ist, weil beispielsweise andere, höherwertige Rechtsgüter auf dem Spiel stehen.

Explizit erwähnt sei jedoch noch zusätzlich, dass nach der Präambel, also im operativen Teil der Richtlinie, als Zweck der Vorratsdatenspeicherung immer die Ermittlung, Feststellung und Verfolgung schwerer Straftaten genannt wird, jedoch die Konkretisierung in Richtung „Terrorismus“ bzw. „organisierter Kriminalität“, wie in der Präambel nicht vorgenommen wird.⁷⁷

Das Spannungsverhältnis zwischen Sicherheit und dem Recht auf Privatleben, also einem liberalen Grundrecht, wird ebenso aufgegriffen wie die Tatsache, dass die Speicherung von Vorratsdaten nicht nur der Verfolgung von Straftaten, sondern auch der Verhütung derselben dienen soll.

Dieser Satzteil ist essentiell in seiner Bedeutung, wenn auch unscheinbar: Durch diesen Ausdruck allein wird klar gezeigt, dass die Vorratsdatenspeicherung und in letzter

⁷⁶ Präambel der Richtlinie des Europäischen Parlaments und des Rates, RL 2006/24/EG, Abs 9.

⁷⁷ Westphal, Die Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten. Neues aus Brüssel zum Verhältnis von Sicherheit und Datenschutz in der Informationsgesellschaft. Juridikum 2006, 34. S. 3.

Konsequenz demnach auch die Verwendung beziehungsweise Auswertung der gespeicherten Daten zwar nicht ausschließlich, aber auch präventiv eingesetzt werden soll.

In Artikel 3 der Richtlinie wird eine Vorratsdatenspeicherpflicht für Anbieter öffentlich zugänglicher Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes konstatiert. Wer zu diesen Daten Zugang erhalten soll, wird in Artikel 4 normiert:

„Die Mitgliedstaaten erlassen Maßnahmen, um sicherzustellen, dass die gemäß dieser Richtlinie auf Vorrat gespeicherten Daten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden.“⁷⁸

Um welche es sich bei diesen „bestimmten Fällen“ handelt, in denen die gespeicherten Daten an die nationalen Behörden weitergegeben werden sollen, wird jedoch nicht weiter ausgeführt. Auch, dass die Mitgliedstaaten bei der Umsetzung der Richtlinie das Völkerrecht, das Unionsrecht und die EMRK zu berücksichtigen haben, bringt keine Konkretisierung der Anforderung.

Schließlich wird in der Richtlinie auf die unterschiedlichen Datentypen eingegangen, die erfasst werden sollen, und als Speicherfrist wird ein Zeitraum von mindestens sechs Monaten bis höchstens zwei Jahren festgelegt. Jedenfalls nicht von der Richtlinie umfasst ist die Speicherung von Inhaltsdaten.

Die Richtlinie wurde am 15.3.2006 beschlossen und sollte wie in Artikel 15 festgelegt – von den Mitgliedstaaten bis spätestens 15.9.2007 umgesetzt werden. Österreich setzte die Richtlinie im April 2012 vollständig um.

c) Die Umsetzung der Vorratsdatenspeicher-Richtlinie in Österreich

Der Schritt vom grundsätzlichen Verbot der Speicherung von Vorratsdaten zur Pflicht derselben wurde auch in Österreich – wenn auch mit einiger Verspätung – vollzogen.

⁷⁸ Richtlinie des Europäischen Parlaments und des Rates, RL 2006/24/EG, Art 4.

Von den Änderungen betroffen waren in Österreich in erster Linie das Telekommunikationsgesetz (TKG 2003) die Strafprozessordnung (StPO 1975) sowie das Sicherheitspolizeigesetz (SPG). Die betreffenden Bestimmungen traten erst am 1.4.2012 in Kraft.

Ogleich es im Vorfeld auch in Österreich massive Bedenken gegen eine vorbehaltlose Umsetzung der Vorratsdatenspeicherrichtlinie gab, die vor allem verfassungsrechtlicher Natur waren, entschied man sich schlussendlich dafür, die erforderlichen gesetzlichen Änderungen vorzunehmen, in Konformität mit der Richtlinie.

Die Umsetzung der Vorratsdatenspeicherungs-Richtlinie wurde schließlich am 28.4.2011 im Nationalrat beschlossen. Ein Grund dafür, dass Österreich sich – wohl oder Übel – dazu durchringen konnte, die erforderlichen Änderungen durchzuführen und sich EU-Rechtskonform zu verhalten, war sicherlich auch die Tatsache, dass Österreich aufgrund seiner Säumigkeit in der Umsetzung der Richtlinie vom EuGH verurteilt worden war.

Es standen auch Strafzahlungen im Raum, was den politischen Druck wesentlich erhöhte.⁷⁹ Die Richtlinie selbst wurde durch eine Novelle zur Änderung des Telekommunikationsgesetzes 2003 umgesetzt, in welcher im Wesentlichen die Bestimmungen der Richtlinie wiedergegeben werden. Zusätzlich gab es Änderungen der österreichischen Strafprozessordnung und des Sicherheitspolizeigesetzes, die sich im Wesentlichen damit auseinandersetzten, unter welchen Umständen auf die gespeicherten Daten zugegriffen werden darf.

Was die Frage betrifft, welche Daten gespeichert werden, sei zur Vermeidung unnötiger Wiederholungen auf das oben bereits Ausgeführte verwiesen.

Die Pflicht zur Speicherung der Daten obliegt – wie bereits kurz angesprochen – Anbietern öffentlicher Kommunikationsdienste. Im Wesentlichen handelt es sich dabei um Internet-Access-Provider, sowie Mobil- und Festnetzprovider.

Nicht von der Pflicht zur Speicherung der Daten umfasst sind wiederum Betreiber öffentlicher Kommunikationsnetze, das heißt all jene, die den Datenverkehr bloß durchleiten, ohne dass eine vertragliche Verbindung zu den einzelnen Nutzern besteht.

Besonders interessant erscheint in diesen Zusammenhang auch die Tatsache, dass bestimmte, kleine Provider ebenfalls von der Speicherpflicht nach dem Telekommunikationsgesetz

⁷⁹ Feiler/Stahov, MR 2011, 111, S.111.

ausgenommen sind.⁸⁰ Dies mag zwar aus praktischen Gründen durchaus gerechtfertigt sein, höhlt jedoch das Argument der Sicherheit aus, auf dem im Grunde ein Großteil der Legitimation der Vorratsdatenspeicherung beruht.

Gemäß § 102a Abs TKG beträgt die verpflichtende Speicherdauer für Vorratsdaten sechs Monate. Einen Monat danach müssen sie gelöscht werden.

Interessanter erscheinen nun jedoch die Regelungen darüber, wann und von wem die so gespeicherten Vorratsdaten *abgefragt* werden dürfen. Die Bestimmungen hinsichtlich der Ansprüche auf Information oder Auskunft über die Datenverwendung finden sich in der Strafprozessordnung.⁸¹

Aufschluss darüber, was die Voraussetzungen für die Auskunftserteilung nach dem Telekommunikationsgesetz sind, gibt vor allem § 102b TKG: „Eine Auskunft über Vorratsdaten ist ausschließlich aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt, zulässig.“⁸²

Die Bestimmung des § 135 Abs 2a StPO vereist wiederum darauf, dass eine Auskunftserteilung über Vorratsdaten ausschließlich aus den Gründen des § 135 Abs 2 Ziffer 2 bis 4 zulässig sind.

Konkret bedeutet dies, dass Vorratsdaten nur dann preisgegeben werden dürfen, „wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt“⁸³ oder „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“⁸⁴ oder „wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich

⁸⁰ Vgl. TKG, § 102a Abs 6: Ausgenommen sind demnach kleine Anbieter, die keinen jährlichen Finanzierungsbeitrag an die Rundfunk und Telekom Regulierungs-GmbH zu leisten haben.

⁸¹ TKG § 102a Abs 9.

⁸² TKG § 102b Abs 1.

⁸³ Strafprozessordnung 1975, § 135 Abs 2 Ziffer 2.

⁸⁴ Strafprozessordnung 1975, § 135 Abs 2 Ziffer 3.

begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann“.⁸⁵

Festzuhalten ist also an dieser Stelle Folgendes: Die Grundregel zum Abruf der gespeicherten Vorratsdaten besagt, dass im Normalfall die Vorratsdaten nur auf Basis einer gerichtlichen Bewilligung durch die Staatsanwaltschaft erfolgen darf. Das heißt, ein Richter muss in den Abruf der Daten einwilligen, und die Staatsanwaltschaft kann auf Basis dieser Einwilligung die entsprechende Anordnung treffen.

Diese Einwilligung des Richters und die Anordnung der Staatsanwaltschaft ist jedenfalls nur dann zulässig, wenn die Vorratsdaten zur Verfolgung besonders schwerer Straftaten benötigt werden.

Je nach Schwere der Straftat wird wiederum in der Strafprozessordnung normiert, dass unter gewissen Umständen sogar verlangt wird, dass der Inhaber des Anschlusses, dessen Daten Preis gegeben werden, ausdrücklich zustimmt. Dies ist eben immer dann der Fall, wenn die zu verfolgende Straftat mit einem Strafraum von mehr als sechs Monaten Freiheitsstrafe bedroht ist.

Werden die Daten zur Aufklärung einer Straftat benötigt, die mit mehr als einem Jahr Freiheitsstrafe bedroht ist oder für das Ausforschen einer Person, die verdächtig ist, eine solche Straftat begangen zu haben, ist die Zustimmung des potentiell Betroffenen nicht nötig. Je höher die Strafandrohung für die Tat, hinsichtlich derer der Verdacht besteht, ist, umso weniger Mitspracherecht hat also der von der Weitergabe der Daten Betroffene.

An noch strengere Voraussetzungen ist die Überwachung von Nachrichten gebunden. Dabei handelt es sich nämlich nicht um die bloße Weitergabe von Verkehrsdaten, sondern um das Ermitteln des Inhalts von Nachrichten, die über ein Kommunikationsnetz im Sinne des Telekommunikationsgesetzes oder einen IT-Dienst weitergeleitet beziehungsweise ausgetauscht werden. Eine solche Überwachung ist insbesondere dann zulässig, wenn der dringende Verdacht auf eine Entführung besteht und die Auskunft hinsichtlich der Daten der Person erfolgt, die verdächtig ist, eine andere Person „entführt oder sich sonst ihrer bemächtigt“ zu haben.⁸⁶

⁸⁵ Strafprozessordnung 1975, § 135 Abs 2 Ziffer 4.

⁸⁶ Strafprozessordnung 1975, § 135 Abs 3.

Grundsätzlich ist, wie erwähnt, für all diese Maßnahmen die Zustimmung durch den Richter und die Anordnung durch die Staatsanwaltschaft erforderlich. Dieser so genannte Richtervorbehalt wird zusätzlich dadurch untermauert, dass das Telekommunikationsgesetz bei Vornahme einer Auskunft von Vorratsdaten ohne Vorliegen einer gerichtlichen Bewilligung eine Geldstrafe von bis zu EUR 37.000,- vorsieht.⁸⁷

Allerdings ist im Telekommunikationsgesetz in manchen Fällen auch dann die Beauskunftung über Vorratsdaten zulässig, ohne dass diese zuvor durch das Gericht bewilligt werden muss. So ist beispielsweise die Auskunft über eine IP-Adresse sowie einer E-Mail Adresse des Absenders einer Mail auf schlichte Aufforderung der Staatsanwaltschaft, ohne das Einholen einer vorherigen gerichtlichen Bewilligung, vorzunehmen.⁸⁸

Des Weiteren besteht eine Ausnahme nach dem Sicherheitspolizeigesetz, welches ebenfalls im Zuge der Umsetzung der Vorratsdatenspeicherrichtlinie modifiziert wurde. Die im Zusammenhang mit den Aufgaben des Staates erläuterten Aufgaben kommen zu einem großen Teil der Sicherheitspolizei zu. Als eine organisatorische Form oder Einheit des Polizeiapparates und Teil der Sicherheitsverwaltung, obliegt der Sicherheitspolizei die Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit sowie die Erfüllung der ersten allgemeinen Hilfeleistungspflicht.

Im Zuge der Wahrnehmung dieser Aufgaben kommen ihr demnach auch gewisse Kompetenzen zu, die im Zusammenhang mit dem Abruf von Daten und im Zuge dessen auch der Vorratsdatenspeicherung stehen. Demnach dürfen die Sicherheitsbehörden nach Maßgabe des Sicherheitspolizeigesetzes personenbezogene Daten ermitteln und weiterverarbeiten, sofern dies für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht, die Abwehr krimineller Verbindungen, die Gefahrenforschung beziehungsweise die Gefahrenabwehr und Vorbeugung wahrscheinlicher gefährlicher Angriffe gegen Leben, Gesundheit, Sittlichkeit, Freiheit, Vermögen und Umwelt, Fahndungszwecke, für die Aufrechterhaltung der öffentlichen Ordnung im Zusammenhang mit einem bestimmten Ereignis, oder die Analyse der Wahrscheinlichkeit einer Gefährdung der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit notwendig ist.⁸⁹

⁸⁷ Feiler/Stahov, MR 2011, 111, S. 114; Telekommunikationsgesetz § 109 Abs 3 Z 24.

⁸⁸ Vgl. hierzu § 76a Abs 2 Z 4 StPO iVm § 99 Abs 5 Z 2 TKG.

⁸⁹ Sicherheitspolizeigesetz, § 53 Abs 1.

Diese im Gesetz aufgezählten Fälle ermöglichen den Sicherheitsbehörden die Ermittlung beziehungsweise Weiterverarbeitung in den unterschiedlichsten Situationen. Insbesondere die doch recht allgemeinen Begriffe „Gefahrenabwehr“ oder „erste allgemeine Hilfeleistungspflicht“, oder auch die „Aufrechterhaltung der öffentlichen Ordnung“ lassen darauf schließen, dass die Befugnisse, die der Sicherheitspolizei im Bereich des Datenschutzes zukommen doch durchaus weitreichend sind.

Die im Zuge der gesetzlich zulässigen Fälle verarbeiteten Daten dürfen in weiterer Folge weiterverarbeitet werden. Es ist jedoch grundsätzlich unzulässig, mit diesen Daten einen automationsunterstützten Datenabgleich durchzuführen.

Weiters sind Sicherheitsbehörden berechtigt, von diversen Körperschaften öffentlichen Rechts Auskünfte zu verlangen, also Daten, welche sie für die Erfüllung ihrer Aufgaben, nämlich die Abwehr gefährlicher Angriffe, die erweiterte Gefahrenforschung oder die Abwehr krimineller Vereinigungen benötigen.

Nur in Fällen, in denen andere Interessen überwiegen und es etwa die Amtsverschwiegenheit unbedingt erfordert, dürfen die Körperschaften öffentlichen Rechts eine Auskunft an die Sicherheitsbehörden verweigern.

Neben diversen Körperschaften sind auch die Betreiber öffentlicher Telekommunikationsdienste und sonstige Diensteanbieter nach dem E-Commerce-Gesetz verpflichtet, den Sicherheitsbehörden Auskunft über Personen zu erstatten. Diese Auskunftspflicht besteht wiederum nur dann, wenn die Sicherheitsbehörden tatsächlich Daten für die Erfüllung ihrer gesetzlichen Aufgaben benötigen und umfasst sowohl Namen, Anschrift und Teilnehmernummer der Kommunikationsteilnehmer, Informationen über die IP-Adresse sowie die Eckdaten der übermittelten Nachrichten, wobei Inhaltsdaten nicht erfasst sind.

Beim Vorliegen eines konkreten Verdachtes, dass eine gegenwärtige Gefahr für das Leben, die Gesundheit oder Freiheit eines Menschen besteht, können die Sicherheitsbehörden – und zwar ohne vorherige Genehmigung durch die Staatsanwaltschaft oder einen Richter – auch Auskunft über Standortdaten verlangen und technische Mittel zum Einsatz bringen, welche die Lokalisierung von Telefonen oder Computern ermöglichen.

Nichtsdestotrotz trifft die Sicherheitsbehörde in einem solchen Fall die, wie es im Gesetz genannt wird, „Verantwortung für die rechtliche Zulässigkeit des Auskunftsbeglehrens“.⁹⁰

Insbesondere, wenn die Auskunft über Standortdaten eingeholt und eine Lokalisierung durchgeführt wird, so muss die ermittelnde Behörde demjenigen, von dem die Auskunft erteilt wird, auch nachträglich, nämlich binnen 24 Stunden eine schriftliche Dokumentation nachreichen. Was dem Diensteanbieter jedoch in dieser Dokumentation bescheinigt werden muss, wird nicht konkretisiert.

Die Kosten der Überwachung sind dem Diensteanbieter jedenfalls von der Behörde, die das Auskunftersuchen stellt, zu erstatten.

Unter gewissen Voraussetzungen hat die Behörde auch diejenigen Personen, die von der Überwachung konkret betroffen sind, nachträglich darüber zu informieren, dass ihre Daten im Zuge der Ermittlung einer IP Adresse oder Standortbeauskunftung eingeholt wurden. Dies selbstverständlich nur, sofern die Ermittlungen dadurch nicht gefährdet erscheinen.

Wie bereits erwähnt, trägt die ansuchende Sicherheitsbehörde letztlich die „Verantwortung für die rechtliche Zulässigkeit des Auskunftsbeglehrens“. Die umfassenden Ausführungen des Gesetzgebers zeigen, dass grundsätzlich nicht anlasslos auf Vorratsdaten zugegriffen werden darf, und zwar auch nicht von den Sicherheitsbehörden.

Es wird normiert, dass dies nur unter bestimmten Voraussetzungen zulässig sein soll, beim Verdacht besonders schlimmer Straftaten, bei besonders schwer wiegenden Gefahren.

Die Beurteilung der „rechtlichen Zulässigkeit“ obliegt jedoch letztlich der einschreitenden Behörde. Der Begriff der rechtlichen Zulässigkeit basiert in Wahrheit auf einer *ex ante* Beurteilung der Fakten. Wenn die Sicherheitsbehörde also einen Verdacht hat, dass eine konkrete Gefahr droht, die eine Beauskunftung von Vorratsdaten zulässig erscheinen lässt, und dieser Verdacht sich schließlich als falsch herausstellt, so war die Beauskunftung im Regelfall wohl dennoch rechtlich zulässig, weil sie faktisch notwendig erschien, und die Beurteilung der Gefahrenlage letztlich der Behörde selbst obliegt.

Die vom Gesetzgeber gewählte, doch recht vage Begrifflichkeit der „Verantwortung für die rechtliche Zulässigkeit des Auskunftsbeglehrens“ lässt daher einen großen Handlungsspielraum.

⁹⁰ Sicherheitspolizeigesetz, § 53 Abs 3c.

Sollte nicht gerade ein wirklich sehr offenkundiger Missbrauch des Auskunftsrechts vorliegen, so scheint es, kann die Notwendigkeit oder der begründete Verdacht doch relativ leicht konstruiert und begründet werden.

Insbesondere ist im diesen Zusammenhang auch darauf hinzuweisen, dass für die Frage der Zulässigkeit der Übermittlung von Daten an die Staatsanwaltschaft oder die Sicherheitspolizei der Strafraumen der potentiell aufzuklärenden beziehungsweise zu verhindernden Tat nicht bedeutsam ist.⁹¹

Die vom Gesetzgeber getroffene Einschränkung auf die Aufklärung oder Verhütung von Straftaten, die sich gegen das Leben, die Gesundheit oder Freiheit eines Menschen richten, lässt durchaus Raum für Interpretationen.

Ist die Gesundheit eines Menschen beispielsweise auch durch eine potentiell stattfindende Versammlung gefährdet? Ließe sich daraus ein Rechtfertigungsgrund für das Anfordern von Kommunikationsdaten konstruieren?

Jedenfalls ist es § 53 Abs 3b SPG zu Folge zulässig, auf Vorrat gespeicherte Standortdaten auch ohne Gerichtsbeschluss an die Sicherheitspolizei zu übermitteln, sofern man davon ausgeht, dass die Person, deren Daten ermittelt werden, beispielsweise in ihrer Gesundheit gefährdet ist und man annimmt, dass man diese Person dadurch anhand ihres Mobiltelefons orten kann. Dies steht im Widerspruch zum bereits erwähnten Richtervorbehalt, der im Telekommunikationsgesetz selbst normiert ist.

Kritiker sehen daher in der Bestimmung des § 109 Abs 3 TKG, die Verwaltungsübertretungen mit bis zu 37.000 Euro Strafe bedroht, einen Verstoß gegen das in Artikel 18 der Bundesverfassung normierten Bestimmtheitsgebot und bezeichnen diese Regelung gar als verfassungswidrig.⁹²

⁹¹ Feiler/Stahov, MR 2011, 111, S. 114.

⁹² Feiler/Stahov, MR 2011, 111, S.114.

5. Der öffentliche Diskurs zur Vorratsdatenspeicherung

Während die EU-Richtlinie zur Vorratsdatenspeicherung vor wenigen Jahren auch in Österreich zwar bereits einige Datenschutzexperten und Juristen zur Publikation von kritischen Beiträgen veranlasste, die sich mit potentiellen Gefahren oder verfassungsrechtlichen Bedenken auseinandersetzten, setzte der Diskurs in der breiten Öffentlichkeit erst viel später ein, nämlich, als die Umsetzung besagter Richtlinie auch in Österreich immer näher rückte. So wurde unter anderem der Arbeitskreis Vorratsdatenspeicherung („AK Vorrat“) auf den Plan gerufen.

Das plötzlich explodierende Interesse an dieser Bürgerinitiative gegen die Vorratsdatenspeicherung zeigt sich beispielhaft am sprunghaften Anstieg der gesammelten Unterschriften zu Beginn des Jahres 2012. Während am 11.01.2012 bereits 31.000 Menschen die AK Vorrat unterstützten, stieg die Unterschriftenanzahl binnen eines Tages, also bis zum 12.01.2012 auf 33.000 Unterschriften an.⁹³

Primäres Ziel dieser Bürgerinitiative war es, die österreichische Regierung dazu zu bewegen, sich gegen die EU-Richtlinie zur Vorratsdatenspeicherung einzusetzen. Weiters wurde gefordert, dass sämtliche aus dem Argument der Terrorbekämpfung beschlossenen Gesetze verpflichtend durch den Nationalrat evaluiert werden sollten. Als Leitspruch wurde von der Initiative Artikel 8 der Europäischen Menschenrechtskonvention verwendet: „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.“

Am 12.12.2011 veröffentlichte die Bürgerinitiative auf Ihrer Website folgenden Text:

„Am 1. April 2012 beginnt in Österreich die Vorratsdatenspeicherung. Hinter dem sperrigen Namen ‚Vorratsdaten‘ verbirgt sich die **verdachtsunabhängige** Speicherung von Verbindungsdaten. Unter anderem wird gespeichert: Wer mit wem, von wo aus, wie lange telefoniert und wer wem, wann Emails schreibt. Diese Daten sollen von **allen** Menschen in Österreich gespeichert werden. Damit stellt die Vorratsdatenspeicherung einen massiven Eingriff in die Privatsphäre jedes Bürgers dar. Dieser Eingriff verstößt gegen das Menschenrecht auf Privatsphäre. Begründet wird die Notwendigkeit der Vorratsdatenspeicherung mit der Verbrechensbekämpfung. Es gibt jedoch keinerlei Belege für einen

⁹³ Vgl. Der Standard Online, 31.000 Unterschriften gegen Vorratsdatenspeicherung, 11.01.2012, verfügbar unter: <http://derstandard.at/1326248945531/zeichnemitat-31000-Unterschriften-gegen-Vorratsdatenspeicherung> (zuletzt abgerufen am: 02.01.2013)

Nutzen von Vorratsdaten. Der Arbeitskreis Vorratsdatenspeicherung setzt sich für eine **Wahrung der Grundrechte** ein. Die Umsetzung der Vorratsdatenspeicherung ist nicht im Einklang mit den Grundrechten möglich. Deshalb fordern wir: Keine Vorratsdatenspeicherung in Europa! Keine Vorratsdatenspeicherung in Österreich! Österreich soll die Richtlinie zur Vorratsdatenspeicherung nicht umsetzen sondern bekämpfen!“

Die Resonanz war beachtlich. Auch die Arge Daten erstattete ein Gutachten, das die Befürchtungen und Skepsis der Bürger nicht beschwichtigte, sondern vor allem mit konkreten Fällen aufwartete, wie man durch die Vorratsdatenspeicherung in Verdacht geraten würde. Der Vorwurf lautete, die Unschuldsvermutung werde durch die neue gesetzliche Regelung ins Gegenteil verkehrt und die Bürger unter Generalverdacht gestellt. Des Weiteren sei es gerade jenen Personen, die tatsächlich illegal aktiv seien möglich, die Vorratsdatenspeicherung zu umgehen.⁹⁴

Die bevorstehenden Gesetzesänderungen anlässlich der Vorratsdatenspeicherung führten auch zu diversen Protestaktionen und Demonstrationen. Schlussendlich fanden sich über 100.000 Personen, die die Petition gegen die Umsetzung der Vorratsdatenspeicherrichtlinie unterzeichneten.

Dementsprechend wenig überraschend ist auch das große mediale Interesse an der Vorratsdatenspeicherung, das sich durch die unterschiedlichsten Medien zieht. Sucht man beispielsweise auf der Online-Plattform der Kronenzeitung mit dem Suchbegriff „Vorratsdaten“, so scheinen über 5.100 Suchergebnisse auf.⁹⁵

Egal, welche österreichische Tages- oder Wochenzeitung man wählt: Die Vorratsdatenspeicherung in Österreich, die EU-Vorratsdatenspeicherrichtlinie und die damit verbundenen Gesetzesänderungen werden durchgehend negativ beurteilt, was sich auch in Leserkommentaren widerspiegelt. Das Sicherheitsargument scheint im Diskurs nur eine verschwindende Rolle zu spielen.

⁹⁴ Vgl. ARGE DATEN, Vorratsdatenspeicherung ist Beginn präventivstaatlicher Maßnahmen, 06.04.2011, verfügbar unter: http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=36951thc (zuletzt abgerufen am: 02.01.2013)

⁹⁵ Anmerkung: Stand 01.01.2013,

Während die Regierung zunächst versuchte, die Sinnhaftigkeit der Vorratsdatenspeicherung zu verteidigen, wurde diese von vielen anderen als Überschreitung staatlicher Kompetenzen wahrgenommen, als ein drastischer Eingriff in die Privatsphäre der/des Einzelnen.⁹⁶

Das Thema Vorratsdatenspeicherung führte jedoch auch von Beginn an zu heftigen politischen Debatten zwischen den Regierungs- und Oppositionsparteien. Während ÖVP und SPÖ versuchten, die Gesetzesänderungsentwürfe zu verteidigen, übten Grüne, FPÖ und das BZÖ laut Kritik an den geplanten Änderungen. In ungewöhnlicher Einigkeit brachten die Oppositionsparteien vor allem das Argumente des Eingriffs in die Freiheitsrechte der Staatsbürger, jenes der Nutzlosigkeit der Vorratsdatenspeicherung an sich und das der Gefahr des Datenmissbrauchs vor.⁹⁷

Während die Oppositionsparteien durchgehend argumentierten, die Vorratsdatenspeicherung sei nicht verfassungs- und grundrechtskonform, beriefen sich die Regierungsparteien auf die Notwendigkeit der Umsetzung der EU-Richtlinie.

Nicht zuletzt wurde vom Argument eines Mangels an Alternativen Gebrauch gemacht und darauf verwiesen, dass die Richtlinie umgesetzt werden *müsse*. Diese Begründung war nicht zuletzt Wasser auf die Mühlen von EU-Skeptiker und Skeptikerinnen.

a) Offizielle Stellungnahmen aus der Politik

Vertreter und Vertreterinnen der Regierungsparteien versuchten zu beschwichtigen und brachten insbesondere vor, dass die Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung sehr wohl in Einklang mit den Grund- und Freiheitsrechten stünde.

Vor allem wurde versucht, das Potential von Vorratsdaten und Stammdaten herunterzuspielen und zu betonen, dass insbesondere keine Inhaltsdaten gespeichert werden dürften. Man dürfe der Polizei, den Gerichten und Staatsanwälte und Staatsanwältinnen nicht die Möglichkeit nehmen, Verbrechen zu verhindern und Täterinnen und Täter auszuforschen.⁹⁸

⁹⁶ Vgl. etwa: Der Standard Leserkommentar, Nutzlosigkeit, auf Vorrat gespeichert, 29.02.2012, <http://derstandard.at/1330389938463/Digitale-Datenspeicherung-Nutzlosigkeit-auf-Vorrat> (zuletzt abgerufen am 03.01.2013)

⁹⁷ Vgl. hierzu: Presseaussendung des Parlaments, 28.04.2011. Verfügbar unter: www.parlament.gv.at/PAKT/PR/JAHR_2011/PK0408/

⁹⁸ Vgl. Rede des Parlamentsabgeordneten Heribert Donnerbauer (ÖVP), wiedergegeben in der Presseaussendung des Parlaments vom 28.04.2011. Verfügbar unter: www.parlament.gv.at/PAKT/PR/JAHR_2011/PK0408/

Innenministerin Johanna Mikl-Leitner brachte vor, die Vorratsdatenspeicherung sei notwendig, um beispielsweise bei Bombendrohungen, beim Schutz von Kindern vor sexuellen Übergriffen und bei angekündigten Selbstmorden rasch eingreifen zu können. Auch die Bundesministerin für Verkehr, Innovation und Technologie, Doris Bures, sprach sich für die Vorratsdatenspeicherung aus und berief sich insbesondere darauf, dass bei der Umsetzung der Vorratsdatenspeicherrichtlinie auch Experten des Ludwig-Boltzmann-Instituts für Menschenrechte beigezogen worden seien. Justizministerin Beatrix Karl berief sich einerseits auf die Notwendigkeit der Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung um eine Geldbuße für Österreich zu vermeiden. Des Weiteren sei die Vorratsdatenspeicherung notwendig, da sie eine wirksame Strafverfolgung und die Wahrung der Rechtstaatlichkeit gewährleiste.⁹⁹

b) Medien und Öffentlichkeit – Reaktionen

Die österreichischen Medien gingen mit der Vorratsdatenspeicherung besonders hart ins Gericht.¹⁰⁰ Befürchtungen bestehen vor allem auch in die Richtung, dass die Vorratsdatenspeicherung indirekt auch zu einer Einschränkung des Redaktionsgeheimnisses und der Meinungsfreiheit in Österreich führe, da die Überwachung journalistischer Arbeit erleichtert würde. Besonders unter Beschuss geriet das Sicherheitspolizeigesetz, demzufolge die Überwachung Einzelner, die „gefährliche“ Kenntnisse besitzen, legitimiert wird.¹⁰¹

Den Regierungsparteien wurde außerdem vorgeworfen, übereilt und nicht überlegt zu handeln. Während die EU-Kommission Deutschland im März 2012 ein Ultimatum setzte¹⁰², wonach für den Fall der Nichtumsetzung der Vorratsdatenspeicherrichtlinie mit einer

⁹⁹ Vgl. Presseaussendung des Parlaments vom 28.04.2011. Verfügbar unter: www.parlament.gv.at/PAKT/PR/JAHR_2011/PK0408/

¹⁰⁰ Anmerkung: Es wurden insbesondere die Tageszeitungen „Die Presse“ und „Der Standard“ untersucht, wobei auch deutsche Zeitungen („Der Spiegel“, „Die Zeit“) und Magazine („Profil“) mit einbezogen wurden. Aufgrund der besseren chronologischen Nachvollziehbarkeit der Stimmung beziehungsweise Einstellung gegenüber der Vorratsdatenspeicherung und der Veränderung dieser Stimmung wurden die nachstehend zitierten Pressemeldungen fast ausschließlich der Tageszeitung „Der Standard“ entnommen.

¹⁰¹ Der Standard, Hausjell: Neue Strafprozessordnung „direkter Angriff“, 09.03.2012, <http://derstandard.at/1331206929199/Recht-Hausjell-Neue-Strafprozessordnung-direkter-Angriff> (zuletzt abgerufen am 05.01.2013)

¹⁰² Der Standard, Vorratsdatenspeicherung: Brüssel setzt Deutschland Frist, 20.03.2012, <http://derstandard.at/1331780173034/Vorratsdatenspeicherung-Bruessel-setzt-Deutschland-Frist> (zuletzt abgerufen am 08.01.2013)

Vertragsverletzungsklage gedroht wurde, war zu diesem Zeitpunkt in Österreich bereits eine Regelung in Sicht.

Der Vorwurf der Übereilung der Umsetzung der umstrittenen Richtlinie freilich ist nicht wirklich haltbar: Österreich wurde aufgrund der um mehrere Jahre verspäteten Umsetzung der Richtlinie sogar vom EuGH verurteilt.

Mit dem Inkrafttreten der österreichischen Regelung zur Umsetzung der Vorratsdatenspeicherrichtlinie war das öffentliche Interesse an der Vorratsdatenspeicherung jedoch nicht beendet. Im Gegenteil – durch das Inkrafttreten der gesetzlichen Änderungen bot sich nunmehr die Chance, diese vor dem Verfassungsgerichtshof zu bekämpfen.

Besondere Aufmerksamkeit erhielt der Antrag des Kärntner Landeshauptmanns Gerhard Dörfler (FPK), der beim Verfassungsgerichtshof einen Antrag auf Aufhebung der einschlägigen Normen¹⁰³ aufgrund ihrer Verfassungswidrigkeit stellte.¹⁰⁴

Die Tageszeitung „Der Standard“ startete im März 2012, kurz vor Inkrafttreten der neuen gesetzlichen Regelungen, eine Umfrage an die Leserinnen und Leser um herauszufinden, wie diese der Vorratsdatenspeicherung gegenüberstehen. Von über 1.000 Leserinnen und Leser, die an dieser Abstimmung teilnahmen, sprachen sich etwa 98% gegen die neuen gesetzlichen Regelungen bezüglich der Vorratsdatenspeicherung aus.¹⁰⁵ Skeptisch waren die Leserinnen und Leser, die sich zu diesem Thema äußerten, vor allem in Hinsicht auf die Auswirkungen auf die Privatsphäre, die Demokratie, Medien- und Meinungsfreiheit. Weiters wurden Bedenken geäußert, die Vorratsdatenspeicherung sei nur der erste Schritt in Richtung Echtzeitüberwachung durch den Staat, der kollektiv alle seine Bürger unter Generalverdacht stelle.

¹⁰³ Anmerkung: In Presseberichten wurde behauptet, beim Verfassungsgerichtshof sei ein Antrag auf Aufhebung der Richtlinie eingebracht worden. Bei dieser Behauptung handelt es sich selbstverständlich um eine Verwechslung, da dem österreichischen Verfassungsgerichtshof in diesem Bereich keine Kompetenzen zukommen. Angefochten wurden vielmehr die innerstaatlichen Gesetze, die in Umsetzung der Richtlinie erlassen wurden.

¹⁰⁴ Der Standard, Kärnten bringt Verfassungsklage ein, 26.03.2012, <http://derstandard.at/1332323819778/Vorratsdaten-Kaernten-bringt-Verfassungsklage-ein> (zuletzt abgerufen am 03.01.2012)

¹⁰⁵ Anmerkung: Wiederum wurden von der Tageszeitung „Der Standard“ falsche Begrifflichkeiten verwendet – so ließ man die LeserInnen darüber abstimmen, ob sie für oder gegen das Inkrafttreten der EU-Richtlinie am 01.04.2012 seien, wobei dieses Thema selbstverständlich nicht zur Debatte stand, da die Richtlinie bereits seit Jahren in Kraft war.

Einige LeserInnen machten jedoch auch darauf aufmerksam, dass es einen Widerspruch darstelle, wenn die Menschen gleichzeitig die Vorratsdatenspeicherung als einen verfassungswidrigen Eingriff in ihre Privatsphäre auffassen würden, gleichzeitig aber alle möglichen Daten über Facebook, Twitter und Co publizierten.¹⁰⁶

Nichts destotrotz stieg schon relativ bald die Nachfrage nach Möglichkeiten, wie man der Vorratsdatenspeicherung entkommen könne. Tipps zur Umgehung der Vorratsdatenspeicherung reichen beispielsweise von der Nutzung von Anonymisierungs-Software, der Einrichtung privater Mail-Server, dem Senden von Datenträgern per Post, der Benützung registrierter Handys, dem Entfernen von Handy-Akkus und Einlegen derselben nur beim Telefonieren, bis hin zur Benützung von Internetcafés und dem Einrichten von Tauschbörsen für Wertkartenhandys, die man möglichst oft wechseln sollte.¹⁰⁷

Auch seitens Amnesty International Österreich wurde die Umsetzung der Vorratsdatenspeicherrichtlinie als Eingriff in die Grundrechte der ÖsterreicherInnen und als Angriff auf den Rechtsschutz kritisiert. Der Generalsekretär von Amnesty International Österreich unterstelle der Politik gar, man wolle einen totalen Überwachungsstaat schaffen, was eine Abkehr vom klassischen Rechtsstaatsprinzip bedeute.¹⁰⁸

Wenig überraschend wurden diese Bedenken auch von der AK Vorrat geteilt, die dem Verfassungsgerichtshof Mitte Juni 2012 die in Schubkarren geladenen 11.139 Vollmachten von all jenen Personen übergab, die eine Individualbeschwerde an den Verfassungsgerichtshof stellten.¹⁰⁹ Diese doch sehr plakative Vorgehensweise brachte der Bürgerinitiative noch zusätzliche Aufmerksamkeit. Bemerkenswert ist in diesem Zusammenhang vor allem, dass trotz der doch sehr oberflächlichen Berichterstattung und der teilweise auch recht offenkundig falschen Aussagen, wie beispielsweise, dass durch die

¹⁰⁶ Der Standard, derStandard.at-UserInnen sind gegen die Vorratsdatenspeicherung, 28.03.2012, <http://derstandard.at/133232397666-derStandardat-UserInnen-sind-gegen-die-Vorratsdatenspeicherung> (zuletzt abgerufen am 01.01.2013)

¹⁰⁷ Profil, Vorratsdatenspeicherung könnte illegal sein, <http://www.profil.at/articles/1214/560/323729/vds-vorratsdatenspeicherung> (zuletzt abgerufen am 02.01.2013)

¹⁰⁸ Der Standard, Amnesty kritisiert Grundrechtseingriffe in Österreich, 23.05.2012, <http://derstandard.at/1336697696851/Jahresbericht-Amnesty-kritisiert-Grundrechtseingriffe-in-Oesterreich> (zuletzt abgerufen am 02.01.2013)

¹⁰⁹ Der Standard, Scheibtruhenweise Klagen gegen die Vorratsdatenspeicherung, 15.06.2012, <http://derstandard.at/1339637967615/Scheibtruhenweise-Klagen-gegen-die-Vorratsdatenspeicherung> (zuletzt abgerufen am 02.01.2013)

Verfassungsklage die EU-Richtlinie gekippt werden sollte, die Resonanz der BürgerInnen unglaublich hoch war.

Der Unmut war trotz – oder vielleicht gerade wegen der spärlichen Aufklärung und der mangelnden Informiertheit der Öffentlichkeit besonders groß. Vorherrschend war wohl vor allem ein Gefühl des Unbehagens, das nur von den wenigsten fundiert argumentiert werden konnte, da kaum jemand genau wusste, was die Vorratsdatenspeicherung konkret bedeutete.

Dies ist nicht zuletzt auf die wenig ambitionierte Aufklärung durch die politischen Parteien, die – sofern überhaupt vorhanden – von den durchwegs negativen und beunruhigenden Presseberichten übertönt wurde.

Umso erstaunlicher ist es dennoch, dass so viele Menschen tatsächlich Initiative zeigten, und sich mit einer Individualklage ganz klar gegen die Vorratsdatenspeicherung aussprachen.

Vom beliebten Argument „Wer nichts verbrochen hat, der hat auch nichts zu befürchten“ ließen sich demnach bei Weitem nicht alle ÖsterreicherInnen überzeugen. Dies wohl auch deshalb, da von DatenschutzexpertInnen das Missbrauchspotential durch die Vorratsdatenspeicherung als durchaus nicht unbedeutend eingestuft wurde. Die AK Vorrat betitelte die Vorratsdatenspeicherung gar mit dem „größten Grundrechtseingriff der Zweiten Republik“.¹¹⁰

Aufgrund des ausgeprägten Widerstands, der auch aus anderen Mitgliedstaaten der Europäischen Union zu vernehmen war, die sich – ebenso wie Österreich – mit Verfassungsbeschwerden und Unvereinbarkeiten mit verfassungsgesetzlich gewährleisteten Rechten konfrontiert sahen, wurde auch seitens der Europäischen Union bereits im Juli 2012 angekündigt, die Vorratsdatenspeicherrichtlinie abändern zu wollen.

Konkret ist laut der zuständigen Kommissarin, Cecilia Malström, eine Entschärfung der Richtlinie geplant. Deren Anwendungsbereich soll in Hinkunft dahingehend eingeschränkt werden, dass die Vorratsdatenspeicherung tatsächlich nur noch für die Bekämpfung von Terrorismus und schweren Verbrechen verwendet werden soll.¹¹¹

¹¹⁰ Profil, Vorratsdatenspeicherung könnte illegal sein.
<http://www.profil.at/articles/1214/560/323729/vds-vorratsdatenspeicherung> (zuletzt abgerufen am 02.01.2013)

¹¹¹ Der Standard, EU-Kommissarin legt Pläne zur Änderung der Vorratsdaten-Richtlinie dar, 04.07.2012, <http://derstandard.at/1339639728035/Plaene-zur-Aenderung-der-Vorratsdaten-Richtlinie-dar>

Auch wenn diese Entwicklung von Skeptikern der besagten Richtlinie wohl wenigstens als Teilerfolg gewertet werden muss, und als ein Schritt in die richtige Richtung angesehen wird, ändert diese Entwicklung jedoch kaum etwas an der fundamentalen Kritik. Insbesondere wird immer wieder betont, dass die Vorratsdatenspeicherung in Wahrheit gar kein wirksames Mittel gegen den Terrorismus darstelle und es deshalb widersinnig sei, sie durch terroristische Gefahren zu legitimieren.

c) Wissenschaftliches Interesse am Thema Vorratsdaten

Aufgrund der Brisanz des Themas wurden auch bereits mehrere Studien veröffentlicht, die die Wirksamkeit der Vorratsdatenspeicherung zur Verbrechensbekämpfung stark in Zweifel ziehen.

Unter anderem führte das renommierte Max-Planck-Institut für ausländisches und international Strafrecht eine Studie durch, in der einerseits eigens gesammelte Daten, sowie bereits existente Daten, die Aufklärungsquoten von Kriminalfällen zwischen 1987 und 2010, sowie Kennzahlen von Ländern, in denen eine Zeit lang die Vorratsdatenspeicherung verpflichtend war, ausgewertet.

Das Ergebnis – von den Wissenschaftlern selbst jedoch ausdrücklich als bloße Momentaufnahme bezeichnet – widerlegt die Annahme, dass die anlasslose Speicherung von Vorratsdaten von essentieller Bedeutung für die Strafverfolgung sei und nicht zur Veränderung der Aufklärungsquote beitrage. Ergo würde die Vorratsdatenspeicherung auch auf die Sicherheit der Bürgerinnen und Bürger keinen maßgeblichen Einfluss haben.¹¹²

Zu einem ähnlich ernüchternden Resultat gelangten auch Forscherinnen und Forscher der Technischen Universität Darmstadt. Diese versuchten, anhand eines virtuellen, an biologische Interaktionen angelehnten Netzwerks von Bürgerinnen/Bürgern und Terroristinnen/Terroristen gefährliche Individuen innerhalb dieses Netzwerkes aufgrund ihrer Unterschiede im Kommunikationsverhalten enttarnen. Dies misslang. Als problematisch wurde vor allem die lange Speicherdauer, die zu einer hohen Wahrscheinlichkeit von

(zuletzt abgerufen am 03.01.2013)

¹¹² Zeit Online, Forscher halten Vorratsdaten für wirkungslos.

<http://www.zeit.de/digital/datenschutz/2012-01/vorratsdatenspeicherung-studie> (zuletzt abgerufen am 04.01.2013)

Fehlalarm führt, sowie die umfassenden Möglichkeiten, das System zu überlisten, identifiziert.¹¹³

Mit diesen und ähnlichen Einschätzungen musste sich letztlich auch der Justizausschuss in einer nicht öffentlichen Sitzung im November 2012 auseinandersetzen, als vor allem auch die Bedenken der Bürgerinitiative AK Vorrat behandelt wurden.¹¹⁴

d) Verfassungsrechtliche Prüfung

Vielleicht doch ein wenig überraschend führte die Prüfung des Verfassungsgerichtshofes dazu, dass auch dieser letztlich mit Nachdruck Bedenken äußerte wonach die EU-Richtlinie zur Vorratsdatenspeicherung unter Umständen dem in der EU-Grundrechtecharta verankerten Grundrecht auf Datenschutz entgegenstehen könnte.

Dass sich der Verfassungsgerichtshof bei seiner Prüfung auf eine EU-Norm, nämlich die Grundrechtecharta stützt, ist keine Selbstverständlichkeit. Erst im Mai 2012 fiel eine diesbezügliche Grundsatzentscheidung, bei welcher der Verfassungsgerichtshof feststellte, dass in Verfahren, in welchen Unionsrecht von Bedeutung ist, auch die Grundrechtecharta der Europäischen Union als Maßstab herangezogen werden kann.¹¹⁵

In einer offiziellen Stellungnahme heißt es, es sei dem Verfassungsgerichtshof durchaus bewusst, dass die Vorratsdatenspeicherung die Ermittlung und Verfolgung schwerer Straftaten zum Ziel habe, sowie einen Beitrag zur Terror-Bekämpfung zu leisten; allerdings betreffe die Vorratsdatenspeicherung faktisch fast ausschließlich Personen, die nicht durch ein bestimmtes Verhalten Anlass für die Speicherung ihrer Daten gegeben haben.¹¹⁶

¹¹³ Der Standard, Vorratsdatenspeicherung kein Mittel gegen Terrorismus, 11.09.2012, <http://derstandard.at/1345166822069/Vorratsdatenspeicherung-kein-Mittel-gegen-Terrorismus> (zuletzt abgerufen am 03.01.2013)

¹¹⁴ Angaben finden sich auf der Website des Parlaments; Justizausschuss, 24. Sitzung, am 28.11.2012; <http://www.parlament.gv.at>

¹¹⁵ Die Presse, Bedenken wegen Vorratsdaten: VfGH schaltet EuGH ein, 18.12.2012, <http://diepresse.com/home/techscience/internet/sicherheit/1325186/Bedenken-wegen-Vorratsdaten> (zuletzt abgerufen am 03.01.2013)

¹¹⁶ Der Standard, Vorratsdatenspeicherung wackelt: Verfassungsrichter haben Bedenken, 18.12.2012, <http://derstandard.at/1355459980072/Vorratsdatenspeicherung-wackelt--Verfassungsrichter-haben-Bedenken> (zuletzt aufgerufen am 03.01.2013)

Der österreichische Verfassungsgerichtshof steht mit dieser Ansicht jedoch nicht allein da – bereits zuvor war der EuGH von den irischen Höchstgerichten derartigen Bedenken konfrontiert worden.¹¹⁷

Der Präsident des Verfassungsgerichtshofes, Gerhart Holzinger, schloss sich in seiner offiziellen Begründung für diesen Schritt weitgehend den zentralen, in der Sammelbeschwerde genannten Kritikpunkten an.¹¹⁸ Insbesondere wurde auch von Seiten des Verfassungsgerichtshofes auf das Problem des Verdächtigens unbescholtener Bürgerinnen und Bürger, sowie der Gefahr des Missbrauchs der gesammelten Daten hingewiesen.

In der Presseaussendung des Verfassungsgerichtshofes wird die Betrauung des EuGH mit der Problematik folgendermaßen begründet:

„Der Verfassungsgerichtshof hat Bedenken, dass die EU-Richtlinie über die sogenannte Vorratsdatenspeicherung der EU-Grundrechtecharta widersprechen könnte. Die 14 Verfassungsrichterninnen und Verfassungsrichter haben aus diesem Grund den Europäischen Gerichtshof (EuGH) eingeschaltet und ihm Fragen zur Auslegung der EU-Grundrechtecharta vorgelegt.“¹¹⁹

Diese vom Verfassungsgerichtshof vorgelegten Fragen beschäftigen sich grundlegend mit der Vereinbarkeit der Richtlinie, konkret mit den Artikeln 3 bis 9 derselben mit der Grundrechtecharta der Europäischen Union, und zwar mit den Artikeln 7, 8 und 11.

Dabei geht es um die Gültigkeit von Handlungen von Organen der Europäischen Union. Außerdem wurden Fragen betreffend die Auslegung der Verträge, nämlich der Grundrechtecharta, an den Europäischen Gerichtshof gestellt.

Die Vorlage der Fragen wirkt sich auch auf das innerstaatliche Verfahren vor dem Verfassungsgerichtshof aus. Dieses ist bis auf Weiteres unterbrochen und wird erst dann fortgesetzt, wenn die an den EuGH gestellten Fragen von diesem beantwortet wurden. Bis dahin bleiben auch die Vorratsdatenspeicherung und die umstrittenen Bestimmungen des Telekommunikationsgesetzes in Kraft und müssen befolgt werden.

¹¹⁷ Der Standard, Vorratsdatenspeicherung: Mutiges Höchstgericht, 18.12.2012, <http://derstandard.at/1355460061183/Vorratsdatenspeicherung-Mutiges-Hoechstgericht> (zuletzt abgerufen am 01.01.2013)

¹¹⁸ Der Standard, Printausgabe vom 19.12.2012, Österreich lässt Vorratsdatenspeicherung prüfen, S. 27.

¹¹⁹ Presseinformation Verfassungsgerichtshof, abrufbar unter www.verfassungsgerichtshof.at

6. Abwägung der Interessen

Nunmehr wurden die Intentionen der Europäischen Union sowie des nationalen Gesetzgebers im Lichte der Entstehungsgeschichte der Vorratsdatenspeicherrichtlinie und ihrer innerstaatlichen Umsetzung wiedergegeben und ausgeführt.

Ins Treffen geführt wurden von dieser Seite vor allem Sicherheitsargumente. Gründe der Terror- und Verbrechensbekämpfung, sowie die umfassenden Möglichkeiten der Aufklärung bereits begangener Verbrechen werden von der Legislative als zentrale Rechtfertigung für die gesetzliche Verankerung der Vorratsdatenspeicherung angeführt.

Die Gegenargumente, die von KritikerInnen der entsprechenden Normen vorgebracht werden, sind demgegenüber vielseitig und unterschiedlicher Natur. Nachstehend sollen die wichtigsten Argumentationslinien nachgezeichnet, und die Pro- beziehungsweise Contra-Argumente einander gegenübergestellt werden.

Dass die Anzahl der kritischen Argumente bei Weitem überwiegt, soll jedoch nicht als qualitative Beurteilung gesehen werden, da vorerst keine Aussage darüber getroffen werden soll, wessen Anliegen höherwertig sind. Bei Betrachtung der nachstehenden Evaluierung sollte – insbesondere in Anbetracht der stark voneinander abweichenden Ausführungslänge der Argumente für und gegen die Vorratsdatenspeicherung – der Leser/die Leserin sich vor allem auch folgenden Gedanken immer wieder in Erinnerung rufen:

Ein einziges gutes Argument vermag unter Umständen hunderte schwache Gegenargumente zu entkräften.

a) Argumente von Befürwortern der Vorratsdatenspeicherung

Befürworterinnen und Befürworter der Vorratsdatenspeicherung lassen sich ganz grundsätzlich nur vereinzelt identifizieren. Argumente, die für eine Speicherung von Vorratsdaten sprechen, wurden fast ausschließlich von Seiten des Gesetzgebers, sei es auf Ebene der Europäischen Union oder auf nationalstaatlicher Ebene, vorgebracht. Vereinzelt finden sich selbstverständlich auch abseits der Politik Stimmen, die die Verankerung der Vorratsdatenspeicherung befürworten, oder – häufiger – die nicht strikt gegen die Vorratsdatenspeicherung sind beziehungsweise die das Thema nicht wirklich beunruhigt.

Die Argumente, die für die Vorratsdatenspeicherung vorgebracht werden, sind ausschließlich Sicherheits- und Strafverfolgungsargumente:

1. Bekämpfung krimineller Organisationen

Die Vorratsdatenspeicherung wird vom Gesetzgeber als wertvolle Waffe im Kampf gegen kriminelle Organisationen betrachtet. Diese Form der Kriminalität wird als besonders verpönt und folgeschwer angesehen. Dass die Mitgliedschaft in einer kriminellen Organisation strafbar ist, ergibt sich aus § 278a StGB, der vom Volksmund auch als „Mafiaparagraph“ bezeichneten Bestimmung, die durch die Tierschützerprozesse¹²⁰ einen wenig positiv behafteten Bekanntheitsgrad erlangte.

Nach § 278a StGB versteht man unter einer kriminellen Organisation eine *auf längere Zeit angelegte unternehmensähnliche Verbindung einer größeren Zahl von Personen*, die unter anderem darauf ausgerichtet ist, wiederholt geplante schwerwiegende strafbare Handlungen zu begehen.

Davon umfasst sind sowohl strafbare Handlungen gegen das Leben, die körperliche Unversehrtheit, die Freiheit oder das Vermögen, die sexuelle Ausbeutung von Menschen, Schlepperei, der unerlaubte Umgang mit Suchtgift, Falschgeld, gefährlichen Stoffen etc. Im Grunde sind von dieser Aufzählung fast alle denkmöglichen Straftatbestände umfasst. Kriminelle Organisationen werden auch dadurch charakterisiert, dass durch sie eine Bereicherung in großem Umfang oder erheblicher Einfluss in Politik und Wirtschaft angestrebt wird, sowie durch Korruption oder Einschüchterung anderer, und in weiterer Folge durch die Abschirmung von Strafverfolgungsmaßnahmen.

Wer sich an einer solchen kriminellen Organisation als Mitglied beteiligt, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

Insbesondere der hohe Organisationsgrad und die wiederkehrende Begehung, sowie ein befürchteter negativer Einfluss auf Wirtschaft und Politik machen die Bekämpfung solcher

¹²⁰ Anmerkung: Bei den so genannten Tierschützerprozessen handelt es sich um einen Strafprozess, der sich über ein Jahr erstreckte. Die Tierschützervereinigung wurden unter den umstrittenen § 278a StGB subsumiert, was in der Öffentlichkeit zu großem Widerstand führte.

krimineller Organisationen laut Befürworterinnen und Befürwortern der Vorratsdatenspeicherung mit allen zur Verfügung stehenden Mitteln notwendig, vor allem, um drohenden Schaden abzuwenden, aber auch, um bereits durch kriminelle Organisationen begangene Straftaten aufzuklären. Sowohl präventive Gründe, als auch solche der Verbrechensaufklärung *ex post* mögen bei diesem Argument eine Rolle spielen.¹²¹ Auch kriminelle Vereinigungen spielen in diesem Zusammenhang eine gewisse Rolle.¹²²

2. Bekämpfung von Terrorismus

Ein weiteres zentrales Argument stellt die Terrorismusbekämpfung dar. Dieses Thema rückte – wie bereits eingangs kurz angesprochen – aufgrund der Terroranschläge in New York, Madrid und London immer mehr in den Fokus unterschiedlicher Staaten. Auch Staaten, die bislang nicht direkt Ziel von Terroranschlägen wurden, begannen sich aufgrund der verheerenden Auswirkungen derselben mit der Gefahr von Terrorismus auseinanderzusetzen.

Der Begriff des Terrorismus wird oftmals eher im Zusammenhang mit Angriffen auf den Staat, die politische Stabilität und öffentliche Sicherheit verwendet. Terrorismus wird dementsprechend auch eher mit feindlichen Aktivitäten, deren Wurzeln im Ausland liegen, in Verbindung gebracht. Grundsätzlich ist der Begriff „Terrorismus“ jenem der kriminellen Organisation sehr ähnlich.

In § 278b StGB wird der Begriff „terroristische Vereinigung“ folgendermaßen definiert:

„Eine terroristische Vereinigung ist ein auf längere Zeit angelegter Zusammenschluss von mehr als zwei Personen, der darauf ausgerichtet ist, dass von einem oder mehreren Mitgliedern dieser Vereinigung eine oder mehrere terroristische Straftaten ausgeführt werden oder Terrorismusfinanzierung betrieben wird.“

Zu den terroristischen Straftaten zählen Mord, Körperverletzungen, erpresserische Entführung, schwere Nötigung, gefährliche Drohung, schwere Sachbeschädigung und Datenbeschädigung, vorsätzliche Gemeingefährungsdelikte und weitere Straftaten.¹²³

¹²¹ Vgl. dazu auch: Benn-Ibler, AnwBl 2008, 12, S. 12.

¹²² Vgl. hierzu Strafgesetzbuch, § 278.

¹²³ Vgl. hierzu Strafgesetzbuch, § 278c.

Ein Akt des Terrorismus muss seine Wurzeln nicht im Ausland haben, und muss ebenso wenig durch das Zünden einer Bombe oder einer sonst veranlassten Explosion realisiert werden.

Folglich ist das Argument der Notwendigkeit der Terrorismusbekämpfung weitgehend mit jenem der Bekämpfung krimineller Organisationen gleichzusetzen, da durch die Vorratsdatenspeicherung einer – wie immer gearteten – Destabilisierung des (staatlichen) Systems durch feindliche (innere oder äußere) Kräfte entgegengewirkt werden soll.

3. Verfolgung von Kinderpornographie

Als weitere Begründung für die Notwendigkeit und Legitimität der Vorratsdatenspeicherung wird das Thema Kinderpornographie herangezogen. Da ein sehr großer Teil von Kinderpornographie über das Internet in Umlauf gebracht beziehungsweise ausgetauscht wird, soll durch die Vorratsdatenspeicherung mitunter sichergestellt werden, dass die Täterinnen und Täter auch tatsächlich ausgeforscht werden können, und schließlich nicht aufgrund gelöschter Daten keine Nachweise erbracht werden können. Das dahinterstehende Kernargument lautet, dass Personen, die sich der Kinderpornographie schuldig machen, sich oftmals anonym durchs Internet bewegen und mit anderen Kriminellen kommunizieren und einen regen Datenaustausch beschreiben.

Dies könne – wenn ein Täter ausgeforscht wird – nunmehr auch dazu führen, dass durch das Nachverfolgen der Kontakte dieses Täters auch weitere Täter ausgeforscht werden können und somit ganze kinderpornographische Netzwerke leichter identifizierbar werden.

4. Auffinden von Menschen in Notlagen

Durch Standortdaten von Mobiltelefonen wird es ermöglicht, den Aufenthaltsort von Menschen in Notlagen, die beispielsweise vermisst werden, entführt wurden, oder denen etwas zugestoßen sein könnte, zu ermitteln. Da durch die Vorratsdatenspeicherung Bewegungsmuster rekonstruiert werden können, ist es auch, wenn beispielsweise das Handy zu einem späteren Zeitpunkt ausgeschaltet ist, etwa weil der Akku leer ist, möglich, zumindest eine ungefähre Suchrichtung zu bestimmen und den Radius einzugrenzen.

5. Allgemein: Notwendigkeit von Mindestspeicherfristen für Verkehrsdaten

Der Vollständigkeit halber sei angemerkt, dass die Befürworterinnen und Befürworter der Vorratsdatenspeicherung ihre Feststellungen und Argumente nicht bloß in den Raum stellten, sondern sehr wohl bemüht waren, die Notwendigkeit und Nützlichkeit der Vorratsdatenspeicherung durch Studien zu untermauern. So wurde etwa in Deutschland bereits im Jahr 2005 vom Bundeskriminalamt eine Studie zu den Mindestspeicherfristen für Telekommunikationsdaten durchgeführt, um einen Beleg für die defizitäre Rechtslage zu liefern.¹²⁴

Diese sollte vor allem auch Ergebnisse zu der Frage liefern, ob so genanntes „data freezing“ (mittlerweile auch als „Quick-Freeze-Verfahren“¹²⁵ bekannt) als gelindere Maßnahme in Betracht käme. In dieser Studie wurde festgehalten, dass oftmals Ermittlungsverfahren nicht erfolgreich geführt werden könnten, da Verkehrsdaten als einzige Ermittlungsansätze zur Verfügung stünden, diese Daten aber in vielen Fällen gar nicht oder nicht mehr gespeichert seien und die Auskunftersuchen der Behörden ins Leere gingen.¹²⁶

Es wurde eine Bund-Länder-Befragung durchgeführt, anhand derer Rechtsmitteldefizite ermittelt werden sollten. Die Schwerpunkte der Vorratsdatenspeicherung beziehen sich laut der genannten Studie vor allem auf Straftaten gegen die sexuelle Selbstbestimmung, auf Betrugsdelikte und Straftaten gegen das Eigentum, allerdings habe die Vorratsdatenspeicherung auch Aufklärungspotential in anderen Straftaten.¹²⁷

Hinsichtlich der Frage nach der Nützlichkeit des Data-Freeze-Verfahrens wurde festgestellt, dass dieses in nur 17% der untersuchten Fällen eine Alternative zur Vorratsdatenspeicherung gewesen wäre, sofern die Daten überhaupt gespeichert worden wären.

Es wird argumentiert, dass in 78% der Fälle die Strafverfolgungsbehörden Verkehrsdaten als wichtig bis sehr wichtig erachten, dies jedoch nicht automatisch zu einer Forderung nach längeren Speicherfristen führe, und dies wiederum auf den verantwortungsvollen, sensiblen

¹²⁴ Mahnken, Mindestspeicherfristen für Telekommunikationsverbindungsdaten, Bundeskriminalamt, 2005.

¹²⁵ Anm.: Beim Quick-Freeze-Verfahren, das aus den Vereinigten Staaten stammt, geht es um das „Einfrieren“ von Verkehrsdaten für die Zwecke der Strafverfolgung. Dies geschieht auf einen richterlichen Beschluss hin, um die Löschung von Daten, die für das Ermittlungsverfahren relevant sein könnten, zu verhindern.

¹²⁶ Mahnken, Mindestspeicherfristen für Telekommunikationsverbindungsdaten, Bundeskriminalamt, Pkt III.

¹²⁷ Mahnken, Mindestspeicherfristen für Telekommunikationsverbindungsdaten, Bundeskriminalamt, Pkt IV.15.

Umgang der Polizei mit rechtspolitischen Forderungen mit datenschutzrechtlicher Relevanz schließen lasse.¹²⁸

b) Argumente der Gegner der Vorratsdatenspeicherung

Im Gegensatz zu den Argumenten der Vorratsdatenspeicherungs- Befürworterinnen und Befürworter sind jene der Kritiker teils sehr unterschiedlicher Natur; doch auch für sie lässt sich ein Sammelbegriff finden: Grundrechtsverletzung.

1. Der gläserne Mensch

Nicht selten wird ins Treffen geführt, dass die Vorratsdatenspeicherung nur einen weiteren, signifikanten Schritt in Richtung Überwachungsstaat darstellt. Kritikerinnen und Kritiker befürchten, dass jeder Mensch, der sich moderner Kommunikationsdaten bedient, sich dadurch unfreiwillig zum „gläsernen Menschen“ macht und indirekt dazu gezwungen wird, einen weiten Bereich seiner Privatsphäre aufzugeben. Der Staat erhält somit Einblick in Dinge, von denen unter Umständen nicht einmal der engste Freundeskreis oder die Familie wissen. Das Gefühl, permanent von öffentlicher Seite überwacht zu werden, löst bei vielen Menschen großes Unbehagen aus. Ein prominentes Beispiel, das immer wieder vorgebracht wird, um die Tragweite des Eingriffes, der durch die Vorratsdatenspeicherung verwirklicht wird, auf den Punkt zu bringen, wird auch vom Grünen Justizsprecher, Albert Steinhauser, aufgeworfen.

„Das ist so, als würde man die Post beauftragen, bei jedem Brief aufzuschreiben, wann er abgeschickt wurde, wann er befördert wurde und wem er zugestellt wurde, und als würde an jeder Straßenecke jemand stehen und notieren, wann man daran vorbeikommt. So ein Gesetz würde jeder als autoritär bezeichnen. In der elektronischen Kommunikation geht alles durch.“¹²⁹

¹²⁸ Mahnken, Mindestspeicherfristen für Telekommunikationsverbindungsdaten, Bundeskriminalamt, Pkt IV. 23.

¹²⁹ Profil, Biedermeier 2.0: Kriminelle müssen Vorratsdatenspeicherung nicht fürchten, www.profil.at/articles/11118/560/295826/biedermeier-2-0-kriminelle-muessen-vorratsdatenspeicherung-nicht-fuerchten (zuletzt abgerufen am 10.01.2013)

Dieser Einwand gegen die Vorratsdatenspeicherung lässt sich nicht völlig von der Hand weisen. Das eben dargestellte Szenario erinnert an Stasi-Methoden und löst wohl bei jedem ein zumindest befremdliches Gefühl aus. Der Unterschied zur Vorratsdatenspeicherung besteht darin, dass durch diese einerseits mehr Daten erfasst werden können, da ein Großteil der Kommunikation über Mobiltelefone und über das Internet stattfindet; gleichzeitig kann die Überwachung bei der Vorratsdatenspeicherung mit etwas Geschick jedoch auch umgangen werden.

Die Vorstellung, dass jemand Aufzeichnungen über unseren Aufenthaltsort führt und diese bei Bedarf an die Behörden weitergibt, ist für viele erschreckend.

Befürworterinnen und Befürworter der Vorratsdatenspeicherung erwähnen immer wieder, dass zwar verdachtsunabhängig gespeichert wird, jedoch der Überwachungsaspekt in Wahrheit nicht die Relevanz habe, die ihm von den Gegnerinnen und Gegnern der Vorratsdatenspeicherung beigemessen wird. Viel mehr würden die Daten ja nur bei einem konkreten Verdacht abgerufen.

Die bloße Tatsache allein, dass theoretisch die Bewegungsprofile und Kommunikationsgewohnheiten von praktisch jedem Menschen jederzeit abgerufen werden könnten, wird nicht als bedeutender Eingriff angesehen.

2. Jeder Mensch ein potentieller Schwerverbrecher

Die Empörung über die Vorratsdatenspeicherung wird zusätzlich noch dadurch verstärkt, dass die verdachtsunabhängige Vorratsdatenspeicherung auch als Ausdruck des Misstrauens des Staates gegenüber seinen Bürgern interpretiert werden kann. Mit anderen Worten: Dadurch, dass der Staat die Aufzeichnung und Speicherung der Daten aller vornimmt, und Unbescholtene auf derselben Grundlage wie verurteilte Kriminelle „überwacht“ werden dürfen, wird der Mensch zum potentiellen Schwerverbrecher gemacht: „Die Erfassung der Telekommunikationsverkehrsdaten betrifft jedermann zu jeder Zeit seiner Telekommunikation. Mit der Maßnahme, die das Vorfeld einer Gefahr oder eingetretener Strafbarkeit betrifft, geht die „Vermutung der Redlichkeit von jedermann“ verloren.

Jedermann wird – zwangsläufig – als potentieller Störer der öffentlichen Sicherheit angesehen.“¹³⁰

Gerade das immer wieder geäußerte Argument, dass derjenige, der nichts zu verbergen habe, ja auch nichts befürchten müsse, entkräftet solche, vor allem emotionalen Bedenken, kaum. Eine Maßnahme wie die Vorratsdatenspeicherung kann sehr wohl als Ausdruck des Verhältnisses zwischen Staat und Bürger gedeutet werden, da solche Überlegungen auch bei der Frage nach dem richtigen Strafrechtssystem und den damit verbundenen Maßnahmen relevant sind: „(...) Generalprävention und Spezialprävention, Tatstrafrecht und Täterstrafrecht – das sagt erst etwas Konkretes, wenn wir die Erziehungs- und Rechtsideale, die Tatauffassung und das Menschenbild kennen, von denen aus ein bestimmter geschichtlich gegebener Nationalstaat diese Gedanken verwertet.“¹³¹

Inwiefern die Vorstellung von dem per se bösen Menschen tatsächlich eine Rolle spielt, mag zweifelhaft sein. In jedem Fall kann jedoch argumentiert werden, dass die Annahme der Notwendigkeit präventiver Maßnahmen sehr wohl Aufschluss darüber gibt, dass ein gewisser Kontrollverlust befürchtet wird, der teilweise auch mit staatlichem Versagen zusammenhängen mag: „Wo Erziehung versagt, tritt Sicherung ein und sie bewährt sich auch als erstes und dringendstes kriminalpolitisches Bekämpfungsmittel, wird daher bei allen Reformarbeiten als Leitziel angesehen.“¹³²

3. Zweifelhafter Nutzen

Eine Frage, die immer wieder in der Diskussion um das Für und Wider der Vorratsdatenspeicherung genannt wird, ist jene nach dem Nutzen derselben. Während die Befürworterinnen und Befürworter immer von der Notwendigkeit der Bevorratung von Daten für die Bekämpfung schwerster Kriminalität sprechen, halten die Gegnerinnen und Gegner derselben mit dem Argument, dass die Vorratsdatenspeicherung in Wahrheit gar nicht zur Aufklärung oder gar zur Verhinderung von Straftaten beitrage, dagegen. Wie bereits oben kurz erwähnte, wurden auch Studien zu diesem Thema durchgeführt.

¹³⁰ Simon, Präzeptoraler Sicherheitsstaat und Risikovorsorge, Frankfurt am Main 2008, S. 289.

¹³¹ Blumenthal, Staatsidee und Strafzweck, Saalfeld 1935, S. 4.

¹³² Sauer, Allgemeine Strafrechtslehre, Berlin 1949, S. 9.

Dementsprechend interessant für die Frage nach dem Nutzen der Vorratsdatenspeicherung sind daher die Erkenntnisse der entsprechenden Studien.

Laut einer Studie¹³³ des Max-Planck Instituts wird der Zugang zu Telekommunikations-Verkehrsdaten immer wichtiger, jedoch ist dies abhängig vom konkreten Delikt. Unterschieden wird auch nach der Art der Verkehrsdatenabfrage. Für Delikte wie Betrugsdelikte, Kinderpornographie und Urheberrechtsverletzungen ist die Abfrage von IP Adressen durchaus oft im Einsatz. Bei Raub, Mord und Betäubungsmitteldelikten oder dem so genannten „Enkeltrick“¹³⁴ werden vor allem Telefonkontaktdaten ausgewertet.

Alles in allem wird jedoch im Forschungsbericht des Max-Planck-Instituts festgehalten, dass nur in 18% der Fälle Hinweise auf Verbindungen zur organisierten Kriminalität zu finden waren. Viel mehr sind jene Verfahren, bei denen die Verkehrsdaten abgefragt werden, viel eher der mittleren Kriminalität zuzuordnen. Nur in jedem fünften Fall kam es laut Forschungsbericht zu einer Verurteilung, und nur 16 % der tatsächlich Verurteilten erhielt eine Freiheitsstrafe von mehr als fünf Jahren.¹³⁵

Der Ansatz einer zweiten deutschen Studie, nämlich jener der Technischen Universität Darmstadt, war ein völlig anderer. Es wurde sich weniger mit Kriminalstatistiken auseinandergesetzt, als viel mehr eine Art Fallstudie durchgeführt. Vor allem nach den Anschlägen des 11. September in New York wurde großer Aufwand betrieben, um terroristische Aktivitäten zu verfolgen. Es wurden im Zuge dessen auch unterschiedliche Datenspeicherungs- und Verarbeitungssysteme eingeführt, wie beispielsweise auf Flughäfen (APIS), oder das so genannte *Terrorist Finance Tracking Program (TFTP)*.

Auch die Vorratsdatenspeicherung sollte ein Instrument darstellen, mit dessen Hilfe Daten in einem großen Rahmen analysiert werden können und das die Verhaltensmuster von gegenwärtigen und zukünftigen Terroristen offenlegen sollte. Aufgrund der doch sehr hohen

¹³³ Albrecht/Kilchling, Die Überwachung von Telekommunikations-Verkehrsdaten; Forschungsbericht Max-Planck-Gesellschaft, Max-Planck-Institut für ausländisches und internationales Strafrecht, 2009.

¹³⁴ Beim Enkeltrick geben sich Fremde gegenüber älteren Personen als deren Enkel oder sonstige Angehörige aus, um sie dazu zu überreden, ihnen beispielsweise Geld zu geben.

¹³⁵ Albrecht /Kilchling, Die Überwachung von Telekommunikations-Verkehrsdaten; Forschungsbericht Max-Planck-Gesellschaft, Max-Planck-Institut für ausländisches und internationales Strafrecht, 2009, S. 3.

Opportunitätskosten entschied man sich an der Technischen Universität Darmstadt schließlich, den Nutzen der Vorratsdatenspeicherung zu analysieren.¹³⁶

Dabei sollte untersucht werden, ob die flächendeckende Ansammlung von Daten es ermöglicht, terroristische Zellen in einem kontrollierten Umfeld zu identifizieren. Um dies festzustellen, wollte man sich mit Kommunikationsdynamiken auseinandersetzen. In weiterer Folge wurde eine Simulation vorgenommen:

„To empirically study the applicability of TDR¹³⁷ in a pre incident analysis scenario, we perform agent-based simulations of networks of communication users (called ‚ordinary users‘ in the sequel), which we amend with small networks of ‚terrorists‘. During the simulation, we keep a log file of all communication events of all agents (that is, both terrorists and ordinary users) in the same way as telecommunication providers implement TDR.“¹³⁸

Durch das Simulieren von Interaktionen „normaler“ Untersuchungsobjekten untereinander und auch jenem der „Terroristen“ sollten folgende Fragen geklärt werden:

Inwiefern unterscheidet sich die Kommunikation von „normalen“ Personen von jener der „Terroristen“? Welche Möglichkeiten gibt es, die „normalen“ Personen automatisiert von den „Terroristen“ zu unterscheiden? Funktioniert eine solche automatisierte Unterscheidung auch zuverlässig, wenn die Umgebung sich mitverändert?

Dazu wurde vor allem das Verhalten in großen Kommunikationsnetzwerken genau untersucht. Das Ergebnis war ernüchternd und bestätigt die Bedenken der Vorratsdatenspeicherungs-SkeptikerInnen:

Es wurde festgestellt, dass je länger der Zeitraum andauert, in dem die Daten gespeichert werden, desto größer ist die Information, die der/die Untersuchende hinsichtlich der Kommunikationsstrukturen seiner/ihrer Untersuchungsobjekte gewinnt. Allerdings werden gleichzeitig auch die Störfaktoren größer, was zu einer niedrigeren Erfolgsquote hinsichtlich der unterschiedlichen Klassifizierung der erfolgten Kommunikation führt.¹³⁹

Das heißt, das mit zunehmender Datenfülle das Ergebnis sich ab einem gewissen Zeitpunkt ins Negative verkehrt – es wird sozusagen öfter Alarm geschlagen, da das System fehleranfällig wird. Ein Mehr an Dateninformation führt also auch zu einem höheren

¹³⁶ Hamacher/Katzenbeisser, Public Security: Simulations Need to Replace Conventional Wisdom, 2011, S. 115.

¹³⁷ Anm.: TDR= Telecommunication Data Retention= Telekommunikationsdatenspeicherung.

¹³⁸ Hamacher/Katzenbeisser, Public Security: Simulations Need to Replace Conventional Wisdom, 2011, S. 116.

¹³⁹ Hamacher/Katzenbeisser, Public Security: Simulations Need to Replace Conventional Wisdom, 2011, S. 121.

Fehlerpotential. Im Ergebnis konnten die „Terroristen“ in der durchgeführten Fallstudie nicht anhand ihrer Kommunikationsmuster in der Gruppe identifiziert werden, was den Nutzen der Vorratsdatenspeicherung massiv in Frage stellt.

Gleichzeitig spielt in diesem Zusammenhang auch noch eine zweite Überlegung eine zentrale Rolle: Bei einem gewissen Aufwand ist es ohne Weiteres – lediglich mit ein paar technischen Grundkenntnissen – möglich, sich der Vorratsdatenspeicherung zu entziehen: „Telekommunikationsdaten sind bedeutungslos, wenn Kommunikationsnetze anonym genutzt werden können.“¹⁴⁰ Die Gefahr besteht nun vor allem darin, dass die Vorratsdatenspeicherung insbesondere jene Menschen betrifft, die im Grunde nichts Unrechtes getan haben, während diejenigen, die kriminell aktiv sind, sich eher die Mühe machen werden, der Vorratsdatenspeicherung zu entgehen.

Da nicht sämtliche Provider speicherpflichtig sind, sondern kleine Anbieter vom Gesetz nicht erfasst werden, ist es gerade für Kriminelle, die sich sogar zu Vereinigungen zusammengeschlossen haben und über einen hohen Organisationsgrad verfügen ein Leichtes, die Lücken im System für ihre Zwecke zu nützen. Was bleibt, ist im schlechtesten Fall eine Fülle an für die Strafverfolgung beziehungsweise Verhinderung von Verbrechen absolut irrelevanten Daten.

4. Die Gefahr des Missbrauchs

Zweifelsohne weist jedes politische System Schwachstellen auf. Gäbe es diese nicht, so wäre eine Maßnahme wie die der Vorratsdatenspeicherung obsolet. Bestünde nämlich nicht die latente Gefahr, dass Menschen kriminelle Aktivitäten setzen, so ließe sich kaum eine Begründung für die Notwendigkeit der Vorratsdatenspeicherung finden.

Aber eben gerade weil leider immer wieder Verhalten gesetzt wird, das nicht mit den gesetzlichen Vorgaben in Einklang steht, muss auch davon ausgegangen werden, dass es auch im unmittelbaren Zusammenhang mit der Vorratsdatenspeicherung zu Verfehlungen kommen kann. Daten und Information sind untrennbar mit Wissen verbunden. Wer über bestimmte

¹⁴⁰ Simon, Präzeptoraler Sicherheitsstaat und Risikovorsorge, Frankfurt am Main 2008, S. 284.

Daten oder Information verfügt oder diese abrufen kann, verfügt über die Fähigkeit, sich relativ einfach Wissen über andere Personen zuzueignen und dieses Wissen zu nützen.

Obgleich vermutlich ein Großteil der Informationen dieser Person nicht von großem Nutzen ist, kann es dennoch möglich sein, dass auch Information enthalten ist, die von Interesse für diejenigen sind, der diese Information abrufen, oder die von Interesse für jemanden sind, für den die Information abgerufen wird. Je mehr jemand über eine andere Person weiß, desto mehr Macht hat er über sie. Wo Macht ist, besteht auch immer die Gefahr des Missbrauchs derselben.

Wer über bestimmte Daten verfügt, ist in der Lage, eine nicht zu unterschätzende Macht über jemand anderen auszuüben, den diese Daten betreffen. Es ist kein Zufall, dass Datenmissbrauch, Cyberkriminalität und Ähnliches immer bedeutsamer werden, und somit sich auch zu einem immer größer werdenden Problem auswachsen.

Grundsätzlich hat der Gesetzgeber in zahlreichen Bestimmungen versucht, diesem Problem entgegenzuwirken. Die Gefahr des Missbrauchs der Information, die durch die Vorratsdatenspeicherung akkumuliert wird, kann dennoch nicht ausgeschlossen werden.

Das Missbrauchsrisiko besteht einerseits bereits bei denjenigen, die per Gesetz dazu verpflichtet werden, die Vorratsdatenspeicherung vorzunehmen und bei den Mitarbeiterinnen und Mitarbeitern der betroffenen Unternehmen, die sich Zugang zu den gespeicherten Daten verschaffen können. Sie stellen die erste Risikogruppe dar. Eine zweite Risikogruppe sind Externe, die sich widerrechtlich Zugang zu dem Datenpool verschaffen können, und die dort enthaltene Information zu ihrem eigenen Vorteil und zum Nachteil eines anderen nützen können. Schließlich gibt es eine dritte Risikogruppe, und zwar die Behörden, die grundsätzlich – aber nur unter gewissen Voraussetzungen – die Serviceprovider um Auskunft ersuchen können.

Gerade wenn man annimmt, dass die Vorratsdaten Aufschluss über die Lebensweise von Personen, ihre Kontakte, ihre Bewegungsmuster geben können, liegt der Gedanke nahe, dass früher oder später auch jemand auf die Idee kommen könnte, dieses Wissen über faktisch alle Personen gegen das staatliche System zu verwenden. Dies erscheint freilich ein extremes Szenario zu sein.

Etwas naheliegender erscheint jedoch, dass jemand, der gute Kontakte zu den Sicherheitsbehörden beziehungsweise einzelnen dort beschäftigten Personen hat, sich seinen

Einfluss zu Nutze machen könnte, um – sei es auch nur privat – andere Personen überprüfen zu lassen oder die Vorratsdaten auszuwerten.

Ist ein solcher Datenpool hingegen gar nicht vorhanden, so kann auch kein Missbrauch stattfinden.

Dass der Spielraum der Sicherheitsbehörden für die Beauskunftung der Vorratsdaten zu weit ist, wird ebenfalls oft ins Treffen geführt. Zwar gibt es, wie oben bereits dargestellt, durchaus gesetzliche Vorgaben, wann ein Gericht oder die Staatsanwaltschaft den Abruf von Vorratsdaten bewilligen muss, und wann die Sicherheitsbehörden autonom anordnen können, die Vorratsdaten herauszugeben. Gleichzeitig muss jedoch hinterfragt werden, ob und inwieweit sich die Behörden tatsächlich an diese Auflagen halten beziehungsweise, ob es nicht eventuell zu einfach ist, *ex post* den Abruf von Vorratsdaten durch das Konstruieren eines Vorwandes oder Verdachts zu rechtfertigen.

Befürworterinnen und Befürworter der Vorratsdatenspeicherung mögen an dieser Stelle vor allem ins Treffen führen, dass schließlich auch kontrolliert werde, ob die Voraussetzungen für die Abfrage der gespeicherten Vorratsdaten auch tatsächlich vorlagen. Diese Rolle kommt dem so genannten Rechtsschutzbeauftragten zu. Dessen primäre Aufgabe ist es, ganz generell zur „Wahrnehmung des Rechtsschutzes im Ermittlungsdienst der Sicherheitsbehörden“¹⁴¹ zu sorgen. Davon umfasst sind grundsätzlich nur Ermittlungen, welche die Sicherheitsorgane unter Berufung auf Aufgaben und Befugnisse des Sicherheitspolizeigesetzes durchführen, nicht umfasst davon sind beispielsweise Ermittlung der Polizei im Dienste der Strafrechtspflege.¹⁴² Als konkreter Gegenstand des „besonderen“ Rechtsschutzes sind die auf Befugnisse des Sicherheitspolizeigesetzes gestützte Maßnahmen, mit Hilfe derer personenbezogene Daten ermittelt werden sollen. Zunächst hat der/die Betroffene nämlich keine Kenntnis von diesen Ermittlungshandlungen, daher kann er/sie seinen/ihren Rechtsschutz selbst nicht wahrnehmen, sodass diese Aufgabe dem Rechtsschutzbeauftragten zuteil wird.

Unter bestimmten Voraussetzungen wird daher eine Meldung zur nachprüfenden Kontrolle an den Rechtsschutzbeauftragten übermittelt.

¹⁴¹ Sicherheitspolizeigesetz, § 91a Abs 1.

¹⁴² Burgstaller, Sicherheitspolizeiliche Ermittlungshandlungen unter Kontrolle des Rechtsschutzbeauftragten beim BMI, ÖJZ 2011/69, S 643.

Im Jahr 2010 wurden insgesamt 2.228 Meldungen an den Rechtsschutzbeauftragten übermittelt. 938 davon, insgesamt also 42% dieser Meldungen bezog sich auf die Ermittlung von Standortdaten.¹⁴³ Die Ermittlung von Standortdaten von Mobiltelefonen stellt somit die mit Abstand häufigste an den Rechtsschutzbeauftragten meldepflichtige Ermittlungsmaßnahme der Polizei dar, was wiederum deutlich zeigt, dass die Standortdaten in jedem Fall – ob nun gerechtfertigt oder nicht – ganz offensichtlich häufig als Ermittlungsmethode herangezogen werden.

5. *Gefährliches Wissen*

Wie bereits kurz erwähnt, können Daten, selbst wenn sie mit den besten Intentionen gesammelt werden, relativ leicht in die falschen Hände geraten. Wenn dies passiert, kann der Schaden verheerend sein.

Angenommen, Daten werden auf Vorrat gespeichert, um für ein gerechteres System mit einer geringeren Kriminalitätsrate und einer größeren Aufklärungsquote zu sorgen. Was passiert, wenn im Extremfall das System kippt und plötzlich die gesamte Datenfülle tatsächlich nicht mehr bloß in konkreten Anlassfällen abgerufen wird, sondern einfach kontrollierend und zur Absicherung eines autoritären Systems Verwendung finden?

In einem Staat wie Österreich, in dem sich die meisten wohl trotz aller Kritik und gelegentlichen politischen Skandalen relativ sicher fühlen, mag das Wort „Systemumsturz“ fremd und sehr theoretisch klingen.

Doch bereits die Überlegung, dass die Vorratsdatenspeicherung, auf einer EU-Richtlinie beruhend, auch von allen anderen Mitgliedstaaten der Europäischen Union umgesetzt werden muss, lässt diese – einem worst case Szenario gleichende – Vorstellung gleich etwas weniger utopisch erscheinen, zumal nicht alle Staaten gleich stabil sind und immer wieder extreme Tendenzen hervorbrechen, die international durchaus für Aufregung sorgen und bedenklich sind.

¹⁴³ Burgstaller, Sicherheitspolizeiliche Ermittlungshandlungen unter Kontrolle des Rechtsschutzbeauftragten beim BMI, ÖJZ 2011/69, S 646.

6. Unsicherheit – was können Vorratsdaten (anrichten)?

Was den Gegnerinnen und Gegnern der Vorratsdatenspeicherung sicherlich besonderen Zulauf brachte und Auftrieb verlieh, ist die Unklarheit der Bedeutung und des Ausmaßes der gesetzlichen Regelung. Es wurde kaum kommuniziert, zumindest nicht auf eine wirklich verständliche Weise, welche Daten von wem gespeichert werden und was man mit diesen Daten anfangen kann, beziehungsweise, damit in Zusammenhang stehend, was man nicht diesen Daten auch anrichten kann.

Klar ist, dass keine Inhaltsdaten gespeichert werden. Dies ist weder von der EU-Richtlinie so vorgesehen, noch durch den nationalen Gesetzgeber gewünscht oder initiiert. Es ist beispielsweise unmöglich aufgrund der Vorratsdatenspeicherung festzustellen, welche Websites ein Internetuser/ eine Internetuserin besucht hat, oder welchen Inhalt diese Websites haben. Es kann auch nicht festgestellt werden, was in einem Telefonat besprochen wurde oder wer tatsächlich abgehoben hat.

Nichts desto trotz stellt sich – nicht nur SkeptikerInnen der Vorratsdatenspeicherung – die Frage, was genau sich aus Standort- und Kommunikationsdaten ermitteln lässt.

Die Antwort darauf lässt sich relativ klar geben: Es lässt sich herausfiltern, von welchem E-Mail Account wann an welchen Empfänger/ an welche Empfängerin eine E-Mail geschickt wurde, sowie von welchem Handy aus wer zu welcher Zeit angerufen wurde. Des Weiteren lässt sich ermitteln, an welchem Ort sich ein bestimmtes Mobiltelefon zu einem gewissen Zeitpunkt befand.

Aus diesen Informationen lässt sich somit herausfiltern, wer Kontakt zu welchen Personen hat, ob Person A eine Person B kennt. Es lässt sich feststellen, wo sich eine Person mit einem Mobiltelefon zu einem gewissen Zeitpunkt befand, und es lassen sich somit sogar Bewegungsprofile erstellen.

Wenn Person A beispielsweise an einem Montag Morgen im Büro in Wien mit dem Mobiltelefon anruft und bekannt gibt, nicht zur Arbeit erscheinen zu können, da sie krank im Bett liege, so ließe sich theoretisch schon allein aufgrund der Standortdaten nachweisen, wenn Person A sich in Wahrheit hunderte Kilometer weiter westlich in Tirol in einem Thermenhotel befindet.

Abgesehen von der Tatsache, dass Person A durch den Anruf etwas moralisch Falsches tut und vermutlich auch gegen den Arbeitsvertrag verstößt, zeigt dieses Beispiel doch recht plakativ, dass die Vorratsdatenspeicherung – wenn missbräuchlich auf Daten zugegriffen wird – nicht nur Schwerstkriminelle, die „etwas zu verbergen haben“ in Bedrängnis bringen können, sondern theoretisch auch jede/ jeden Einzelne(n), der/die gegen privatrechtliche oder auch nur gesellschaftliche Konventionen verstößt.

7. Welche Handlung macht einen verdächtig

Es wurde bereits vorgebracht, dass SkeptikerInnen der Vorratsdatenspeicherung grundsätzlich kritisieren, dass der Staat seinen StaatsbürgerInnen als Gesamtheit die Unschuldsvermutung aberkennt und durch die anlassunabhängige Speicherung von Verkehrs- und Standortdaten viel mehr das Bild eines Generalverdachts gegenüber allen vermittelt wird.

Was jedoch insbesondere bemängelt wird ist, dass man durch bestimmte Verhaltensweisen sich auch tatsächlich relativ schnell in einer Situation wiederfinden kann, die für die Ermittlerinnen und Ermittler einen Verdacht begründen und diese dazu veranlasst, die Vorratsdaten einer Person abzurufen. Insbesondere die ARGE Daten bringt hier vor, dass „typische“ Verhaltensmuster von Kriminellen auf alle Bürgerinnen und Bürger übertragen würden:

So lassen beispielsweise kurze Telefonate mit vielen verschiedenen, aber wiederkehrenden Telefonnummern relativ leicht den Verdacht entstehen, die betroffene Person sei ein Drogendealerinnen und Drogendealer, die/der sich telefonisch mit den Kundinnen/Kunden Abholtermine vereinbart.

Lange Telefonate mit einer Zeitungsredaktion können auf Geheimnisverrat hindeuten.

Bei vielen eingehenden Anrufen von immer neuen Anschlüssen beim Handy einer Frau könnte als Hinweis auf Geheimprostitution gedeutet werden. Und schließlich sei auch nicht auszuschließen, dass regelmäßig wiederkehrende Anrufreihenfolgen als Hinweise auf organisierte Kriminalität oder Terrorismus mit genau definierten Informationsbeziehungsweise Befehlsstrukturen gedeutet werden könnten.

Auch regelmäßige Anrufe bei einer liechtensteinischen Bank könnten verdächtig sein und schnell den Eindruck erwecken, dass der oder die Betroffene Geldwäsche betreibt, Steuern hinterzieht oder Terrorismus finanziert.¹⁴⁴

Bedenklich erscheint den Initiatoren der ARGE Daten vor allem, dass bei einem einmal vorliegenden Verdacht und eventuellen Ermittlungen relativ schnell und unwiederbringlich der gute Ruf einer an sich unschuldigen und unbescholtenen Person beschädigt werden könnte.

8. Nur ein erster Schritt in die falsche Richtung

Die Kritik an der Vorratsdatenspeicherung orientiert sich nicht ausschließlich am rechtlichen und gegenwärtigen Status quo. Mit Argumenten, die sich darauf berufen, dass de facto ohnehin die meisten Provider auch ohne rechtliche Grundlage bisher schon Daten auf Vorrat gespeichert hätten, lassen sich die KritikerInnen nicht abpeisen.

Die Tatsache, dass nunmehr die Vorratsdatenspeicherung rechtlich nicht nur legitimiert, sondern auch geboten ist, zeigt nämlich auch eine Veränderung der Bewertung des Charakters der Vorratsdatenspeicherung.

Sie wird nicht mehr bloß still geduldet, sie wird aktiv gefordert. Ihre gesetzliche Verankerung spiegelt einen Trend wider, und zwar jenen, der in Richtung zunehmender Kontrolle für mehr Sicherheit zeigt, selbst wenn der Preis für diese Sicherheit das Aufgeben eines beachtlichen Teils der Privatsphäre ist.

Diejenigen, die ohnehin bereits die Praxis der Vorratsdatenspeicherung skeptisch sehen, fragen sich, wohin dieser Trend führen soll. Ist das Speichern von Verkehrs- und Standortdaten auf Vorrat tatsächlich das Ziel? Oder ist es nur ein weiterer Schritt in Richtung einer umfassenden Überwachung? Wird in Zukunft im Namen der Sicherheit auch die temporäre Abspeicherung von Inhaltsdaten zulässig sein?

Zusammengefasst könnte man sagen, dieses letzte Contra-Argument der Vorratsdatenspeicherungs-Gegnerin und Gegnerinnen zielt auf Zukünftiges ab und beschäftigt

¹⁴⁴ Vgl. dazu ARGE Daten (2011): Vorratsdatenspeicherung ist Beginn präventivstaatlicher Maßnahmen. Abrufbar unter: http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=36951the (zuletzt abgerufen am 21.01.2013)

sich vor allem mit einer gewissen Tendenz, die als falsch und gefährlich eingeschätzt wird, als ersten Schritt einer schleichenden Aushöhlung eines verfassungsmäßig gewährleisteten Rechts, nämlich jenem auf Privatsphäre.

9. Immer weitere Entfernung von europäischen Werten

Bereits die bislang aufgezählten Argumente weisen auf eine Entwicklung hin, die mit den europäischen Werten weitgehend im Widerspruch steht, und auch die „Grundfreiheiten im Binnenmarkt“¹⁴⁵ nachhaltig beeinflusst.

Vorstellbar – und keineswegs aus der Luft gegriffen – ist beispielsweise, dass die unternehmerische Freizügigkeit durch die „Überwachung“, die durch die Vorratsdatenspeicherung zusätzlich begünstigt wird, beeinträchtigt werden könnte. So macht es die Vorratsdatenspeicherung, unabhängig von deren eigentlicher Zweckwidmung leichter möglich, die Schritte eines/einer Unternehmers/Unternehmerin nachzuvollziehen,¹⁴⁶ seine/ihre Kontakte festzustellen und somit auch seine unternehmerischen Vorhaben zu kennen.

Doch auch andere Grundwerte, die nicht nur in Österreich einen sehr hohen Stellenwert haben, sondern auch zu den Grundwerten der Europäischen Union zählen, können indirekt von der Vorratsdatenspeicherung berührt werden. Die bereits erläuterte Möglichkeit, Bewegungsprofile zu erstellen, macht auch vor Kirchen oder Vereinslokalen keinen Halt. Es ist durchaus auch diskutierbar, ob die Religionsfreiheit¹⁴⁷ nicht – wenngleich vielleicht auch nur indirekt – dadurch berührt werden könnte, wenn jederzeit nachvollzogen werden kann, wer sich zu welcher Zeit in welcher Kirche aufhält, wer seine Religion aktiv praktiziert. Fraglich ist, ob dies nicht auch dazu führen könnte, auf eine „Liste von Verdächtigen“ zu gelangen.

Auch kritische Vereine, die – einmal ganz losgelöst von etwaiger Rechtfertigbarkeit – ohnehin leichter zum Objekt staatlicher Beobachtung oder Überwachung werden, sind von

¹⁴⁵ Vgl. dazu den Vertrag über die Arbeitsweise der Europäischen Union, AEUV.

¹⁴⁶ Vgl. Weh, Verfassungsgerichtshof prüft Vorratsdatenspeicherung, ZUV 2013, 32, S 35.

¹⁴⁷ Glaubens- und Gewissensfreiheit, Artikel 14 Staatsgrundgesetz 1867.

der Überwachung im weitesten Sinne betroffen. Es könnte daher auch die Vereinsfreiheit¹⁴⁸ beeinflusst werden. Die Vorratsdatenspeicherung hat also durchaus Potential, auch weitere Grundrechte, nicht bloß jenes auf Privatsphäre, in ihren Auswirkungen zu beeinträchtigen.

10. Einschränkung der Meinungsfreiheit?

Ein weiterer triftiger Grund zu Kritik an der Vorratsdatenspeicherung stellt das Bedenken der Einschränkung der Meinungsfreiheit¹⁴⁹ dar. So wird vermehrt ins Treffen geführt, dass das bloße Wissen um die Existenz der Vorratsdatenspeicherung geeignet sei, auf die Kommunikationsteilnehmerinnen und Teilnehmer Druck auszuüben, und sie somit zu einer Änderung ihres Kommunikationsverhaltens zu führen vermag.¹⁵⁰

Diese Bedenken werden vor allem auch durch die vielen Tipps und Tricks, wie man sich vor der Vorratsdatenspeicherung „schützen“ kann, die auch in diversen Datenschützer- Blogs angeboten werden, zum Ausdruck gebracht. Das Potential, das Verhalten von Vorratsdatenspeicher-Skeptikerinnen und Skeptikern auch im Alltag maßgeblich und nachhaltig zu verändern, ist ganz losgelöst von der Frage, ob eine solch ausgeprägte Skepsis eigentlich tatsächlich begründet ist, enorm und nicht nur aus ethischer, sondern auch aus rechtlicher Sicht problematisch. Denn bereits das Setzen von Maßnahmen, die geeignet sind, das „natürliche“ Kommunikationsverhalten eines Menschen zu verändern, stellt einen Eingriff in die Kommunikations- und Meinungsfreiheit dar und ist somit verfassungsrechtlich bedenklich.

Bei der Betrachtung bestimmter Berufsgruppen, wie beispielsweise jene der Journalistinnen und Journalisten, sind sogar noch drastischere Auswirkungen der Vorratsdatenspeicherung zu erkennen, als auf den ersten Blick zu vermuten wäre: So ist beispielsweise das Bedenken, das Wissen ob der Nachweisbarkeit des Kommunikationsverhaltens könne weiterführend auch negativ in die Pressefreiheit einfließen, nicht gänzlich von der Hand zu weisen.

¹⁴⁸ Versammlungs- und Vereinsfreiheit, Artikel 12 Staatsgrundgesetz 1867.

¹⁴⁹ Meinungs- und Pressefreiheit, Artikel 13 Staatsgrundgesetz 1867.

¹⁵⁰ Vgl. Weh, Verfassungsgerichtshof prüft Vorratsdatenspeicherung, ZUV 2013, 32, S. 34.

Dass die Vorratsdatenspeicherung – aus diversen Gründen – verfassungsrechtlich nicht ganz unbedenklich ist, scheint auch der österreichische Verfassungsgerichtshof so zu sehen. Dieser beschloss daher, die Richtlinie über die Vorratsdatenspeicherung dem Europäischen Gerichtshof zur Prüfung auf ihre unionsrechtliche Grundrechtskonformität vorzulegen.

Dies ist deshalb notwendig, da der Verfassungsgerichtshof zwar die nationalen Normen prüfen kann, ihm jedoch keine Prüfungskompetenz bei Unionsrecht zukommen und die betroffenen nationalen Normen auf einer unionsrechtlichen Richtlinie basieren.

7. Zusammenfassung

Nunmehr gilt es, die eingangs gestellten Fragen nochmals zusammenfassend – so weit wie möglich auch abschließend – zu beantworten und ein paar abschließende Gedanken zu formulieren:

a) Entfernen wir uns immer weiter von einer liberalen Verfassung?

Wie im Zuge dieser Arbeit bereits angesprochen, scheint sich der Fokus von den Grundfesten „Freiheit und Staat“ immer mehr zu „Sicherheit und Staat“ zu verschieben. Jahrzehnte, wenn nicht Jahrhunderte lang wurde für einen liberaleren Staat gekämpft, in dem der/die Einzelne frei sein sollte, seine/ihre Entscheidungen selbstbestimmt, aber auch auf eigene Verantwortung zu treffen. Der Begriff des „Liberalismus“ ist, egal ob im wirtschaftlichen Kontext oder davon losgelöst betrachtet, ist einerseits mit dem Gefühl erweiterter Möglichkeiten, Freiheiten konnotiert. Gleichzeitig versteckt sich hinter dem Wort auch das Risiko, die Gefahr, die jeder, ob freiwilliger oder unfreiwilliger Kontrollverlust mit sich bringt.

Lange Zeit herrschte die Überzeugung, dass der Entzug aus der allumfassenden staatlichen Kontrolle, ein Entkommen von der allumfassenden Macht und Kontrolle des absolutistischen Herrschers, oberstes Ziel sein müsse, damit der Mensch sich frei entfalten könne. Es gab die Bereitschaft dazu, selbst einen Teil der Verantwortung zu tragen, um im Gegenzug mehr Freiheiten zu erlangen und vor allem, um frei für sich selbst entscheiden zu können. Es gab die Bereitschaft dazu, auch ein Risiko einzugehen, einen Kontrollverlust in Kauf zu nehmen, um Alternativen eröffnet zu bekommen und sich individuell entfalten zu können. Für die Chance, etwas zu gewinnen, wurde ein möglicher Verlust in Kauf genommen.

Lange Zeit wurden die schrittweise errungenen kleinen Freiheiten für fast unantastbar erklärt. Betrachtet man beispielsweise das Staatsgrundgesetz aus dem Jahr 1867, so wird bewusst, wie hoch das Bewusstsein um den Stellenwert der liberalen Grundrechte zu dieser Zeit gewesen sein musste. Fast alle der dort normierten Grundrechte sind als Abwehrrechte gegenüber dem Staat konzipiert: die Personenfreizügigkeit, die Eigentumsfreiheit, die

Erwerbsfreiheit, die Unverletzlichkeit des Hausrechtes, das Briefgeheimnis, das Fernmeldegeheimnis, das Petitionsrecht, die Versammlungs- und Vereinsfreiheit, die Meinungs- und Pressefreiheit, die Glaubens- und Gewissensfreiheit, die Freiheit der Lehre und Wissenschaft, die Kunstfreiheit, die freie Berufswahl.

Dass diese Rechte und Freiheiten, die uns heute durchwegs selbstverständlich erscheinen, eigentlich ursprünglich nicht – vor allem nicht jedem – gewährleistet waren, wird oftmals vergessen.

Diese Rechte sind jedoch gleichzeitig Bedingung dafür als auch Konsequenz daraus, dass von mündigen Staatsbürgerinnen und Staatsbürgern ausgegangen werden muss.

Nicht vergessen werden darf jedoch, dass es stets die Möglichkeit gab, auch die liberalen Grundrechte einzuschränken. Diese Möglichkeit der Einschränkung ist auch als etwas durchaus Positives zu sehen, da ein Gewähren von umfassenden Freiheiten auch immer dazu führen kann, dass diese Freiheiten in einem solchen Ausmaße gelebt werden, dass dies sich auf die Freiheiten anderer im Staat auswirkt. Das auch der vorliegenden Arbeit zu Grunde liegende Problem ist nämlich, dass die Gewährleistung von Freiheiten bei Weitem nicht die einzige Aufgabe des Staates ist. Vielmehr hat er auch andere Aufgaben zu erfüllen und einen möglichst guten Ausgleich zwischen vielseitigen, unterschiedlichen Interessen herzustellen. Dazu ist eine gewisse Kompromissbereitschaft unabdinglich.

Im konkreten Fall sieht die Kollision der Interessen folgendermaßen aus: Einerseits soll der Staat seine Bürger schützen und ihnen größtmögliche Sicherheit gegen interne, aber auch externe Angriffe im weitesten Sinne bieten; andererseits soll vermieden werden, dass dieser Schutz auf Kosten der liberalen Rechte derjenigen erfolgt, denen die staatlichen Maßnahmen zu Gute kommen sollen.

Da die Interessen im konkreten Fall jedoch einander entgegen stehen, muss eine Entscheidung getroffen werden. Die oben gestellte Frage wird also neu formuliert: Geht der Trend hin zu mehr Kontrolle und Sicherheit, selbst wenn dies die Einschränkung der liberalen Grundrechte mit sich bringt? Eine Prognose ist naturgemäß schwierig aber dennoch wird das Risiko in dieser Conclusio eingegangen und eine Antwort gegeben. Und ebenso risikofreudig wie die Verfasserin dieser Arbeit selbst wird die Einstellung der Europäerinnen und Europäer eingeschätzt: Die rege Diskussion ob der bereits ergangenen Richtlinie, die Vielzahl an Initiativen und das Medieninteresse in Österreich aber auch in anderen Staaten der Europäischen Union, ebenso wie die Bedenken des Verfassungsgerichtshofes sind ein deutliches Indiz dafür, dass keine Bereitschaft dazu besteht, für Argumente der Sicherheit und

des Terrorismusschutzes liberale Grundrechte aufzugeben, die über einen langen Zeitraum hinweg hart erkämpft wurden und die fast jede Europäerin und jeder Europäer für nahezu selbstverständlich erachtet. Die Frage nach dem Trend zu mehr Sicherheit auf Kosten der Freiheit wird daher mit einem klaren Nein beantwortet.

Aus einem – wohl notwendigen – gesamteuropäischen Betrachtungsweise heraus ergibt sich nämlich, dass die Europäerinnen und Europäer wohl keinen Anlass sehen, der eine solche Verschiebung der Prioritäten rechtfertigen würde, und es in Wirklichkeit wohl auch gar keinen solchen Grund gibt. Zweifelsohne gab es auch vor fünfzig oder hundert Jahren Bedrohungsszenarien innerhalb Europas, die wohl noch viel unmittelbarer waren als dies heute der Fall ist.

In der Diskussion um die Notwendigkeit der besseren Verfolgung schwerer Straftaten und der Terrorismusprävention wird nämlich ein ganz essentielles Argument immer wieder vernachlässigt oder schlichtweg vergessen: Europa war wohl nie so sicher wie heute. Diese Sicherheit ist auch bestimmt kein Resultat staatlicher Überwachung, als viel mehr das freiwilliger, zwischenstaatlicher Kooperation und Diplomatie.

Weshalb Bereitschaft bestehe sollte, Freiheitsrechte aufzugeben und worin das Argument für die Notwendigkeit der Einschränkung liberaler Rechte gesehen werden sollte, ist daher nicht nachzuvollziehen.

Der Trend weg von den liberalen Grundrechten und eine Verschiebung zu Gunsten der Sicherheit ist also nur eine scheinbare und wird sich in der Praxis nicht durchsetzen.

b) Werden Sicherheit und Prävention in unserer Gesellschaft höher eingestuft als Privatsphäre und freie Meinungsäußerung?

Sicherheit und Prävention ist in unserer Gesellschaft sicherlich ein hoher Stellenwert zuzuschreiben. Ganz allgemein ist Sicherheit ein großes Thema, und Prävention, beispielsweise hinsichtlich der Vorbeugung gegen Gewaltverbrechen, ist den Menschen ein wichtiges Anliegen. In Relation zur Bedeutung von Privatsphäre und der freien Meinungsäußerung wirkt dieser grundsätzlich hohe Rang, den Sicherheit in unserem

Wertesystem einnimmt, nicht mehr ganz so herausragend. Sicherheit mag per se zwar als etwas durchaus Essentielles betrachtet werden, die Vorkehrung präventiver Maßnahmen ist jedoch, sofern sich aus ihr negative Auswirkungen auf die Privatsphäre und freie Meinungsäußerung ergeben, nur eingeschränkt erwünscht.

Losgelöst von den vorstehenden Beobachtungen mag Sicherheit zwar durchaus an der Spitze der Prioritäten vieler Menschen stehen, gleichzeitig ist das geringe Maß an Sicherheitszuwachs, das von der Vorratsdatenspeicherung erwartet werden kann nicht ausreichend, um Abstriche bei der Privatsphäre und der freien Meinungsäußerung zuzulassen.

c) Wie drastisch sind die Auswirkungen der Gesetzgebung zur Vorratsdatenspeicherung wirklich?

Immer wieder wird das Argument vorgebracht, die Auswirkungen der Vorratsdatenspeicherung seien in Wahrheit nicht so drastisch, wie dies in den Medien behauptet würde. Zweifelsohne war die Berichtserstattung zur Vorratsdatenspeicherung bislang eher darauf konzentriert, die Nachteile derselben ins Treffen zu führen, anstatt beispielsweise auch klarzustellen, dass Inhaltsdaten von dieser gar nicht umfasst sind. Ergo mag es stimmen, dass die tatsächlichen Auswirkungen der Vorratsdatenspeicherung gar nicht so weit reichend sind, wie – vor allem wenig informierte Bürgerinnen und Bürger – glauben könnten. Gleichzeitig ist jedoch die Verharmlosung der Befürworterinnen und Befürworter der Vorratsdatenspeicherung auch nicht ganz zutreffend. Selbst wenn keine Inhaltsdaten von der Vorratsdatenspeicherung erfasst werden, so ist jedoch das Potential von Verkehrsdaten ebenfalls nicht zu unterschätzen. Die Möglichkeit der Erstellung ausführlicher Bewegungsprofile ist keineswegs ein bloß leichter Eingriff in die Privatsphäre der Menschen, sondern durchaus ernst zu nehmen. Durch Technik wird es machbar, aufzuzeichnen, wer mit wem wie lang und zu welchem Zeitpunkt von welchem Ort aus Kontakt hatte. Die Macht, die solche Informationen mit sich bringen, ist nicht zu unterschätzen.

Alles in allem sind also Aussagen, die ganz allgemein das Potential der Vorratsdatenspeicherung als gering ansetzen, schlichtweg falsch.

Losgelöst davon zu sehen ist freilich die Frage, wie sich die Vorratsdatenspeicherung in der Praxis gestalten wird. Zieht man zur Beantwortung dieser Frage lediglich die Ziele – wie bei

der Formulierung der Vorratsdatenspeicherrichtlinie verwendet – heran, so ist die das Speichern von Vorratsdaten eigentlich unbedenklich. Bleibt es bei der theoretischen Möglichkeit, die gesammelten Daten auszuwerten und zu analysieren, ist das Gros der Europäerinnen und Europäer davon nicht betroffen.

Jedoch liegt es – wie an mehreren Beispielen weiter oben ausgeführt – durchaus im Bereich des Möglichen, dass auch unbescholtene Menschen, die sich zu keinem Zeitpunkt etwas strafrechtlich Relevantes zu Schulden haben kommen lassen, auf das Radar von Ermittlern und Ermittlerinnen gelangen und zu unfreiwillig zu direkt Betroffenen werden. Insofern ist die Vorratsdatenspeicherung bereits als weit weniger „unproblematisch“ einzustufen.

Ein weiteres Risiko liegt selbstverständlich im Datenmissbrauch: Ein Sammelsurium an Daten, zentral verwaltet, birgt ein enormes Gefährdungspotential in sich. Dass Unbefugte auf die Daten zugreifen, aber auch, dass innerhalb der Reihen derjenigen, die mit der Verwaltung dieser Daten betraut sind, Missbrauch erfolgt, kann schlichtweg nicht ausgeschlossen werden. Was in einem solchen Fall passieren könnte, bleibt vorerst den Phantasien der/des Einzelnen überlassen.

Die Möglichkeiten, die durch die Vorratsdatenspeicherung eröffnet werden, sind jedenfalls enorm. Sich darauf zu beschränken zu sagen, es sei ohnehin auch bisher zur (illegalen) Speicherung solcher Daten gekommen, löst das Problem nicht, sondern verlagert dieses bloß auf eine andere Stufe. Es ist vielmehr als bedenklich zu sehen, dass einer solchen Massenspeicherung ohne tatsächlich eine Risikoevaluierung vorzunehmen nunmehr auch eine rechtliche Grundlage gegeben wurde.

d) Abschließende Gedanken

Nach der umfassenden Analyse der rechtlichen Grundlagen der Vorratsdatenspeicherung, deren potentieller Auswirkung und den technischen Möglichkeiten, sollen nunmehr ein paar abschließende Gedanken zu der allgemeinen Diskussion und Grundproblematik formuliert werden.

Wenn eine Maßnahme wie die der Vorratsdatenspeicherung eingeführt wird, so ist immer danach zu fragen, was tatsächlich die Intention dahinter ist. Will man dem Staat nicht unterstellen, seine Bürgerinnen und Bürger lediglich bespitzeln und kontrollieren zu wollen,

so sind zunächst die von der Europäischen Union im Zuge der Erlassung der Richtlinie ins Treffen geführten Sicherheitsargumente zu evaluieren, die sicherlich nicht von vornherein von der Hand gewiesen werden sollten. Diese sind vor allem auch im Zusammenhang mit der nationalstaatlichen Umsetzung der Richtlinie gegen liberale Überlegungen abzuwägen:

„Der Konflikt zwischen der Erfüllung der Schutzpflicht und der verfassungsrechtlichen Freiheit wird auch und vor allem durch das einfache Gesetz gesteuert. Gesetze sind fast nie ausschließlich freiheitsbeschränkend oder freiheitsschützend. Gesetze sollen im Idealfall einen Ausgleich zwischen den widerstrebenden Interessen herstellen. Freiheit wird nach allgemeiner Auffassung erst durch legislatives Handeln überhaupt geschaffen, selbst wenn damit die Beschränkung – naturrechtlich verstandener – Freiheit verbunden ist.“¹⁵¹

Zweifelsohne wird durch legislatives Handeln der Grundstein für die Freiheiten im Staat überhaupt gelegt. Ein gewisses Maß an Kontrolle und auch Einschränkung der Freiheit des Einzelnen ist (leider) notwendig, um größtmögliche Freiheit für alle zu gewährleisten.

Zu diesen Einschränkungen gehören sicherlich auch Maßnahmen zur Verstärkung von Sicherheit und zur Bekämpfung von Kriminalität.

Dennoch sollte bei solchen Überlegungen auch immer das Verhältnis der gesetzten Maßnahme zu ihrer eigenen Wirkung, als auch die Verhältnismäßigkeit der Maßnahme zu ihren Auswirkungen auf andere Bereiche, die für das tägliche Leben der Menschen von Bedeutung sind, im Blick behalten werden.

Wird unter Berücksichtigung aller Umstände ein krasses Missverhältnis zwischen Kosten und Nutzen festgestellt, ist eine solche Maßnahme keinesfalls rechtfertigbar.

Die Bedeutung der Grundrechte kann gar nicht zu hoch veranschlagt werden: „Sie werden eingeleitet und bestimmt durch die Menschenwürde, die jedem Menschen allein durch sein Menschsein zukommt. Die Entwicklung eines Menschen in seiner Würde setzt Raum zur Entfaltung des Menschen voraus. Und so sollten die Abwehrrechte einen staatsfreien Raum belassen, in dem der Mensch unreglementiert, unkontrolliert, nur der eigenen Willkür unterworfen, sein Leben eigenverantwortlich sollte gestalten können.“¹⁵²

¹⁵¹ Simon, Präzeptoraler Sicherheitsstaat und Risikoversorge, Frankfurt am Main 2008, S. 175.

¹⁵² Simon, Präzeptoraler Sicherheitsstaat und Risikoversorge, Frankfurt am Main 2008, S. 299.

Welcher Nutzen tatsächlich aus der Vorratsdatenspeicherung erfolgt, ist ebenfalls fraglich, wobei die Verhinderung von Straftaten durch die Vorratsdatenspeicherung wohl kaum gewährleistet werden kann: „Es kann sicherlich ohne weiteres angenommen werden, dass die Bevorratung von Verkehrsdaten und der Zugriff auf diese Daten allein einer repressiven Strafverfolgung überhaupt dienen kann.“¹⁵³

Ihr Nutzen könnte jedoch allenfalls darin gesehen werden, dass bislang unentdeckte Straftaten durch sie nunmehr aufgeklärt werden könnten.¹⁵⁴ Allerdings kann man die Vorratsdatenspeicherung – radikal ausgedrückt – in ihrer jetzigen Form fast als präventive Vorverurteilung aller ansehen, und somit auch als präventive Bestrafung aller, da fast jede(r) zumindest indirekt von der Bevorratung der Daten betroffen ist. Hier stellt sich wiederum die fast philosophische Frage nach der Natur des Strafrechts, und welche Art des Strafrechts und der Strafe erwünscht ist. Dies ist immer auch unter ideologischen Gesichtspunkten zu bewerten: „Der Strafzweck und die sittliche Rechtfertigung der Strafe, die Art ihrer Ausgestaltung, alle diese Fragen sind in ihrer jeweils gültigen Lösung weltanschaulich bedingt.“¹⁵⁵

Allein der Einführung der Vorratsdatenspeicherung kommt daher bereits eine bestimmte Symbolik zu, die gewissermaßen den Zeitgeist widerspiegelt. Doch viel mehr wird der eigentliche Zeitgeist durch die Reaktionen der Menschen in den unterschiedlichsten Mitgliedstaaten der Europäischen Union zum Ausdruck gebracht und gezeigt, dass bezüglich des Großteils dieser Menschen keine Bereitschaft besteht, ihre Freiheiten einschränken zu lassen, auch nicht im Namen der Sicherheit.

Wenn man auf die Entstehungsgeschichte um die Vorratsdatenspeicherung blickt, so könnte man zu der Schlussfolgerung gelangen, dass es sich dabei um Anlassgesetzgebung handelte. Dass das Einsetzen der Diskussionen zum systematischen Sammeln von Daten zeitlich knapp nach einer Reihe terroristischer Akte erfolgte, ist kein Zufall. Es ist zwar mehr als fraglich, ob diese Anschläge hätten verhindert werden können, wäre die Vorratsdatenspeicherung bereits zu einem früheren Zeitpunkt erfolgt; nichtsdestotrotz ist jedenfalls eindeutig, dass die Geschehnisse zu jener Zeit das Kernargument für die Vorratsdatenspeicherung waren.

¹⁵³ Simon, Präzeptoraler Sicherheitsstaat und Risikovorsorge, Frankfurt am Main 2008, S. 280.

¹⁵⁴ Simon, Präzeptoraler Sicherheitsstaat und Risikovorsorge, Frankfurt am Main 2008, S. 281.

¹⁵⁵ Dahm/Schaffstein, Liberales oder autoritäres Strafrecht, Hamburg 1932, S. 7.

Genaue Überlegungen führen zu dem Schluss, dass die Bevorratung von Verkehrsdaten eigentlich im Widerspruch zu sonstigen kürzlich eingeführten gesetzlichen Bestimmungen des Bereichs der elektronischen Daten steht.

Der eigentliche Trend war und ist – eben mit Ausnahme der Vorratsdatenspeicherung – einer, der die Datensicherheit und den Datenschutz in den Mittelpunkt stellt. So fand beispielsweise der Schutz personenbezogener Daten durch Artikel 8 der europäischen Grundrechtecharta explizit Eingang in das Primärrecht der Europäischen Union, was durchaus bemerkenswert ist und den Stellenwert elektronischer Daten nochmals besonders deutlich hervorhebt. Auch in Artikel 16 AEUV wurde der Schutz personenbezogener Daten verankert.

Diese Entwicklungen im Datenschutzrecht sind nicht überraschend, sondern die logische Konsequenz der Tatsache, dass moderne Kommunikationsmittel wie Internet im weitesten Sinne, aber auch Mobiltelefone einen unglaublichen Verbreitungsgrad erreicht haben.

Während als auf europäischer Ebene, aber auch auf nationalstaatlicher grundsätzlich erkannt wurde, welche Bedeutung dem Datenschutz zukommt und auch in Zukunft zukommen wird, welches Potential in Daten liegt und welchen – auch wirtschaftlichen – Wert Daten haben und konsequenterweise der Datenschutz sogar als Grundrecht verankert wurde, ist es doch überraschend, dass plötzlich all diesen Entwicklungen zuwiderlaufend die Vorratsdatenspeicherung derart schnell in eine Richtlinie gegossen wurde.

Allein aus systematischen Überlegungen heraus sind daher die Chancen, dass die Vorratsdatenspeicherung tatsächlich rückgängig gemacht wird, als nicht unrealistisch einzustufen.

Es konnten außerdem keine schlüssigen Nachweise erbracht werden, die der Vorratsdatenspeicherung das Potential attestieren, Akte von Terrorismus sowie organisierte Kriminalität zu verhindern und sich positiv auf die Kriminalstatistik auszuwirken. Und obgleich der Schutz seiner Bürgerinnen und Bürger sicherlich eine wichtige Aufgabe des Staates darstellt, so kann er diese einerseits ohnehin nicht vollständig erfüllen:

„Die Gefahren von Organisierter Kriminalität und Terrorismus können durch den Staat ebenfalls nicht gänzlich beseitigt werden. (...) Will man auch das kleinste Risiko menschlichen Verhaltens vermeiden, so beginnt der Staat, der nur wegen und aus der Freiheit

seiner Bürger besteht (...) sich gegen seine ‚Erfinder‘ zu wenden.“¹⁵⁶ Dem Gesetzgeber kommt die wichtige Aufgabe zu, die Interessen, die durch neue Gesetze berührt werden könnten, zunächst zu erkennen und in einem weiteren Schritt abzuwägen, welches Interesse schwerer wiegt. Eine solche Interessenabwägung ist im Fall der Vorratsdatenspeicherung ganz offensichtlich unzureichend erfolgt.

Eine derart drastische Maßnahme, deren Geeignetheit den von ihr verfolgten Zweck zu erfüllen zweifelhaft ist, sollte auf keinen Fall in die Freiheitsrechte eingreifen.

Es bleibt daher zu hoffen, dass bei der Prüfung der Vorratsdatenspeicherrichtlinie auf ihre Grundrechtskonformität mit größerer Sorgfalt vorgegangen werden wird.

Neben der Verletzung diverser liberaler Grundrechte ist auch die Tatsache, dass sämtliche Personen, die von der Vorratsdatenspeicherung betroffen sind, in Wahrheit unter Generalverdacht zu stehen scheinen, was aus ideologischer Sicht mehr als bedenklich ist da de facto in den Lebensbereich aller Betroffenen eingegriffen wird, bevor überhaupt klar ist, ob jemals eine Straftat von Seiten der betroffenen Person gesetzt werden wird, ob es einen Versuch geben wird, welche Absichten jemand hat.

Dieser Generalverdacht stellt die Grundproblematik dar, ist jedoch bei Weitem noch nicht das größte Problem an der Vorratsdatenspeicherung. Denn das Stehen unter Generalverdacht mag zwar ideologisch bedenklich sein und wirkt sich unter Umständen auch – wie eben durch die Einschränkung gewisser anderer Rechte – auf das Leben der Betroffenen aus. Noch kritischer wird die Lage jedoch dann, wenn jemand auch ganz konkret verdächtigt wird, sich beispielsweise durch ein gewisses Kommunikationsverhalten verdächtig macht. In einem solchen Fall wird den Behörden nämlich unheimliche Macht und ein weiter Handlungsspielraum eingeräumt, und auch wenn sich im Nachhinein der Verdacht vielleicht gar nicht bestätigt und ein gewisses, „verdächtiges“ Kommunikationsverhalten einfach Zufall war, so können konkret gesetzte Handlungen nicht mehr rückgängig gemacht werden, der Eingriff ist bereits erfolgt.

Wie unzuverlässig die Auswertung gewissen Kommunikationsverhaltens nach festgelegten Parametern ist, wird durch die oben zitierte Studie doch recht deutlich zum Ausdruck gebracht. Indizien sind eben keine Beweise und diese Unterscheidung war seit jeher wichtig.

¹⁵⁶ Simon, Präzeptoraler Sicherheitsstaat und Risikovorsorge, Frankfurt am Main 2008, S. 154.

„Die bloße straflose Vorbereitung tritt in das Stadium des strafwürdigen Versuches mit der unmittelbaren konkreten Gefährdung eines bestimmten Rechtsguts in einer besonderen (individuell bestimmten) Sachlage. Bisher bestand, wenn überhaupt, nur eine unbestimmte, generelle Gefahr, deren Richtung und Entladung für ein objektives Wahrscheinlichkeitsurteil nicht voraussehbar war. Wenn jemand Gift kauft oder mit einer Schusswaffe, mit Dietrich und Zange das Haus verläßt, so weiß ein objektiver Beobachter nicht, wann und wo ein Verbrechen, welches und gegen wen, begangen wird, selbst wenn der Täter sich durch gewisse Redensarten verdächtig macht, so daß ein Zweifel über kriminelle Absicht nicht besteht.“¹⁵⁷

Es wäre nun selbstverständlich möglich zu sagen, dass diese Problematik eben in der Natur präventiver Maßnahmen liegt, und dass es unmöglich ist, mit dem Einschreiten von Behörden so lange zu warten bis zweifelsfrei feststeht, dass ein krimineller Akt gesetzt werden wird, da in einem solchen Falle nie eine Straftat verhindert werden könnte. Dies mag stimmen und zweifelsfrei muss den Behörden hier ein gewisser Handlungsspielraum zugestanden werden. Dies ist jedoch im bestehenden Strafrecht, nach der Strafprozessordnung, ohnehin der Fall. Die Möglichkeiten der Ermittlerinnen und Ermittler sind weitreichend, wenn es einen begründeten Verdacht gibt. Dies ist auch legitim und wichtig.

Das präventive Ansammeln von Daten, die – zumindest auf den zweiten, genaueren Blick – gar nicht so harmlos sind, wie man auf den ersten Blick vermuten würde, ist jedoch in Anbetracht des oben Ausgeführten als überzogene und wohl auch grundrechtswidrige Maßnahme zu sehen.

Wenn gesagt wird, das Sammeln von Daten sei in Wahrheit schon allein deshalb unproblematisch, da die meisten Menschen diese ohnehin auf diversen Plattformen im Internet, wie beispielsweise Facebook, Twitter ecetera preisgeben, kann ebensowenig als Argument für die Vorratsdatenspeicherung dienen: Es mag zwar stimmen, dass viele Personen sehr leichtsinnig mit ihren personenbezogenen Daten umgehen.

Doch der Unterschied besteht schon allein darin, dass grundsätzlich jede(r) selbst entscheiden sollte, welche Daten er oder sie der Öffentlichkeit zur Verfügung stellen will, und welche

¹⁵⁷ Sauer, Allgemeine Strafrechtslehre, Berlin 1949, S. 90.

nicht. Jedenfalls ist darin keine Rechtfertigung für eine einseitige Ermächtigung zu sehen, sich bestimmte Daten aller zu besorgen, diese zu sammeln und zu speichern.

Der anstehenden Entscheidung, die auf europäischer Ebene gefällt werden wird, ist ganz losgelöst von den konkreten Auswirkungen der Vorratsdatenspeicherung auf die davon Betroffenen eine unglaubliche Bedeutung beizumessen. Sie wird insofern richtungsweisend sein, als die Europäische Union sich zu den gemeinsamen Verfassungstraditionen bekennt und ein ganz essentieller Bestandteil dieser Verfassungen eben die liberalen Grundrechte darstellen. Sollte der Europäische Gerichtshof der Ansicht sein, dass die Vorratsdatenspeicherrichtlinie gegen europäisches Primärrecht verstößt, und diese als inexistenten Rechtsakt qualifizieren, so werden auch die innerstaatlichen Umsetzungsakte, sprich, die auf Grundlage der Richtlinie erlassenen Gesetze, aufzuheben sein.

Selbst im Haager Programm von November 2004 betonte der Europäische Rat, dass der Terrorismus unter uneingeschränkter Wahrung der Grundrechte zu verhüten und zu bekämpfen ist,¹⁵⁸ was sinngemäß auch für die Bekämpfung organisierter Kriminalität gelten muss. Von uneingeschränkter Wahrung der Grundrechte kann bei derart drastischen Maßnahmen jedoch kaum noch gesprochen werden. Vielmehr ist nachvollziehbar, dass so manche Bürgerin und so mancher Bürger das Gefühl bekommen kann, „auf Schritt und Tritt vom Staat verfolgt“¹⁵⁹ zu werden und zwar unabhängig von der Setzung delinquenten Verhaltens. Von Verhältnismäßigkeit kann daher vor allem dann keine Rede sein, wenn die Regelungen zur Datensicherheit, zu den Zwecken und zur Transparenz der Datenverwendung sowie zum Rechtsschutz nicht den verfassungsrechtlichen Anforderungen entsprechen.¹⁶⁰

¹⁵⁸ Benn-Ibler, Gemeinsame Kriminalitäts- und Terrorbekämpfung im Spannungsverhältnis zu den europäischen Bürgerrechten, AnwBl 2008, S. 12.

¹⁵⁹ Weh, Verfassungsgerichtshof prüft Vorratsdatenspeicherung, ZUV 2013, S. 33.

¹⁶⁰ Otto/Seitlinger, Zur Umsetzung der Data Retention-Richtlinie in Österreich. Der Begutachtungsentwurf des Ludwig Boltzmann Instituts für Menschenrechte im Lichte der Entscheidung des Bundesverfassungsgerichts vom 2.3.2010, MR 2010, S. 63.

8. Nachwort

Eine genaue Analyse der Vorratsdatenspeicherung, der pro und contra Argumente und der damit verbundenen Emotionen verdeutlicht, dass es sich um einen Rechtsakt besonders großer Tragweite handelt.

Die akute Missbrauchsgefahr stellt ein immenses Risiko dar, und der Schaden, der in einem tatsächlichen Missbrauchsfall angerichtet werden könnte, ist kaum abschätzbar und kann nur erahnt werden: „Daten, die einmal vorhanden sind, sind bereits dadurch akut gefährdet, ihr Missbrauch liegt geradezu in der Natur ihrer Existenz.“¹⁶¹

Und dennoch wurde die Richtlinie zur Vorratsdatenspeicherung relativ rasch erlassen und schließlich, wenn auch teils widerwillig, von den Mitgliedstaaten der Europäischen Union umgesetzt. Auf Kritik wurde bislang kaum merklich reagiert.

Der immer wieder von Seiten der Politik verlautbarte Spruch „Wer nichts verbrochen hat, hat nichts zu verbergen“ ist ein Totschlagargument, das in Wahrheit nicht dazu geeignet ist, Kritikerinnen und Kritiker zu beruhigen, sondern eher die Vermutung nahe legt, dass man sich durch Kritik erst recht verdächtig mache.

Aussagen dieser Art sind besorgniserregend und vermitteln den Eindruck, dass Eingriffe in die Freiheitsrechte, in die Privatsphäre der Menschen mittlerweile von einigen als etwas Selbstverständliches, etwas Unvermeidbares angesehen werden.

Wenn in einem Staat die Grundrechte nicht mehr oberste Priorität haben, wenn Freiheitsrechte nach Belieben beschränkt werden können, und im Namen der Sicherheit eine fast schrankenlose Dauerüberwachung des Kommunikationsverhaltens aller ermöglicht wird – in welcher Art von Staat leben wir dann?

In einem demokratischen Rechtsstaat, in dem der Einzelne letztlich bewusst an der Verantwortung für politische Prozesse mitzutragen hat, muss die Wahrung der Grundrechte oberste Priorität haben. Logische Konsequenz daraus ist, dass eine Einschränkung der Freiheiten in einem modernen, demokratischen Rechtsstaat auf das kleinstmögliche Maß

¹⁶¹ Weh, Verfassungsgerichtshof prüft Vorratsdatenspeicherung, ZUV 2013, S. 35.

reduziert werden muss.¹⁶² Dass mehr Freiheiten auch mit mehr Risiken verbunden sind, muss schlichtweg akzeptiert werden.

„Sicherheit um jeden Preis“ ist wohl nur in einem Präventivstaat wie jenem aus George Orwells Roman 1984 vorstellbar, in dem das Ausmaß an staatlicher Kontrolle so ausgeprägt ist, dass selbst falsche Gedanken strafbar sind.

Sind die europäischen Staaten tatsächlich auf dem besten Weg dazu, zu Präventivstaaten nach dem Vorbild Orwells „Ozeanien“ zu werden, und die Europäerinnen und Europäer dabei, zu gläsernen Menschen zu werden – *sicherheitshalber*?

Ein vielleicht etwas überzogener Gedanke. Dennoch würde es wohl nicht schaden, 1984 (nochmals) zur Hand zu nehmen, ein paar Vergleiche anzustellen und eventuelle Parallelen aufzuspüren. Selbstverständlich bloß *sicherheitshalber*.

¹⁶² Benn-Ibler, Gemeinsame Kriminalitäts- und Terrorbekämpfung im Spannungsverhältnis zu den europäischen Bürgerrechten, AnwBl 2008, S. 14.

Literatur

Primärliteratur

- Bundesverfassungsgesetz über den Schutz der persönlichen Freiheit
- Datenschutzgesetz 2000
- Erkenntnis des Verwaltungsgerichtshofes vom 30.09.1997, VwSlg 14748 A/1997
- Europäische Menschenrechtskonvention
- Gesetz zum Schutze des Hausrechts
- Richtlinie 2006/24/EG
- Richtlinie 2002/58/EG
- Sicherheitspolizeigesetz
- Staatsgrundgesetz 1867
- Strafgesetzbuch
- Strafprozessordnung
- Telekommunikationsgesetz
- Vertrag über die Arbeitsweise der Europäischen Union

Internetquellen

- ARGE Daten: www.argedaten.at
- AK Vorrat: www.akvorrat.at
- Bundeskriminalamt Deutschland: www.bka.de
- Der Standard: <http://derstandard.at>
- Die Presse: <http://diepresse.com>
- Die Zeit: www.zeit.de
- Parlament - Aussendung, Reden: www.parlament.gv.at
- Profil: www.profil.at
- Spiegel Online: www.spiegel.de

Sekundärliteratur

- Adamovich, Ludwig/Funk, Bernd-Christian/Holzinger, Gerhard: Österreichisches Staatsrecht³. Grundrechte. Wien 2003.
- Ahrens, Jörn Hans Peter: Der Beginn des Staatsgeheimnisses im deutschen und ausländischen Staatsschutzrecht. Hamburg 1966.
- Albrecht, Hans-Jörg/Kilchling, Michael: Die Überwachung von Telekommunikations-Verkehrsdaten; Forschungsbericht Max-Planck-Gesellschaft, Max-Planck-Institut für ausländisches und internationales Strafrecht, 2009.
- Benn-Ibler, Gerhard: Gemeinsame Kriminalitäts- und Terrorbekämpfung im Spannungsverhältnis zu den europäischen Bürgerrechten. AnwBl 2008, 12.
- Berka, Walter: Lehrbuch Verfassungsrecht². Wien 2008.

- Blumenthal, Alfred: Staatsidee und Strafzweck. Saalfeld 1935.
- Burgstaller, Manfred: Sicherheitspolizeiliche Ermittlungshandlungen unter Kontrolle des Rechtsschutzbeauftragten beim BMI, ÖJZ 2011/69, 2011.
- Dahm, Georg/Schaffstein, Friedrich: Lieberales oder autoritäres Strafrecht, in: Blumenthal, Alfred: Staatsidee und Strafzweck. Saalfeld 1935.
- Ehs, Tamara/ Gschiegl, Stefan/ Ucakar, Karl/ Welan, Manfred: Politik und Recht. Spannungsfelder der Gesellschaft, Wien 2012.
- Feiler, Lukas/ Stahov, Ana: Die Einführung der Vorratsdatenspeicherung in Österreich. MR 2011, 111.
- Felsner, Karol: Vorratsdatenspeicherung. Juridikum 2011, 31.
- Flechtheim, Ossip Kurt: Hegels Strafrechtstheorie. Brünn 1936.
- Funk, Bernd-Christian: Grund- und Menschenrechte im Spannungsfeld zwischen Politik und Recht, in Ehs, Tamara/ Gschiegl, Stefan/ Ucakar, Karl/ Welan, Manfred: Politik und Recht. Spannungsfelder der Gesellschaft, Wien 2012.
- Greco, Luis: Feindstrafrecht. Baden-Baden 2010.
- Hamacher, Kay/ Katzenbeisser, Stefan: Public Security: Simulations Need to Replace Conventional Wisdom, 2011.
- Hegel, Georg Wilhelm Friedrich: Grundlinien der Philosophie des Rechts, zit. in WK² Vor §§ 32–36 Rz 6.
- Hengstschläger, Johannes/Leeb, David: Grundrechte, Wien 2012.
- Höpfel, Frank/Ratz, Eckart: Wiener Kommentar zum StGB², 2005-2013.
- Larenz, Karl (Hg): Rechtsidee und Strafrechtsgedanke. Berlin 1930.
- Lurger, Das Europarecht aus der Perspektive des Unionsbürgers, ZfRV, Graz 2000.
- Mahnken, Eva: Mindestspeicherfristen für Telekommunikationsverbindungsdaten, Bundeskriminalamt 2005.
- Noll, Alfred-Johannes: Sicherheitsstaat Österreich? Kritik der Sicherheitsgesetzgebung. ÖVDJ, Wien 1991.
- Öhlinger, Theo: Verfassungsrecht⁸. Wien 2009.
- Öhlinger, Theo: Verfassung und Verfassungsrecht zwischen Politik und Recht, in Ehs, Tamara/ Gschiegl, Stefan/ Ucakar, Karl/ Welan, Manfred: Politik und Recht. Spannungsfelder der Gesellschaft, Wien 2012.
- Gerald Otto/Michael Seitlinger: Zur Umsetzung der Data Retention-Richtlinie in Österreich. Der Begutachtungsentwurf des Ludwig Boltzmann Instituts für Menschenrechte im Lichte der Entscheidung des Bundesverfassungsgerichts vom 2.3.2010, MR 2010.
- Sauer, Wilhelm: Allgemeine Strafrechtslehre. Berlin, 1949.
- Schönert, Jörg (Hg): Literatur und Kriminalität. Tübingen 1983.
- Simon, Dirk: Präzeptoraler Sicherheitsstaat und Risikoversorge. Frankfurt am Main 2008.
- Weh, Wilfried Ludwig: Verfassungsgerichtshof prüft Vorratsdatenspeicherung, ZUV 2013.
- Weissel, Erwin: Sicherheit um jeden Preis? ZfRV 1998.
- Westphal, Dietrich: Die Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten. Neues aus Brüssel zum Verhältnis von Sicherheit und Datenschutz in der Informationsgesellschaft. Juridikum 2006, 34.

9. Anhang

Zusammenfassung:

Diese Arbeit beschäftigt sich mit Spannungsverhältnissen zwischen unterschiedlichen staatlichen Aufgaben. Das liberale Grundprinzip der Verfassung soll die Freiheit des Einzelnen garantieren. Gleichzeitig ist jedoch auch Sicherheit im weitesten Sinne eine der obersten Prioritäten des Staates.

Anhand des Beispiels der Vorratsdatenspeicherung zeigt sich deutlich, dass die Freiheit der/des Einzelnen relativ schnell mit Sicherheitsinteressen kollidieren kann. Dies insbesondere deshalb, da Sicherheit zumeist auch durch die Einrichtung gewisser Kontroll- und Überwachungsmechanismen gewährleistet werden soll.

Die vorliegende Arbeit analysiert die Rolle der Gesetzgebung in diesem Zusammenhang und thematisiert das Zusammenspiel von Politik, Gesellschaft und Recht.

Die Gesetzgebung zur Vorratsdatenspeicherung berührt gleich mehrere Grundrechte, allesamt Freiheitsrechte. Auf diese Grundrechte wird explizit eingegangen und dargestellt, unter welchen Voraussetzungen eine Einschränkung dieser fundamentalen Rechte zulässig ist.

Anschließend werden die positiven Aspekte der Vorratsdatenspeicherung analysiert und darauf eingegangen, wie es zur Vorratsdatenspeicherrichtlinie und zur Einführung der Vorratsdatenspeicherung in Österreich kam. Auch der öffentliche Diskurs zu diesem Thema wird skizziert.

Es folgt eine umfassende Interessenabwägung. Berücksichtigt wird dabei auch das immense Risiko des Missbrauchs, das allein schon durch das bloße Sammeln von Daten gegeben ist.

Betrachtet man die Vorratsdatenspeicherung, ihr Potential und ihre Auswirkungen genauer, so fragt man sich: Entfernen wir uns immer weiter von einer liberalen Verfassung, und verliert Freiheit ihren Stellenwert in Anbetracht globaler Bedrohungsszenarien? Diese und ähnliche Fragen stehen im Zentrum der arbeitsgegenständlichen Analyse.

Abstract:

This paper deals with the relationship and possible tensions between different government functions. The basic principle of the liberal constitution should guarantee the freedom of the individual. At the same time, however, security is also one of the top priorities of the state.

Using the example of data retention it is clear that the freedom of individuals can easily clash with security interests. This might be the case because safety should often be ensured by the establishment of certain control and monitoring mechanisms.

This paper analyzes the role of the legislator in this context and focuses on the interaction between politics, society and law.

The data retention legislation affects several fundamental rights, mainly liberal rights. Those liberal rights can be limited under certain conditions.

In this context the positive aspects of the data retention are analyzed. Also, the history of the Data Retention Directive and its implementation in Austria will be discussed and the public discourse on this topic is outlined.

A comprehensive weighing of interests once again shows the immense risk of abuse, which derives from the mere collection of data.

Taking a closer look at the data retention legislation, its potential and its effects, one might wonder: Are we moving further and further away from a liberal constitution? Is freedom losing its significance in the light of global threats? These questions are to be answered by the present thesis.

Die Autorin, geboren 1988, stammt aus dem Salzburger Pinzgau. Sie studierte Politik- und Rechtswissenschaften in Wien. Während der Studienfokus im Bakkalaureatsstudium zunächst auf internationaler Politik lag, ergab sich aus der Kombination der beiden Studienfächer allmählich ein verstärktes Interesse an der Staatswissenschaft. Insbesondere beschäftigte sich die Autorin mit verfassungs- und grundrechtlichen Fragen und den Wechselwirkungen zwischen Gesetzgebung und Politik. Einen weiteren Forschungsschwerpunkt bildet die Analyse von Prozessen auf Unionsebene und deren Auswirkung auf die österreichische Gesetzgebung.

1. STAATSGRUNDGESETZ

Artikel 9. Das Hausrecht ist unverletzlich.

Das bestehende Gesetz vom 27. October 1862 (Reichs-Gesetz-Blatt Nr. 88) zum Schutze des Hausrechtes wird hiemit als Bestandtheil dieses Staatsgrundgesetzes erklärt.

Artikel 12. Die österreichischen Staatsbürger haben das Recht, sich zu versammeln und Vereine zu bilden. Die Ausübung dieser Rechte wird durch besondere Gesetze geregelt.

Artikel 13. Jedermann hat das Recht, durch Wort, Schrift, Druck oder durch bildliche Darstellung seine Meinung innerhalb der gesetzlichen Schranken frei zu äußern.

Die Presse darf weder unter Censur gestellt, noch durch das Concessions-System beschränkt werden. Administrative Postverbote finden auf inländische Druckschriften keine Anwendung.

Artikel 14. Die volle Glaubens- und Gewissensfreiheit ist Jedermann gewährleistet.

Der Genuß der bürgerlichen und politischen Rechte ist von dem Religionsbekenntnisse unabhängig; doch darf den staatsbürgerlichen Pflichten durch das Religionsbekenntniß kein Abbruch geschehen.

Niemand kann zu einer kirchlichen Handlung oder zur Theilnahme an einer kirchlichen Feierlichkeit gezwungen werden, in sofern er nicht der nach dem Gesetze hiezu berechtigten Gewalt eines Anderen untersteht.

2. EUROPÄISCHE MENSCHENRECHTSKONVENTION

Artikel 8 - Recht auf Achtung des Privat- und Familienlebens

(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.

(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

Artikel 10 - Freiheit der Meinungsäußerung

(1) 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. Dieser Artikel schließt nicht aus, daß die Staaten Rundfunk-, Lichtspiel- oder Fernsehunternehmen einem Genehmigungsverfahren unterwerfen.

(2) Da die Ausübung dieser Freiheiten Pflichten und Verantwortung mit sich bringt, kann sie bestimmten, vom Gesetz vorgesehenen Formvorschriften, Bedingungen, Einschränkungen oder Strafdrohungen unterworfen werden, wie sie in einer demokratischen Gesellschaft im Interesse der nationalen Sicherheit, der territorialen Unversehrtheit oder der öffentlichen Sicherheit, der Aufrechterhaltung der Ordnung und der Verbrechensverhütung, des Schutzes der Gesundheit und der Moral, des Schutzes des guten Rufes oder der Rechte anderer unentbehrlich sind, um die Verbreitung von vertraulichen Nachrichten zu verhindern oder das Ansehen und die Unparteilichkeit der Rechtsprechung zu gewährleisten.

3. DATENSCHUTZGESETZ

Artikel 1

(Verfassungsbestimmung)

Grundrecht auf Datenschutz

§ 1. (1) 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. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBI. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

(5) Gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, ist, 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. In allen übrigen Fällen ist die Datenschutzkommission zur Entscheidung zuständig, es sei denn, daß Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind.

Artikel 2

1. Abschnitt

Allgemeines

Definitionen

§ 4. Im Sinne der folgenden Bestimmungen dieses Bundesgesetzes bedeuten die Begriffe:

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;
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;
3. „Betroffener“: jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden;
4. Auftraggeber: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden (Z 8), unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen. Sie gelten auch dann als Auftraggeber, wenn der mit der Herstellung eines Werkes beauftragte Dienstleister (Z 5) die Entscheidung trifft, zu diesem Zweck Daten zu verwenden (Z 8), es sei denn dies wurde ihm ausdrücklich untersagt oder der Beauftragte hat auf Grund von Rechtsvorschriften oder Verhaltensregeln über die Verwendung eigenverantwortlich zu entscheiden;
5. Dienstleister: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwenden (Z 8);

6. „Datei“: strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;
7. „Datenanwendung“: die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung);
8. Verwenden von Daten: jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten;
9. Verarbeiten von Daten: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittels (Z 12) von Daten;
10. Anm.: aufgehoben;
11. Überlassen von Daten: die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses (Z 5);
12. Übermitteln von Daten: die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;
13. „Informationsverbundsystem“: die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, daß jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden;
14. „Zustimmung“: die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, daß er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt;
15. „Niederlassung“: jede durch feste Einrichtungen an einem bestimmten Ort räumlich und funktional abgegrenzte Organisationseinheit mit oder ohne Rechtspersönlichkeit, die am Ort ihrer Einrichtung auch tatsächlich Tätigkeiten ausübt.

Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten

§ 9. Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten ausschließlich dann nicht verletzt, wenn

1. der Betroffene die Daten offenkundig selbst öffentlich gemacht hat oder
2. die Daten in nur indirekt personenbezogener Form verwendet werden oder
3. sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen, oder
4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung ihrer Verpflichtung zur Amtshilfe geschieht oder
5. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben, oder
6. der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
7. die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder
8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist oder
9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
10. Daten für private Zwecke gemäß § 45 oder für wissenschaftliche Forschung oder Statistik gemäß § 46, zur Benachrichtigung oder Befragung des Betroffenen gemäß § 47 oder im Katastrophenfall gemäß § 48a verwendet werden oder
11. die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und sie nach besonderen Rechtsvorschriften zulässig ist, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse im Hinblick auf die Datenverwendung unberührt bleiben, oder
12. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder
13. nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen

ihrer erlaubten Tätigkeit verarbeiten und es sich hierbei um Daten von Mitgliedern, Förderern oder sonstigen Personen handelt, die regelmäßig ihr Interesse für den Tätigkeitszweck der Vereinigung bekundet haben; diese Daten dürfen, sofern sich aus gesetzlichen Vorschriften nichts anderes ergibt, nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden.

4. TELEKOMMUNIKATIONSGESETZ

Kommunikationsgeheimnis, Datenschutz

Allgemeines

§ 92. (1) Die Bestimmungen dieses Abschnitts gelten für die Verarbeitung und Übermittlung von personenbezogenen Daten in Verbindung mit der Bereitstellung öffentlicher Kommunikationsdienste in öffentlichen Kommunikationsnetzen einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen. Soweit dieses Bundesgesetz nicht anderes bestimmt, sind auf die in diesem Bundesgesetz geregelten Sachverhalte die Bestimmungen des Datenschutzgesetzes 2000, BGBI. I Nr. 165/1999, anzuwenden.

(2) Die Bestimmungen der Strafprozessordnung bleiben durch die Bestimmungen dieses Abschnittes unberührt.

(3) In diesem Abschnitt bezeichnet unbeschadet des § 3 der Begriff

1. “Anbieter” Betreiber von öffentlichen Kommunikationsdiensten;
2. “Benutzer” eine natürliche Person, die einen öffentlichen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst zwangsläufig abonniert zu haben;
 - 2a. „Teilnehmerkennung“ jene Kennung, welche die eindeutige Zuordnung eines Kommunikationsvorgangs zu einem Teilnehmer ermöglicht;
 - 2b. „E-Mail-Adresse“ die eindeutige Kennung, die einem elektronischen Postfach von einem Internet-E-Mail-Anbieter zugewiesen wird;
3. „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:
 - a) Name (Familiennamen und Vorname bei natürlichen Personen, Name bzw. Bezeichnung bei juristischen Personen),
 - b) akademischer Grad bei natürlichen Personen,
 - c) Anschrift (Wohnadresse bei natürlichen Personen, Sitz bzw. Rechnungsadresse bei juristischen Personen),
 - d) Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,
 - e) Information über Art und Inhalt des Vertragsverhältnisses,

f) Bonität;

4. “Verkehrsdaten” Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

4a. “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;

5. “Inhaltsdaten” die Inhalte übertragener Nachrichten (Z 7);

6. “Standortdaten” Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben, im Fall von festen Telekommunikationsendeinrichtungen sind Standortdaten die Adresse der Einrichtung;

6a. „Standortkennung“ die Kennung einer Funkzelle, über welche eine Mobilfunkverbindung hergestellt wird (Cell-ID);

6b. „Vorratsdaten“ Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a gespeichert werden;

7. “Nachricht” jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können;

8. „Anruf“ eine über einen öffentlichen Telefondienst aufgebaute Verbindung, die eine zwei- oder mehrseitige Echtzeit-Kommunikation ermöglicht;

8a. „erfolgloser Anrufversuch“ einen Telefonanruf, bei dem die Verbindung erfolgreich aufgebaut wurde, der aber unbeantwortet bleibt oder bei dem das Netzwerkmanagement eingegriffen hat;

9. “Dienst mit Zusatznutzen” jeden Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht;

10. „elektronische Post“ jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird;
11. „elektronisches Postfach“ ein elektronisches Ablagesystem, das einem Teilnehmer eines E-Mail-Dienstes zugeordnet ist;
12. „E-Mail“ elektronische Post, die über das Internet auf Basis des „Simple Mail Transfer Protocol“ (SMTP) versendet wird;
13. „Internet-Telefondienst“ einen öffentlichen Telefondienst im Sinne des § 3 Z 16, der auf paketvermittelter Nachrichtenübertragung über das Internet-Protokoll basiert;
14. „Internet-Zugangsdienst“ einen Kommunikationsdienst im Sinne von § 3 Z 9, der in der Bereitstellung von Einrichtungen oder Diensten zur Erbringung von Zugangsleistungen zum Internet besteht;
15. „E-Mail-Dienst“ einen Kommunikationsdienst im Sinne von § 3 Z 9, welcher den Versand und die Zustellung von E-Mails auf Basis des „Simple Mail Transfer Protocol“ (SMTP) umfasst;
16. „öffentliche IP-Adresse“ eine einmalige numerische Adresse aus einem Adressblock, der durch die Internet Assigned Numbers Authority (IANA) oder durch eine regionale Vergabestelle (Regional Internet Registries) einem Anbieter eines Internet-Zugangsdienstes zur Zuteilung von Adressen an seine Kunden zugewiesen wurde, die einen Rechner im Internet eindeutig identifiziert und im Internet geroutet werden kann. Öffentliche IP-Adressen sind Zugangsdaten im Sinne des § 92 Abs. 3 Z 4a. Wenn eine konkrete öffentliche IP-Adresse einem Teilnehmer für die Dauer des Vertrages zur ausschließlichen Nutzung zugewiesen ist, handelt es sich zugleich um ein Stammdatum im Sinne des § 92 Abs. 3 Z 3;
17. „Verletzung des Schutzes personenbezogener Daten“ jede Verletzung der Sicherheit, die auf versehentliche oder unrechtmäßige Weise zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Weitergabe von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlicher Kommunikationsdienste in der Gemeinschaft verarbeitet werden.

Verkehrsdaten

§ 99. (1) Verkehrsdaten dürfen außer in den in diesem Gesetz geregelten Fällen nicht gespeichert oder übermittelt werden und sind vom Anbieter nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren. Die Zulässigkeit der weiteren Verwendung

von Verkehrsdaten, die nach Abs. 5 übermittelt werden, richtet sich nach den Vorschriften der StPO sowie des SPG.

(2) Sofern dies für Zwecke der Verrechnung von Endkunden- oder Vorleistungsentgelten erforderlich ist, hat der Betreiber eines öffentlichen Kommunikationsnetzes oder -dienstes Verkehrsdaten zu speichern. Die Verkehrsdaten sind zu löschen oder zu anonymisieren, sobald der Bezahlvorgang durchgeführt wurde und innerhalb einer Frist von drei Monaten die Entgelte nicht schriftlich beeinsprucht wurden. Die Daten sind jedoch nicht zu löschen, wenn:

1. ein fristgerechter Einspruch erhoben wurde, bis zum Ablauf jener Frist, innerhalb derer die Abrechnung rechtlich angefochten werden kann.
2. die Rechnung nicht beglichen wurde, bis zum Ablauf jener Frist, bis zu der der Anspruch auf Zahlung geltend gemacht werden kann, oder
3. ein Verfahren über die Höhe der Entgelte eingeleitet wurde, bis zur endgültigen Entscheidung.

Diese Daten sind im Streitfall der entscheidenden Einrichtung sowie der Schlichtungsstelle (§ 122) unverkürzt zur Verfügung zu stellen. Der Umfang der gespeicherten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken.

(3) Die Verarbeitung von Verkehrsdaten darf nur durch solche Personen erfolgen, die für die Entgeltverrechnung oder Verkehrsabwicklung, Behebung von Störungen, Kundenanfragen, Betrugsermittlung oder Vermarktung der Kommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen zuständig sind oder die von diesen Personen beauftragt wurden. Der Umfang der verwendeten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken.

(4) Dem Anbieter ist es außer in den in diesem Gesetz besonders geregelten Fällen untersagt, einen Teilnehmeranschluss über die Zwecke der Verrechnung hinaus nach den von diesem Anschluss aus angerufenen Teilnehmernummern auszuwerten. Mit Zustimmung des Teilnehmers darf der Anbieter die Daten zur Vermarktung für Zwecke der eigenen Telekommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen verwenden.

(5) Eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken ist zulässig zur Auskunft über

1. Daten einer Nachrichtenübermittlung gemäß § 134 Z 2 StPO;
2. Zugangsdaten, auch wenn diese als Vorratsdaten gemäß § 102a Abs. 2 Z 1, Abs. 3 Z 6 lit. a und b oder § 102a Abs. 4 Z 1, 2, 3 und 5 längstens sechs Monate vor der Anfrage gespeichert wurden, an Gerichte und Staatsanwaltschaften nach Maßgabe des § 76a Abs. 2 StPO.

3. Verkehrsdaten und Stammdaten, wenn hierfür die Verarbeitung von Verkehrsdaten erforderlich ist, sowie zur Auskunft über Standortdaten an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a und 3b SPG. Ist eine aktuelle Standortfeststellung nicht möglich, darf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang der Endeinrichtung verarbeitet werden, auch wenn hierfür ein Zugriff auf gemäß § 102a Abs. 3 Z 6 lit. d gespeicherte Vorratsdaten erforderlich ist;
4. Zugangsdaten, auch wenn diese als Vorratsdaten gemäß § 102a Abs. 2 Z 1 oder § 102a Abs. 4 Z 1, 2,3 und 5 längstens drei Monate vor der Anfrage gespeichert wurden, an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a Z 3 SPG.

Vorratsdaten

§ 102a. (1) Über die Berechtigung zur Speicherung oder Verarbeitung gemäß den §§ 96, 97, 99, 101 und 102 hinaus haben Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe der Abs. 2 bis 4 Daten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern. Die Speicherung erfolgt ausschließlich zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt.

(2) Anbietern von Internet-Zugangsdiensten obliegt die Speicherung folgender Daten:

1. Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war;
2. Datum und Uhrzeit der Zuteilung und des Entzugs einer öffentlichen IP-Adresse bei einem Internet-Zugangsdienst unter Angabe der zugrundeliegenden Zeitzone;
3. die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss;
4. die eindeutige Kennung des Anschlusses, über den der Internet-Zugang erfolgt ist.

(3) Anbietern öffentlicher Telefondienste einschließlich Internet-Telefondiensten obliegt die Speicherung folgender Daten:

1. Teilnehmernummer oder andere Kennung des anrufenden und des angerufenen Anschlusses;
2. bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Teilnehmernummer, an die der Anruf geleitet wird;
3. Name und Anschrift des anrufenden und des angerufenen Teilnehmers;

4. Datum, Uhrzeit des Beginns und Dauer eines Kommunikationsvorganges unter Angabe der zugrundeliegenden Zeitzone;

5. die Art des in Anspruch genommenen Dienstes (Anrufe, Zusatzdienste und Mitteilungs- und Multimediadienste).

6. Bei Mobilfunknetzen zudem

a) der internationalen Mobilteilnehmerkennung (IMSI) des anrufenden und des angerufenen Anschlusses;

b) der internationalen Mobilfunkgeräteerkennung (IMEI) des anrufenden und des angerufenen Anschlusses;

c) Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Standortkennung (Cell-ID), an dem der Dienst aktiviert wurde, wenn es sich um vorbezahlte anonyme Dienste handelt;

d) der Standortkennung (Cell-ID) bei Beginn einer Verbindung.

(4) Anbietern von E-Mail-Diensten obliegt die Speicherung folgender Daten:

1. die einem Teilnehmer zugewiesene Teilnehmerkennung;

2. Name und Anschrift des Teilnehmers, dem eine E-Mail-Adresse zu einem bestimmten Zeitpunkt zugewiesen war;

3. bei Versenden einer E-Mail die E-Mail-Adresse und die öffentliche IP-Adresse des Absenders sowie die E-Mail-Adresse jedes Empfängers der E-Mail;

4. beim Empfang einer E-Mail und deren Zustellung in ein elektronisches Postfach die E-Mail-Adresse des Absenders und des Empfängers der Nachricht sowie die öffentliche IP-Adresse der letztübermittelnden Kommunikationsnetzeinrichtung;

5. bei An- und Abmeldung beim E-Mail-Dienst Datum, Uhrzeit, Teilnehmerkennung und öffentliche IP-Adresse des Teilnehmers unter Angabe der zugrunde liegenden Zeitzone.

(5) Die Speicherpflicht nach Abs. 1 besteht nur für jene Daten gemäß Abs. 2 bis 4, die im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet werden. Im Zusammenhang mit erfolglosen Anrufversuchen besteht die Speicherpflicht nach Abs. 1 nur, soweit diese Daten im Zuge der Bereitstellung des betreffenden Kommunikationsdienstes erzeugt oder verarbeitet und gespeichert oder protokolliert werden.

(6) Die Speicherpflicht nach Abs. 1 besteht nicht für solche Anbieter, deren Unternehmen nicht der Verpflichtung zur Entrichtung des Finanzierungsbeitrages gemäß § 34 KommAustriaG unterliegen.

(7) Der Inhalt der Kommunikation und insbesondere Daten über im Internet aufgerufene Adressen dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(8) Die nach Abs. 1 zu speichernden Daten sind nach Ablauf der Speicherfrist unbeschadet des § 99 Abs. 2 unverzüglich, spätestens jedoch einen Monat nach Ablauf der Speicherfrist, zu löschen. Die Erteilung einer Auskunft nach Ablauf der Speicherfrist ist unzulässig.

(9) Im Hinblick auf Vorratsdaten, die gemäß § 102b übermittelt werden, richten sich die Ansprüche auf Information oder Auskunft über diese Datenverwendung ausschließlich nach den Bestimmungen der StPO.

Auskunft über Vorratsdaten

§ 102b. (1) Eine Auskunft über Vorratsdaten ist ausschließlich aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt, zulässig.

(2) Die nach § 102a zu speichernden Daten sind so zu speichern, dass sie unverzüglich an die nach den Bestimmungen der StPO und nach dem dort vorgesehenen Verfahren für die Erteilung einer Auskunft über Daten einer Nachrichtenübermittlung zuständigen Behörden übermittelt werden können.

(3) Die Übermittlung der Daten hat in angemessen geschützter Form nach Maßgabe des § 94 Abs. 4 zu erfolgen.

5. RL 2002/58/EG

Artikel 15

Anwendung einzelner Bestimmungen der Richtlinie

95/46/EG

(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen entsprechen.

(2) Die Bestimmungen des Kapitels III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen gelten im Hinblick auf innerstaatliche Vorschriften, die nach der vorliegenden Richtlinie erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte.

(3) Die gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzte Datenschutzgruppe nimmt auch die in Artikel 30 jener Richtlinie festgelegten Aufgaben im Hinblick auf die von der vorliegenden Richtlinie abgedeckten Aspekte, nämlich den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der elektronischen Kommunikation wahr.

6. RL 2006/24/EG

Präambel:

(1) Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [3] verpflichtet die Mitgliedstaaten zum Schutz der Grundrechte und Grundfreiheiten und insbesondere der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten, um den freien Verkehr personenbezogener Daten in der Gemeinschaft sicherzustellen.

(2) Die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) [4] transponiert die Grundsätze der Richtlinie 95/46/EG in besondere Vorschriften für den Bereich der elektronischen Kommunikation.

(3) Die Artikel 5, 6 und 9 der Richtlinie 2002/58/EG enthalten Vorschriften für die Verarbeitung von Verkehrs- und Standortdaten, die im Zuge der Nutzung elektronischer Kommunikationsdienste erzeugt wurden, durch Netzbetreiber und Diensteanbieter. Daten dieser Art müssen gelöscht oder anonymisiert werden, sobald sie zur Übermittlung einer Nachricht nicht mehr benötigt werden, außer wenn es sich um Daten handelt, die für die Abrechnung von Gebühren oder Bezahlung von Zusammenschaltungen erforderlich sind. Mit Einwilligung des Betroffenen dürfen bestimmte Daten auch für Vermarktungszwecke oder die Bereitstellung von Diensten mit einem Zusatznutzen verarbeitet werden.

(4) In Artikel 15 Absatz 1 der Richtlinie 2002/58/EG ist festgelegt, unter welchen Bedingungen die Mitgliedstaaten die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 der genannten Richtlinie beschränken dürfen. Etwaige Beschränkungen müssen zu besonderen Zwecken der Aufrechterhaltung der öffentlichen Ordnung, d. h. für die nationale Sicherheit (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit oder die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen, in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig sein.

(5) Einige Mitgliedstaaten haben Rechtsvorschriften über eine Vorratsspeicherung von Daten durch Diensteanbieter zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten erlassen. Diese nationalen Vorschriften weichen stark voneinander ab.

(6) Die rechtlichen und technischen Unterschiede zwischen den nationalen Vorschriften zur Vorratsdatenspeicherung zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten beeinträchtigen den Binnenmarkt für elektronische Kommunikation, da Diensteanbieter mit unterschiedlichen Anforderungen in Bezug auf die zu speichernden Arten von Verkehrs- und Standortdaten, die für die Vorratsspeicherung geltenden Bedingungen und die Dauer der Vorratsspeicherung konfrontiert sind.

(7) In seinen Schlussfolgerungen vom 19. Dezember 2002 betont der Rat "Justiz und Inneres", dass die beträchtliche Zunahme der Möglichkeiten bei der elektronischen Kommunikation dazu geführt hat, dass Daten über die Nutzung elektronischer Kommunikation besonders wichtig sind und daher ein wertvolles Mittel bei der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten und insbesondere der organisierten Kriminalität darstellen.

(8) In der vom Europäischen Rat am 25. März 2004 angenommenen Erklärung zum Kampf gegen den Terrorismus wurde der Rat aufgefordert, Vorschläge für Rechtsvorschriften über die Aufbewahrung von Verkehrsdaten durch Diensteanbieter zu prüfen.

(9) Gemäß Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) hat jede Person das Recht auf Achtung ihres Privatlebens und ihrer Korrespondenz. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist, unter anderem für die nationale oder öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten oder zum Schutz der Rechte und Freiheiten anderer. Da sich die Vorratsspeicherung von Daten in mehreren Mitgliedstaaten als derart notwendiges und wirksames Ermittlungswerkzeug für die Strafverfolgung, insbesondere in schweren Fällen wie organisierter Kriminalität und Terrorismus, erwiesen hat, muss gewährleistet werden, dass die auf Vorrat gespeicherten Daten den Strafverfolgungsbehörden für einen bestimmten Zeitraum unter den in dieser Richtlinie festgelegten Bedingungen zur Verfügung stehen. Die Annahme eines Instruments zur Vorratsspeicherung von Daten gemäß den Anforderungen des Artikels 8 der EMRK ist daher eine notwendige Maßnahme.

(10) Am 13. Juli 2005 hat der Rat in seiner Erklärung, in der die Terroranschläge von London verurteilt wurden, nochmals auf die Notwendigkeit hingewiesen, so rasch wie möglich gemeinsame Maßnahmen zur Vorratsspeicherung von Telekommunikationsdaten zu erlassen.

(11) Da sowohl wissenschaftliche Untersuchungen als auch praktische Erfahrungen in mehreren Mitgliedstaaten gezeigt haben, dass Verkehrs- und Standortdaten für die Ermittlung, Feststellung und Verfolgung von Straftaten von großer Bedeutung sind, muss auf europäischer Ebene sichergestellt werden, dass Daten, die bei der Bereitstellung von Kommunikationsdiensten von den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder den Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, für einen bestimmten Zeitraum unter den in dieser Richtlinie festgelegten Bedingungen auf Vorrat gespeichert werden.

(12) Artikel 15 Absatz 1 der Richtlinie 2002/58/EG gilt weiterhin für Daten, einschließlich Daten im Zusammenhang mit erfolglosen Anrufversuchen, deren Vorratsspeicherung nach der vorliegenden Richtlinie nicht ausdrücklich vorgeschrieben ist und die daher nicht in den Anwendungsbereich der vorliegenden Richtlinie fallen, und für die Vorratsspeicherung zu anderen — einschließlich justiziellen — Zwecken als denjenigen, die durch die vorliegende Richtlinie abgedeckt werden.

(13) Diese Richtlinie bezieht sich nur auf Daten, die als Folge einer Kommunikation oder eines Kommunikationsdienstes erzeugt oder verarbeitet werden; sie bezieht sich nicht auf Daten, die Inhalt der übermittelten Information sind. Die Vorratsspeicherung von Daten sollte so erfolgen, dass vermieden wird, dass Daten mehr als einmal auf Vorrat gespeichert werden. Daten, die im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet wurden, beziehen sich auf Daten, die zugänglich sind. Insbesondere bei der Vorratsspeicherung von Daten im Zusammenhang mit Internet-E-Mail und Internet-Telefonie kann die Verpflichtung zur Vorratsspeicherung nur für Daten aus den eigenen Diensten des Anbieters oder des Netzbetreibers gelten.

(14) Die technische Entwicklung in der elektronischen Kommunikation schreitet rasch voran, und damit verändern sich möglicherweise auch die legitimen Anforderungen der zuständigen Behörden. Um sich beraten zu lassen und den Austausch von Erfahrungen mit bewährten Praktiken in diesen Fragen zu fördern, beabsichtigt die Kommission, eine Gruppe einzusetzen, die aus Strafverfolgungsbehörden der Mitgliedstaaten, Verbänden der Branche für elektronische Kommunikation, Vertretern des Europäischen Parlaments und europäischen Datenschutzbehörden, einschließlich des Europäischen Datenschutzbeauftragten, besteht.

(15) Die Richtlinie 95/46/EG sowie die Richtlinie 2002/58/EG sind auf die gemäß der vorliegenden Richtlinie auf Vorrat gespeicherten Daten uneingeschränkt anwendbar. Artikel 30 Absatz 1 Buchstabe c der Richtlinie 95/46/EG verlangt die Anhörung der durch Artikel 29

der letztgenannten Richtlinie eingesetzten Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten.

(16) Die Pflichten von Diensteanbietern hinsichtlich Maßnahmen zur Sicherstellung der Datenqualität, die sich aus Artikel 6 der Richtlinie 95/46/EG ergeben, und ihre Pflichten hinsichtlich Maßnahmen zur Gewährleistung der Vertraulichkeit und der Sicherheit der Datenverarbeitung, die sich aus den Artikeln 16 und 17 der genannten Richtlinie ergeben, gelten uneingeschränkt für Daten, die im Sinne der vorliegenden Richtlinie auf Vorrat gespeichert werden.

(17) Die Mitgliedstaaten müssen gesetzgeberische Maßnahmen ergreifen, um sicherzustellen, dass die gemäß dieser Richtlinie auf Vorrat gespeicherten Daten nur in Übereinstimmung mit den innerstaatlichen Rechtsvorschriften und unter vollständiger Achtung der Grundrechte der betroffenen Personen an die zuständigen nationalen Behörden weitergegeben werden.

(18) In diesem Zusammenhang sind die Mitgliedstaaten gemäß Artikel 24 der Richtlinie 95/46/EG verpflichtet, Sanktionen für Verstöße gegen die zur Umsetzung der Richtlinie 95/46/EG erlassenen Vorschriften festzulegen. Nach Artikel 15 Absatz 2 der Richtlinie 2002/58/EG besteht die gleiche Pflicht in Bezug auf die innerstaatlichen Vorschriften zur Umsetzung der Richtlinie 2002/58/EG. In dem Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme [5] ist vorgesehen, dass der vorsätzliche und rechtswidrige Zugang zu Informationssystemen, einschließlich der darin auf Vorrat gespeicherten Daten, unter Strafe gestellt werden muss.

(19) Das Recht jeder Person, der wegen einer rechtswidrigen Verarbeitung oder jeder anderen mit den einzelstaatlichen Vorschriften zur Umsetzung der Richtlinie 95/46/EG nicht zu vereinbarenden Handlung ein Schaden entsteht, Schadensersatz zu verlangen, das sich aus Artikel 23 der genannten Richtlinie ergibt, besteht auch im Zusammenhang mit einer rechtswidrigen Verarbeitung personenbezogener Daten gemäß der vorliegenden Richtlinie.

(20) Das Übereinkommen des Europarates über Datennetzkriminalität von 2001 und das Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten von 1981 gelten auch für Daten, die im Sinne dieser Richtlinie auf Vorrat gespeichert werden.

(21) Da die Ziele dieser Richtlinie, nämlich die Harmonisierung der Pflichten für Diensteanbieter bzw. Netzbetreiber im Zusammenhang mit der Vorratsspeicherung bestimmter Daten und die Gewährleistung, dass diese Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen, auf Ebene der

Mitgliedstaaten nicht ausreichend erreicht werden können und daher wegen des Umfangs und der Wirkungen dieser Richtlinie besser auf Gemeinschaftsebene zu erreichen sind, kann die Gemeinschaft gemäß dem in Artikel 5 des Vertrags niedergelegten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Richtlinie nicht über das zur Erreichung dieser Ziele erforderliche Maß hinaus.

(22) Diese Richtlinie wahrt die vor allem mit der Charta der Grundrechte der Europäischen Union anerkannten Grundrechte und Grundsätze. In Verbindung mit der Richtlinie 2002/58/EG ist die vorliegende Richtlinie insbesondere bestrebt, die volle Wahrung der Grundrechte der Bürger auf Achtung des Privatlebens und ihrer Kommunikation sowie auf Schutz personenbezogener Daten gemäß Artikel 7 und 8 der Charta zu gewährleisten.

(23) Da die Pflichten von Anbietern elektronischer Kommunikationsdienste verhältnismäßig sein sollten, wird in dieser Richtlinie vorgeschrieben, dass sie nur solche Daten auf Vorrat speichern müssen, die im Zuge der Bereitstellung ihrer Kommunikationsdienste erzeugt oder verarbeitet werden. Soweit derartige Daten nicht von diesen Anbietern erzeugt oder verarbeitet werden, besteht auch keine Pflicht zur Vorratsspeicherung. Durch diese Richtlinie soll nicht die Technologie für die Vorratsspeicherung von Daten harmonisiert werden, deren Wahl eine Angelegenheit ist, die auf nationaler Ebene zu regeln ist.

(24) Nach Nummer 34 der Interinstitutionellen Vereinbarung über bessere Rechtsetzung [6] sind die Mitgliedstaaten aufgefordert, für ihre eigenen Zwecke und im Interesse der Gemeinschaft eigene Tabellen aufzustellen, aus denen im Rahmen des Möglichen die Entsprechungen zwischen dieser Richtlinie und den Umsetzungsmaßnahmen zu entnehmen sind, und diese zu veröffentlichen.

(25) Diese Richtlinie berührt nicht das Recht der Mitgliedstaaten, Rechtsvorschriften über den Zugang zu und die Nutzung von Daten durch von ihnen benannte nationale Behörden zu erlassen. Fragen des Zugangs zu Daten, die gemäß dieser Richtlinie von nationalen Behörden für solche Tätigkeiten auf Vorrat gespeichert werden, die in Artikel 3 Absatz 2 erster Gedankenstrich der Richtlinie 95/46/EG aufgeführt sind, fallen nicht in den Anwendungsbereich des Gemeinschaftsrechts. Sie können aber durch nationales Recht oder Maßnahmen nach Titel VI des Vertrags über die Europäische Union geregelt werden. Derartige Rechtsvorschriften oder Maßnahmen müssen die Grundrechte, wie sie sich aus den gemeinsamen Verfassungstraditionen der Mitgliedstaaten ergeben und durch die EMRK gewährleistet sind, in vollem Umfang wahren. Nach Artikel 8 der EMRK in der Auslegung durch den Europäischen Gerichtshof für Menschenrechte müssen Eingriffe von Behörden in

das Recht auf Privatsphäre den Anforderungen der Notwendigkeit und Verhältnismäßigkeit genügen und deshalb festgelegten, eindeutigen und rechtmäßigen Zwecken dienen, wobei sie in einer Weise erfolgen müssen, die dem Zweck des Eingriffs entspricht, dafür erheblich ist und nicht darüber hinausgeht —

Artikel 4

Zugang zu Daten

Die Mitgliedstaaten erlassen Maßnahmen, um sicherzustellen, dass die gemäß dieser Richtlinie auf Vorrat gespeicherten Daten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden. Jeder Mitgliedstaat legt in seinem innerstaatlichen Recht unter Berücksichtigung der einschlägigen Bestimmungen des Rechts der Europäischen Union oder des Völkerrechts, insbesondere der EMRK in der Auslegung durch den Europäischen Gerichtshof für Menschenrechte, das Verfahren und die Bedingungen fest, die für den Zugang zu auf Vorrat gespeicherten Daten gemäß den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind.

7. STRAFPROZESSORDNUNG

Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Auskunft über Vorratsdaten sowie Überwachung von Nachrichten

§ 135. (1) Beschlagnahme von Briefen ist zulässig, wenn sie zur Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, erforderlich ist und sich der Beschuldigte wegen einer solchen Tat in Haft befindet oder seine Vorführung oder Festnahme deswegen angeordnet wurde.

(2) Auskunft über Daten einer Nachrichtenübermittlung ist 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,

2. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann

und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt, oder

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.

(2a) Auskunft über Vorratsdaten (§§ 102a und 102b TKG) ist in den Fällen des Abs. 2 Z 2 bis 4 zulässig.

(3) Überwachung von Nachrichten ist zulässig,

1. in den Fällen des Abs. 2 Z 1,

2. in den Fällen des Abs. 2 Z 2, sofern der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Überwachung zustimmt,

3. wenn dies zur Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, erforderlich erscheint oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten strafbaren Handlungen ansonsten wesentlich erschwert wäre und

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

b. auf Grund bestimmter Tatsachen anzunehmen ist, dass eine der Tat (lit. a) dringend verdächtige Person die technische Einrichtung benützen oder mit ihr eine Verbindung herstellen werde;

4. in den Fällen des Abs. 2 Z 4.

8. STRAFGESETZBUCH

Kriminelle Organisation

§ 278a. Wer eine auf längere Zeit angelegte unternehmensähnliche Verbindung einer größeren Zahl von Personen gründet oder sich an einer solchen Verbindung als Mitglied beteiligt (§ 278 Abs. 3),

1. die, wenn auch nicht ausschließlich, auf die wiederkehrende und geplante Begehung schwerwiegender strafbarer Handlungen, die das Leben, die körperliche Unversehrtheit, die Freiheit oder das Vermögen bedrohen, oder schwerwiegender strafbarer Handlungen im Bereich der sexuellen Ausbeutung von Menschen, der Schlepperei oder des unerlaubten Verkehrs mit Kampfmitteln, Kernmaterial und radioaktiven Stoffen, gefährlichen Abfällen, Falschgeld oder Suchtmitteln ausgerichtet ist,

2. die dadurch eine Bereicherung in großem Umfang oder erheblichen Einfluß auf Politik oder Wirtschaft anstrebt und

3. die andere zu korrumpieren oder einzuschüchtern oder sich auf besondere Weise gegen Strafverfolgungsmaßnahmen abzusichern sucht,

ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen. § 278 Abs. 4 gilt entsprechend.

Terroristische Vereinigung

§ 278b. (1) Wer eine terroristische Vereinigung (Abs. 3) anführt, ist mit Freiheitsstrafe von fünf bis zu fünfzehn Jahren zu bestrafen. Wer eine terroristische Vereinigung anführt, die sich auf die Drohung mit terroristischen Straftaten (§ 278c Abs. 1) oder Terrorismusfinanzierung (§ 278d) beschränkt, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

(2) Wer sich als Mitglied (§ 278 Abs. 3) an einer terroristischen Vereinigung beteiligt, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

(3) Eine terroristische Vereinigung ist ein auf längere Zeit angelegter Zusammenschluss von mehr als zwei Personen, der darauf ausgerichtet ist, dass von einem oder mehreren Mitgliedern dieser Vereinigung eine oder mehrere terroristische Straftaten (§ 278c) ausgeführt werden oder Terrorismusfinanzierung (§ 278d) betrieben wird.

9. SICHERHEITSPOLIZEIGESETZ

Zulässigkeit der Verarbeitung

§ 53. (1) Die Sicherheitsbehörden dürfen personenbezogene Daten ermitteln und weiterverarbeiten

1. für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht (§ 19);
 2. für die Abwehr krimineller Verbindungen (§§ 16 Abs. 1 Z 2 und 21);
 - 2a. für die erweiterte Gefahrenforschung (§ 21 Abs. 3) unter den Voraussetzungen des § 91c Abs. 3;
 3. für die Abwehr gefährlicher Angriffe (§§ 16 Abs. 2 und 3 sowie 21 Abs. 2); einschließlich der im Rahmen der Gefahrenabwehr notwendigen Gefahrenforschung (§ 16 Abs. 4 und § 28a);
 4. für die Vorbeugung wahrscheinlicher gefährlicher Angriffe gegen Leben, Gesundheit, Sittlichkeit, Freiheit, Vermögen oder Umwelt (§ 22 Abs. 2 und 3) oder für die Vorbeugung gefährlicher Angriffe mittels Kriminalitätsanalyse, wenn nach der Art des Angriffes eine wiederholte Begehung wahrscheinlich ist;
 5. für Zwecke der Fahndung (§ 24);
 6. um bei einem bestimmten Ereignis die öffentliche Ordnung aufrechterhalten zu können;
 7. für die Analyse und Bewertung der Wahrscheinlichkeit einer Gefährdung der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit durch die Verwirklichung eines Tatbestandes nach dem Vierzehnten und Fünfzehnten Abschnitt des Strafgesetzbuches.
- (2) Die Sicherheitsbehörden dürfen Daten, die sie in Vollziehung von Bundes- oder Landesgesetzen verarbeitet haben, für die Zwecke und unter den Voraussetzungen nach Abs. 1 ermitteln und weiterverarbeiten; ein automationsunterstützter Datenabgleich im Sinne des § 141 StPO ist ihnen jedoch untersagt. Bestehende Übermittlungsverbote bleiben unberührt.
- (3) Die Sicherheitsbehörden sind berechtigt, von den Dienststellen der Gebietskörperschaften, den anderen Körperschaften des öffentlichen Rechtes und den von diesen betriebenen Anstalten Auskünfte zu verlangen, die sie für die Abwehr gefährlicher Angriffe, für die erweiterte Gefahrenforschung unter den Voraussetzungen nach Abs. 1 oder für die Abwehr krimineller Verbindungen benötigen. Eine Verweigerung der Auskunft ist nur zulässig, soweit andere öffentliche Interessen die Abwehrinteressen überwiegen oder eine über die

Amtsverschwiegenheit (Art. 20 Abs. 3 B-VG) hinausgehende sonstige gesetzliche Verpflichtung zur Verschwiegenheit besteht.

(3a) Die Sicherheitsbehörden sind berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I Nr. 70) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001) Auskünfte zu verlangen:

1. über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses wenn dies zur Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben erforderlich ist,

2. über die Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr

a) einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§ 19),

b) eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1) oder

c) einer kriminellen Verbindung (§ 16 Abs. 1 Z 2) benötigen,

3. über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr

a) einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§ 19),

b) eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1) oder

c) einer kriminellen Verbindung (§ 16 Abs. 1 Z 2) benötigen,

auch wenn hierfür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 4 iVm § 102a TKG 2003 erforderlich ist,

4. über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer, wenn dies zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder zur Abwehr gefährlicher Angriffe erforderlich ist.

(3b) Ist auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen besteht, sind die Sicherheitsbehörden zur Hilfeleistung oder Abwehr dieser Gefahr berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten oder diesen begleitenden Menschen mitgeführten Endeinrichtung zu verlangen, auch wenn hierfür die Verwendung von

Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist, sowie technische Mittel zur Lokalisierung der Endeinrichtung zum Einsatz zu bringen.

(3c) In den Fällen der Abs. 3a und 3b trifft die Sicherheitsbehörde die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens. Die ersuchte Stelle ist verpflichtet, die Auskünfte unverzüglich und im Fall des Abs. 3b gegen Ersatz der Kosten nach der Überwachungskostenverordnung – ÜKVO, BGBI. II Nr. 322/2004, zu erteilen. Im Falle des Abs. 3b hat die Sicherheitsbehörde dem Betreiber überdies unverzüglich, spätestens innerhalb von 24 Stunden eine schriftliche Dokumentation nachzureichen. In den Fällen des Abs. 3a Z 3 sowie Abs. 3b ist die Sicherheitsbehörde verpflichtet, den Betroffenen darüber zu informieren, dass eine Auskunft zur Zuordnung seines Namens oder seiner Anschrift zu einer bestimmten IP-Adresse (§ 53 Abs. 3a Z 3) oder zur Standortbeauskunftung (§ 53 Abs. 3b) eingeholt wurde, sofern hierfür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 oder 4 iVm § 102a TKG 2003 erforderlich war. Dabei sind dem Betroffenen nachweislich und ehestmöglich die Rechtsgrundlage sowie das Datum und die Uhrzeit der Anfrage bekannt zu geben. Die Information Betroffener kann aufgeschoben werden, solange durch sie der Ermittlungszweck gefährdet wäre, und kann unterbleiben, wenn der Betroffene bereits nachweislich Kenntnis erlangt hat oder die Information des Betroffenen unmöglich ist.

(3d) Die Sicherheitsbehörden sind zur Vorbeugung und Abwehr gefährlicher Angriffe gegen die Umwelt berechtigt, von Behörden des Bundes, der Länder und Gemeinden Auskünfte über von diesen genehmigte Anlagen und Einrichtungen zu verlangen, bei denen wegen der Verwendung von Maschinen oder Geräten, der Lagerung, Verwendung oder Produktion von Stoffen, der Betriebsweise, der Ausstattung oder aus anderen Gründen besonders zu befürchten ist, dass im Falle einer Abweichung der Anlage oder Einrichtung von dem der Rechtsordnung entsprechenden Zustand eine Gefahr für das Leben, die Gesundheit mehrerer Menschen oder in großem Ausmaß eine Gefahr für Eigentum oder Umwelt entsteht. Die ersuchte Behörde ist verpflichtet, die Auskunft zu erteilen.

(4) Abgesehen von den Fällen der Abs. 2 bis 3b und 3d sind die Sicherheitsbehörden für Zwecke des Abs. 1 berechtigt, personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere durch Zugriff auf allgemein zugängliche Daten, zu ermitteln und weiterzuverarbeiten.

(5) Die Sicherheitsbehörden sind im Einzelfall und unter den Voraussetzungen des § 54 Abs. 3 ermächtigt, für die Abwehr gefährlicher Angriffe und krimineller Verbindungen, wenn bestimmte Tatsachen auf eine schwere Gefahr für die öffentliche Sicherheit schließen lassen, für die erweiterte Gefahrenforschung (§ 21 Abs. 3) und zur Fahndung (§ 24)

personenbezogene Bilddaten zu verwenden, die Rechtsträger des öffentlichen oder privaten Bereichs mittels Einsatz von Bild- und Tonaufzeichnungsgeräten rechtmäßig ermittelt und den Sicherheitsbehörden übermittelt haben. Dabei ist besonders darauf zu achten, dass Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit (§ 29) zum Anlass wahren. Nicht zulässig ist die Verwendung von Daten über nichtöffentliches Verhalten.

Rechtsschutzbeauftragter

§ 91a. (1) Zur Wahrnehmung des besonderen Rechtsschutzes im Ermittlungsdienst der Sicherheitsbehörden ist beim Bundesminister für Inneres ein Rechtsschutzbeauftragter mit zwei Stellvertretern eingerichtet, die bei der Besorgung der ihnen nach dem Sicherheitspolizeigesetz zukommenden Aufgaben unabhängig und weisungsfrei sind und der Amtsverschwiegenheit unterliegen.

(2) Der Rechtsschutzbeauftragte und seine Stellvertreter haben gleiche Rechte und Pflichten. Sie werden vom Bundespräsidenten auf Vorschlag der Bundesregierung nach Anhörung der Präsidenten des Nationalrates sowie der Präsidenten des Verfassungsgerichtshofes und des Verwaltungsgerichtshofes auf die Dauer von fünf Jahren bestellt. Wiederbestellungen sind zulässig.

(3) (Verfassungsbestimmung) Eine Einschränkung seiner Befugnisse nach § 91c sowie seiner Rechte und Pflichten nach § 91d kann vom Nationalrat nur in Anwesenheit von mindestens der Hälfte der Mitglieder mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen beschlossen werden.

Die Autorin, geboren 1988, stammt aus dem Salzburger Pinzgau. Sie studierte Politik- und Rechtswissenschaften in Wien. Während der Studienfokus im Bakkalaureatsstudium zunächst auf internationaler Politik lag, ergab sich aus der Kombination der beiden Studienfächer allmählich ein verstärktes Interesse an der Staatswissenschaft. Insbesondere beschäftigte sich die Autorin mit verfassungs- und grundrechtlichen Fragen und den Wechselwirkungen zwischen Gesetzgebung und Politik. Einen weiteren Forschungsschwerpunkt bildet die Analyse von Prozessen auf Unionsebene und deren Auswirkung auf die österreichische Gesetzgebung.