SCHEUCHER RECHTSANWALT GMBH

in Kooperation mit Mag. Tina Große Rechtsanwältin_Attorney at law

Mag. Ewald Scheucher
Rechtsanwalt_Attorney at law

[A] Lindengasse 39, A-1070 Wien
[T] +43/1/710 92 51
[F] +43/1/710 92 51-51
[E] office@scheucher.eu
[I] www.scheucher.eu

Gerichtshof der Europäischen Union
Kanzlei
Boulevard Konrad Adenauer
L-2925 Luxemburg

C-594/12, RS Seitlinger u.a.
(926102 DE)
130328 Äußerung_EuGH/IA/1/ems/gt

Antragsteller des Ausgangsverfahrens:

1. **Ing. Dr. Christof TSCHOHL,** geb. [redacted]
   Jurist, Ludwig Boltzmann Institut für Menschenrechte
   [redacted]
2. **Mag. Andreas KRISCH**, geb. [redacted]
   IT-Consultant,
   Obmann Arbeitskreis Vorratsdatenspeicherung
   [redacted]
3. **Mag. Albert STEINHAUSER**, geb. [redacted]
   Nationalratsabgeordneter, Justizsprecher der „Grünen"
   [redacted]
4. **Jana HERWIG**, M.A:, [redacted]
   Medienwissenschafterin,
   [redacted]
5. **Sigrid MAURER**, geb. [redacted] Studentin,
   [redacted]
6. **Mag. DDr. Erich SCHWEIGHOFER**, geb [redacted]
   Ao. Univ. Prof. Universität Wien,
   Leiter der Arbeitsgruppe Rechtsinformatik,
   [redacted]

7. **Dr. Hannes TRETTER,** geb. [redacted]
ao. Univ.-Prof., Universität Wien,
Direktor des Boltzmann-Instituts für Menschenrechte,
[redacted]

8. **SCHEUCHER Rechtsanwalt GmbH**, FN 335393a
1070 Wien, Lindengasse 39

9. **Dr. Maria WITTMANN-TIWALD,** geb. [redacted] Richterin,
[redacted]

10. **Philipp SCHMUCK,** geb. [redacted] Student,
[redacted]

11. **Dr. Stefan PROCHASKA**, geb. [redacted] Rechtsanwalt
Vizepräsident der Rechtsanwaltskammer Wien
Geschäftsführer PHHV Rechtsanwälte OG
1010 Wien, Julius-Raab Platz 4

12. bis 11.130. **Antragsteller/in** gemäß dem österr. VfGH vorliegender CD

alle vertreten durch: **SCHEUCHER Rechtsanwalt GmbH**
1070 Wien, Lindengasse 39
RA-Code P131306

(Vollmachten gem. § 8 RAO erteilt)

Antragsgegnerin: **BUNDESREGIERUNG DER REPUBLIK ÖSTERREICH**
p.A. Bundeskanzleramt
1014 Wien, Ballhausplatz 2

wegen: Ersuchen um Vorabentscheidung, C-594/12, RS Seitlinger u.a.
Richtlinie 2006/24/EG („Vorratsdatenspeicherung")
Charta der Grundrechte der EU (GRC), Artikel 7, 8, 11, 12, 48

STELLUNGNAHME
der Antragsteller/innen des Ausgangsverfahrens im Vorabentscheidungsverfahren
gemäß Artikel 267 AEUV

3-fach

Inhaltsverzeichnis **Seite**

I.	**Vollmachtsbekanntgabe und Einleitung**	4
I.1	Vollmachtsbekanntgabe	4
I.2	Einleitung	4
II.	**Bedeutung der EU Grundrechte-Charta im Ausgangsverfahren**	6
III.	**Materielle Bedenken gegen die Vorratsdatenspeicherung**	7
III.1.	Überblick	7
III.2.	Die schleichende (atmosphärische) Veränderung der Gesellschaft durch VDS	8
III.3.	Zur Bedeutung der Unschuldsvermutung in einem freien Gemeinwesen	9
III.4.	Argumentation nach dem Schema der Verhältnismäßigkeitsprüfung	10
III.4.1	VDS trifft alle Nutzer/innen von Kommunikationsdienstleistern	10
III.4.2	VDS zur Zweckerreichung nicht geeignet	11
III.4.3	VDS nicht das schonendste Mittel	11
III.4.4	Kein angemessenes Verhältnis zu den Nachteilen	12
III.4.5	Normative Zwecke	12
III.4.6	Anforderungen an die gesetzlichen Grundlagen	13
III.4.7	Sonderproblem IP-Adressen	15
III.4.8	Praxis der VDS und Verletzung materieller Grundrechte	15
III.4.9	Eingriff in den Schutzbereich	17
III.4.10	Unverhältnismäßigkeit	18
IV.	**Anstelle einer Zusammenfassung**	20

I. Vollmachtsbekanntgabe, Einleitung

I.1. Eine CD mit der vollständigen Liste der 11.130 Antragsteller/innen wurde dem österreichischen Verfassungsgerichtshof (VfGH) im Ausgangsverfahren vorgelegt. Im Rubrum angeführt werden die sogenannten Erstantragsteller/innen, das sind einige jener Personen, die diesen „Sammel-Individualantrag" aktiv getragen, organisiert und/oder prominent öffentlich vertreten haben. Dem Rechtsvertreter wurde von sämtlichen Antragsteller/innen Vollmacht erteilt, auch die hier vorgelegte Äußerung im Vorabentscheidungsverfahren vorzulegen. Der Rechtsvertreter beruft sich ausdrücklich auf diese erteilte Vollmacht.

Dem Rechtsvertreter wurde die Einladung zur Abgabe einer Erklärung zum Vorabentscheidungsersuchen am **01.02.2013** zugestellt.

I.2. Einleitung

Die Umsetzung der Richtlinie 2006/24/EG stellt für die Antragsteller/innen einen Dammbruch dar, eine Art Quantensprung in den „Überwachungsstaat". Setzen sich diese Prinzipien durch und fort, ist die auf persönlicher Freiheit basierende Ordnung westlicher Demokratien am Ende – ungeachtet, wie das Staatswesen formal organisiert und verwaltet wird.

Im Kern leitet der Antrag der hier vertretenen Antragsteller/innen des Ausgangsverfahrens dem österreichischen Verfassungsgerichtshof die Frage zur Entscheidung zu, ob die Vorratsdatenspeicherung an sich mit der Europäischen Grundrechte-Charta und den Österreichischen Grundrechten, insbesondere der europäischen Menschenrechtskonvention vereinbar ist. Im Hinblick auf die innerstaatliche Rechtslage kann diese Klarstellung nur vom VfGH kommen. Er ist damit aus Sicht der Antragsteller/innen in Österreich gleichsam die letzte Verteidigungslinie einer auf Freiheitsrechten basierenden Staats- und Gesellschaftsordnung – wenn auf europäischer Ebene der Schutz der Grundrechte gemäß GRC nicht (mehr) gewährleistet wird oder werden kann. Ob dieser Schutz auf Ebene der EU gewährleistet wird, ist nun primär im Rahmen des gegenständlichen Vorabentscheidungsverfahrens durch den EuGH gemäß Art 267 AEUV zu klären.

Die legalisierte präventive Überwachung des Kommunikationsverhaltens aller in der Europäischen Union lebenden und elektronisch kommunizierenden Menschen stellt einen unumkehrbaren Paradigmenwechsel dar, der mit dem Konzept eines von Grund- und Freiheitsrechten geprägten Rechtsstaates unvereinbar ist. Die vollständige Erfassung des Kommunikationsverhaltens stellt mit dem Argument, (weitgehende) Sicherheit in einer unsicheren Welt zum Preis der Aufgabe der bürgerlichen Privatsphäre schaffen zu können, das Konzept „unveräußerlicher Rechte", das seit der amerikanischen und französischen Revolution das geistige Fundament der freiheitlich geprägten westlichen Gesellschaften darstellt, gleichsam auf den Kopf:

Die Europäische Union und die die Richtlinie umsetzenden Mitgliedstaaten erklären den Bürgerinnen und Bürgern, welches Ausmaß an unbeobachteter, unregulierter und ungespeicherter Freiheit ihnen im Namen der (Staats-)Sicherheit noch zukommt.

Um diesen Gedanken zu überspitzen: Wird in einem nächsten Schritt – natürlich wiederum im Namen hehrer Ziele wie der Bekämpfung des Terrorismus, der internationalen Kriminalität bzw. von Geldwäsche und Steuerhinterziehung – das Bargeld abgeschafft und sämtliche von Bürgerinnen und Bürgern getätigten Überweisungen verdachtsunabhängig gespeichert, ist insbesondere in Zusammenschau mit der Vorratsdatenspeicherung die Privatsphäre endgültig abgeschafft. Eine unbeobachtete, unregulierte und ungespeicherte Lebensäußerung – außer vielleicht Meditation und Selbstbefriedigung – gibt es dann nicht mehr.

Die Vorratsdatenspeicherung unterminiert nicht nur den Schutz der Privatsphäre völlig, sie bewirkt auch eine nachhaltige Erosion von demokratischen Grundpfeilern wie der Meinungs- und Medienfreiheit, dem Schutz von Berufsgeheimnissen und schließlich der Unschuldsvermutung.

Betreffend die Richtlinie zur Vorratsdatenspeicherung ist– ohne auf die verschiedenen Grundrechtstheorien, die verschiedenen naturrechtlichen und rechtspositivistischen Konzeptionen von Grund- und Menschenrechten bzw. bürgerlichen Freiheiten und ihre Interpretationen im Laufe der letzten 250 Jahre einzugehen – aus Sicht der Antragsteller/innen (bereits) im Vorabentscheidungsverfahren eine Grundsatzfrage von nicht zu überschätzender Bedeutung vorab zu entscheiden:

- Interpretieren wir, die Bürgerinnen und Bürger Europas, interpretiert der EuGH den Staat, die Europäische Union, die Institutionen und deren Beziehung zu Normunterworfenen von „oben nach unten“ oder von „unten nach oben“?

- „Gewähren“ der Staat, die Europäische Union, die Institutionen „Freiheit“ oder geben die Normunterworfenen in einem davor liegenden Akt in freier Übereinkunft Freiheit ab, um bestimmten Zwecken zu dienen. Anders formuliert: Bedarf es einer kontrollierten und kontrollierbaren Zustimmung zum Tausch von Freiheit gegen (angebliche) Sicherheit, wenn ein Quantensprung in der Freiheitsbeschneidung erfolgt – wie im gegenständlichen Fall der Vorratsdatenspeicherung durch eine Aushöhlung der Privatsphäre durch verdachtsunabhängige Überwachung

Im Hinblick auf obige Überlegungen nutzen die Antragsteller/innen des Ausgangsverfahrens als Bürgerinnen und Bürger der Europäischen Union die Gelegenheit zur Stellungnahme, um die wesentlichen, im Antrag zum Ausgangsverfahren detailliert dargelegten Bedenken hier nochmals im Überblick zu präsentieren. Damit wird insbesondere begründet, warum Frage 1 des vorlegenden Gerichts mit „nein“ zu beantworten ist.

II. Bedeutung der EU-Grundrechte-Charta im Ausgangsverfahren

Der primäre Antrag im Ausgangsverfahren bezieht sich auf den Kern der Vorratsdatenspeicherung an sich, nämlich auf die **verdachtsunabhängige flächendeckende Speicherung von Kommunikationsdaten**, wie sie **durch die Richtlinie 2006/24/EG insofern ohne Spielraum der Mitgliedsstaaten normiert** wird. Die Bestimmungen zur Umsetzung der Richtlinie 2006/24/EG, die im Ausgangsverfahren mit dem primären Antrag als verfassungswidrig bekämpft werden, liegen im Anwendungsbereich des Unionsrechts. Bei der Beurteilung ihrer Verfassungsmäßigkeit sind daher auch die Garantien der GRC Prüfungsmaßstab und zugleich unmittelbar anwendbare Bestimmungen des Unionsrechts.

Bisher ist keine Entscheidung des EuGH ergangen, die auch nur eine Prognose erlaubt, wie der Gerichtshof die Vereinbarkeit der Richtlinie 2006/24/EG mit den Bestimmungen der GRC beurteilen könnte. Auch die Entscheidung des EuGH vom 19. April 2012 in der Rechtssache C-461/10 enthält keine Aussage zur grundrechtlichen Zulässigkeit der Vorratsdatenspeicherung oder zu bestimmten Verwendungsfällen von Vorratsdaten. Die Entscheidung berührt nämlich gar nicht die Verwendung von Vorratsdaten sondern stellt lediglich klar, dass die VDS-RL (und deren "Beschränkung" auf die Aufklärung, Feststellung und Verfolgung schwerer Straftaten) einer innerstaatlichen Bestimmung nicht entgegensteht, welche die Verwendung von Daten auch für solche Auskunftsverfahren zulässt, wenn die betreffenden Daten aus anderen Gründen im Einklang mit Art. 15 der RL 2002/58/EG und im Einklang mit dem innerstaatlichen Recht gespeichert und dann beauskunftet werden.

Zum Bedeutungsgehalt der Rechte der EU Grundrechte-Charta bestimmt Art. 52 GRC: *"So weit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird. (...)"*. Weiters garantiert das „Günstigkeitsprinzip" des Art. 53, dass keine Bestimmung dieser Charta als eine Einschränkung oder Verletzung der Menschenrechte und Grundfreiheiten", insbesondere der Europäischen Menschenrechtskonvention (EMRK), ausgelegt werden darf. Art. 8 GRC garantiert jeder Person das *„Recht auf Schutz der sie betreffenden personenbezogenen Daten"*, wohingegen die EMRK ein Recht auf Datenschutz nicht explizit erwähnt. Allerdings hat der EGMR eine bemerkenswerte Dichte an Vorgaben in diesem Zusammenhang in seiner Rechtsprechung zu Art. 8 EMRK entwickelt (siehe zB *S. und Marper gg UK*, Erkenntnis vom 4. Dezember 2008). Wenngleich also das neue Grundrecht auf Datenschutz in Art. 8 GRC nicht ausdrücklich ein "entsprechendes Recht" in der EMRK hat, definiert doch die Rechtsprechung zu Art. 8 EMRK den Mindeststandard für den Datenschutz in der EU.

Eine ausdrückliche Rechtsprechung des EGMR zur Frage der Vorratsdatenspeicherung im Sinne der Richtlinie 2006/24/EG existiert bislang nicht. Die bestehende Judikatur zu Artikel 8 EMRK lässt aber durchaus darauf schließen, dass die Vorratsdatenspeicherung den Anforderungen der EMRK nicht genügt.

Aus diesen Gründen basiert die nachfolgende Argumentation zur Reichweite des neuen Grundrechts auf Datenschutz vor allem auf Art. 8 EMRK und dessen Interpretation durch die Rechtsprechung des EGMR.

III. Materielle Bedenken gegen die Vorratsdatenspeicherung

III.1. Überblick

Nachstehend sollen in der gebotenen Knappheit die Bedenken der Antragsteller/innen dargestellt werden. Die Vorratsdatenspeicherung („VDS") im Sinne der Richtlinie 2006/24/EG („VDS-RL") verletzt nach Ansicht der Antragsteller/innen (insbesondere) folgende Bestimmungen der EU Grundrechte-Charta („GRC"):

- **Art 7 GRC** (Privatleben und Familienleben, Schutz der Kommunikation)
- **Art 8 GRC** (Grundrecht auf Datenschutz)
- **Art 11 GRC** (Meinungs- und Informationsfreiheit, Redaktionsgeheimnis)
- **Art 12 GRC** (Versammlungs- und Vereinigungsfreiheit)
- **Art 48 GRC** (Unschuldsvermutung im Strafverfahren)

Grundsätzlich sollte das Verhältnis zwischen einem demokratischen Verfassungsstaat und seinen Bürgerinnen und Bürgern bzw. allen in seinem Machtbereich lebenden Menschen von Vertrauen geprägt sein. Die/der Einzelne soll darauf vertrauen können, dass in ihre/seine grundrechtlich geschützten Positionen im Zuge von Ermittlungstätigkeiten bzw. Strafverfolgungsmaßnahmen grundsätzlich nur bei Vorliegen entsprechender Verdachtsmomente, also als ultima ratio, unter Wahrung der rechtstaatlichen Prinzipien, insbesondere unter Beachtung des Verhältnismäßigkeitsprinzips eingegriffen wird. Der Grundsatz, dass gegen eine bestimmte Person ausschließlich bei Vorliegen von Verdachtsmomenten Ermittlungs- bzw. Verfolgungsmaßnahmen gesetzt werden, zieht sich gleich einem roten Faden durch alle rechtsstaatlichen Gesetzgebungen moderner demokratischer Prägung.

Die VDS-RL geht von diesem Grundsatz ab, indem sie eine **verdachtsunabhängige**, gleichsam antizipierte **„Sicherung von Beweismitteln"** vorschreibt. Die Grundidee dabei ist simpel: Potenziell und prinzipiell ist jeder verdächtig.

Es wurden zwar schon vor Inkrafttreten der VDS-RL vielfältig personenbezogene Daten ermittelt und verarbeitet. Bisher mussten verarbeitete Verkehrs- und Standortdaten jedoch teilweise sofort, grundsätzlich aber jedenfalls dann gelöscht werden, wenn und soweit sie etwa für die Bereitstellung von Telekommunikationsdiensten und in weiterer Folge für die Abrechnung nicht mehr erforderlich waren, wurde diese im Sinne eines effektiven und grundrechtskonformen Datenschutzes normierte Löschungsverpflichtung durch die Richtlinie 2006/24/EG in eine verdachtsunabhängige, flächendeckende Speicherungspflicht verkehrt, um „schwere Straftaten", insbesondere Terrorakte und organisierte Kriminalität, bekämpfen zu können.

Die Vorratsdatenspeicherung stellt im Ergebnis einen **Paradigmenwechsel** dar, der **aus grundrechtlicher Sicht nicht zu rechtfertigen** ist. Eine vergleichbare Maßnahme in der „realen" Welt wäre, wenn künftig gesetzlich vorgeschrieben würde, alle Absender und Adressaten jedweden Briefes durch die Post dokumentieren zu lassen, weil potentiell jeder Briefkontakt ermittlungsrelevante Information liefern könnte.

III.2. Die schleichende (atmosphärische) Veränderung der Gesellschaft durch die VDS

Die Intensität des Eingriffs für den Grundrechtsträger wird davon beeinflusst, welche über die Informationserhebung hinausgehenden Nachteile ihm aufgrund der Maßnahme drohen oder von ihm nicht ohne Grund befürchtet werden. Die Schwere des Eingriffs nimmt mit der Möglichkeit der Nutzung der Daten für Folgeeingriffe in Grundrechte der Betroffenen zu, sowie mit der Möglichkeit der Verknüpfung mit anderen Daten, die wiederum andere Folgemaßnahmen auslösen können [Vgl BVerfGE 100, 313 (376); 113, 348 (382); 115, 320 (347 f); BVerfG, NJW 2007, 2464 (2469)].

Zu bedenken ist auch, dass im Fall einer konkreten Datenverwendung durch Strafverfolgungsbehörden aber nicht nur in die Rechtssphäre etwa eines möglichen Straftäters oder dessen Komplizen eingegriffen wird, sondern auch in die Rechtssphäre derjenigen Personen, die mit den Adressaten der Maßnahme über Telekommunikationseinrichtungen nur zufällig in Verbindung standen oder stehen. Dies schafft ein System der Überwachung zum Schutze der Sicherheit (vorgeblich) der Gesellschaft, tatsächlich aber vorrangig jener des Staates; dieses System könnte die Demokratie bzw. die Rechtsstaatlichkeit, die es schützen soll, aushöhlen bzw. umgehen.

Vor allem aber verlieren die Menschen das Gefühl, frei, selbstbestimmt und unbeobachtet leben zu können und nicht behelligt zu werden, wenn, soweit und solange sie die Gesetze des Staates achten und befolgen und nicht delinquent werden. Das Verhalten der Menschen wird sich unter der verdachtsunabhängigen Erfassung alltäglicher Lebensäußerungen schleichend verändern, wo Vertrauen die Basis zwischenmenschlicher Kommunikation war, wird Misstrauen herrschen.

Anhand einiger weniger Beispiele soll verdeutlicht werden, inwieweit Menschen durch die Vorratsdatenspeicherung in der angstfreien Inanspruchnahme ihrer Grundrechte eingeschränkt oder verunsichert werden können:

- Inanspruchnahme von Aidsberatungsstellen, psychologischen Diensten, Seelsorgern, Kontakt zu Rechtsanwälten, Ärzten generell, Kontakt zu diskriminierten bzw. unter Generalverdacht stehenden Gruppen usw. (**Art. 7 GRC**);
- Mitteilungen an Medien/Redaktionen im öffentlichen Interesse (whistleblowing), Meinungsäußerung in Blogs, Foren etc (**Art. 11 GRC**);

- Beitritt oder auch nur Besuch von oder Kontaktnahme zu politischen Parteien, Religionsgemeinschaften, Vereinigungen (zB unbequeme Bürgerinitiativen), Teilnahme an Demonstrationen etc. (**Art. 12 GRC**).

Überall dort, wo Personen befürchten, aufgrund der Vorratsdatenspeicherung bei der Inanspruchnahme von Grundrechten eventuell Nachteile zu erleiden, beeinträchtigt die Vorratsdatenspeicherung diese Grundrechte.

III.3 Zur Bedeutung der Unschuldsvermutung in einem freien Gemeinwesen

Die garantierte Unschuldsvermutung ist eine wesentliche Voraussetzung einer auf angstfreier Kommunikation basierenden Gesellschaft freier Menschen. Der EGMR hat zur Bedeutung der Unschuldsvermutung in S. und Marper vs UK klargestellt (zitiert aus NL Menschenrechte, http://www.menschenrechte.ac.at/docs/08_6/08_6_14):
„Im vorliegenden Zusammenhang kommt der Gefahr der Stigmatisierung besondere Bedeutung zu. Diese ergibt sich aus der Tatsache, dass Personen in der Situation der Bf., die nicht verurteilt wurden und für die daher die Unschuldsvermutung gilt, gleich behandelt werden wie verurteilte Personen. Zwar kann die Speicherung der privaten Daten der Bf. nicht mit der Äußerung eines Verdachts gleichgesetzt werden. Ihre Wahrnehmung, nicht als unschuldig behandelt zu werden, wird aber dadurch verdeutlicht, dass ihre Daten ebenso wie die von verurteilten Personen unbeschränkt gespeichert werden, während die Daten von nie verdächtigten Personen vernichtet werden müssen. Die Regierung bringt dazu vor, der einzige Grund für die Speicherung der Daten bestehe in der Steigerung der Größe und damit der Nutzbarkeit der Datenbank zur künftigen Identifizierung von Straftätern. Der GH hält dieses Argument jedoch für schwer vereinbar mit der gesetzlichen Verpflichtung zur Vernichtung der Fingerabdrücke und Proben von Freiwilligen, hätte dieses Material doch ähnlichen Wert für die Vergrößerung der Datenbank."

Die flächendeckende Speicherung erhöht zweifellos die Wahrscheinlichkeit, dass sich auch unbescholtene und unschuldige Menschen in einem Ermittlungsverfahren rechtfertigen müssen, warum sie in einer bestimmten Weise zu einer bestimmten Zeit mit einem bestimmten Anschluss in Kontakt standen. Allein in solche Ermittlungen zu geraten – auch wenn sich später herausstellt, dass es rein zufällig war und keine rechtlichen Konsequenzen folgen – kann schon zu erheblichen nachteiligen privaten oder beruflichen Konsequenzen führen.

Die Vorratsdatenspeicherung ist jedenfalls geeignet, den Kreis der Verdächtigen zu vergrößern, weil die Zahl der auswertbaren Kommunikationsverbindungen größer und umfassender wird. Beachtlich ist dabei auch die Gefahr, die aus der systemimmanenten unzuverlässigen Aussagekraft der durch die Vorratsspeicherung erfassten Verbindungs- und Zugangsdaten resultiert.

Die Verkehrsdaten werden dabei der Person des Anschlussinhabers zugeordnet. Zugleich ist ein Rückschluss vom Inhaber des Anschlusses auf den tatsächlichen Nutzer des Kommunikationsmittels weder technisch noch logisch zwingend indiziert. Die Informationen aus den Verkehrsdaten können also stets nur ein erster Ermittlungsansatz sein.

Damit kommt der Inhaber eines von der VDS erfassten Kommunikationsanschlusses mit stark erhöhter Wahrscheinlichkeit in die Lage, sich im Zuge konkreter Ermittlungen praktisch „frei beweisen" zu müssen. Man muss dann bis zu zwei Jahre im Nachhinein erklären können, warum man jemanden kontaktiert hat (oder von jemandem kontaktiert wurde). Denn die andere Person mag verdächtig sein – man selbst ist es aufgrund der Kommunikation also auch. **Die bloße Behauptung *„ich kann mich nicht erinnern"* wird zwar sehr oft der Wahrheit entsprechen, aber nützen wird sie nichts – bis zur Beseitigung jeglichen Verdachts!**

Die Vorratsdatenspeicherung ist eine Abkehr vom Grundsatz der Vertraulichkeit der Kommunikation aufgrund eines generellen Misstrauens gegenüber allen Menschen. Wenngleich die Unschuldsvermutung erst im Zuge konkreter Ermittlungsmaßnahmen im Einzelfall unmittelbar relevant wird, wird eine Verletzung derselben durch die VDS doch perpetuiert.

III.4 Argumentation nach dem Schema der Verhältnismäßigkeitsprüfung

III.4.1 Die Vorratsdatenspeicherung (VDS) betrifft alle Nutzer von Kommunikationsdiensten aktuell, unmittelbar und nachteilig in ihrer Grundrechtssphäre.

Schon die Speicherung der Verbindungsdaten ist ein Grundrechtseingriff, nicht erst eine allfällige Auskunft an die Behörden – diese aber natürlich auch.

Der EGMR wertet in *Segerstedt-Wiberg u.a. v. Schweden*, Nr. 62332/00, 06.06.2006 in § 72 des Urteils die Sammlung und Aufbewahrung allgemein zugänglicher Quellen wie Artikel in Zeitschriften als Eingriff in das Privatleben, sofern sie systematisch durch Behörden (Geheimdienste, Verfassungsschutz) erfolgt. **Revolutionär für den EGMR ist in *Segerstedt-Wiberg* aber die Feststellung, dass allein schon die (überschießende bzw. nicht gerechtfertigte) Speicherung von Daten einerseits Art. 8 EMRK verletzt, andererseits aber auch Art. 10 und 11 EMRK,** also die Rechte auf Meinungs- und Versammlungsfreiheit (in § 107 des Urteils stellte der GH fest, dass eine Speicherung von Daten zu politischen Überzeugungen, Tätigkeiten und Parteizugehörigkeit, die nicht nach Art. 8 Abs. 2 gerechtfertigt werden kann, ipso facto auch eine Verletzung der politischen Rechte aus Art. 10 und 11 EMRK bedeute).

Dieser Argumentation folgend bewirkt die in der VDS-RL normierte Speicherverpflichtung einen Eingriff in **Art 7 GRC, Art 8 GRC, Art 11 GRC und Art 12 GRC**. Der Eingriff in **Art 48 GRC** (Unschuldsvermutung) wurde bereits unter Punkt III.3 argumentiert.

III.4.2 Die VDS ist gar nicht geeignet, die vorgeblichen Zwecke zu erreichen

Die von der zugrundeliegenden Richtlinie vorgegebene Bekämpfung schwerer Kriminalität wird durch die VDS nicht merkbar gefördert (belegt durch Studien, keine Gegenstudien, immer nur emotionale Einzelfälle). Beispielsweise fasst eine aktuelle Studie des deutschen Max-Planck-Instituts für Strafrecht und Kriminologie als Ergebnis ihrer Untersuchung zu den deliktsspezifischen Aufklärungsquoten für den Zeitraum 1987 bis 2010 in Deutschland zusammen, dass der Wegfall der Vorratsdatenspeicherung nicht als Ursache für Bewegungen in der Aufklärungsquote herangezogen werden kann. Dieser Befund gilt insbesondere für die Bereiche der Computerkriminalität sowie der so genannten Internetkriminalität. Die Studie selbst liefert die Zahlen deliktsspezifisch und stellt fest, dass sich keine Bewegung durch den Wegfall der VDS ergibt.

Ein „Ausweichen" ist in vielen Fällen trivial. Untersuchungen zeigten auch, dass Terroristen bereits jetzt gerade so kommunizieren, dass sie von der VDS nicht erfasst werden. Nutzlos erscheint die VDS auch hinsichtlich der häufig besonders zur Rechtfertigung der VDS angeführten Einzeltäter (Breivik etc.): Diese kommunizieren nämlich mit gar niemandem (über die geplante Tat) und wären daher von der VDS gar nicht erfasst. Selbst dessen Suche nach Bombenbauanleitungen wäre mit der VDS nach aktueller Rechtslage auch nicht erfassbar, da die Speicherung von Inhaltsdaten ausdrücklich ausgeschlossen ist.

Selbst für den mittelschweren Bereich – zB Straftaten mit knapp über einem Jahr Strafrahmen (worunter aufgrund der unübersehbaren Tendenz zur Verschärfung der Strafdrohungen in ganz Europa inzwischen fast jedes delinquente Verhalten fällt) – konnte kein Anstieg der Aufklärungsquote in jenen Mitgliedsstaaten belegt werden, in denen die VDS schon umgesetzt wurde. Gerade durch die Umsetzung könnte in diesem Bereich die Aufklärung sogar erschwert werden, da das Problem auch bei Kriminellen ins Blickfeld gerät und diese aktiv Gegenmaßnahmen ergreifen. Umgehungsmöglichkeiten werden allgemein bekannt.

Beachtenswert sind in diesem Zusammenhang insbesondere die Pläne in Großbritannien, die VDS auszuweiten auf Facebook-, Twitter- und Online-Spiel-Kommunikation - also sind die bisherigen Mittel der VDS offensichtlich nicht ausreichend oder nicht geeignet.

III.4.3 Die VDS ist selbst dort, wo sie möglicherweise in manchen Einzelfällen die Ermittlungen unterstützt, nicht das schonendste Mittel, den Zweck zu erreichen.

In den meisten Fällen würden schon betrieblich notwendig vorhandene Daten reichen, wenn die Investitionen zur VDS besser in mehr Personal der Exekutive investiert und Ermittlungen beschleunigt würden.

In den übrigen Fällen würde ein abgekürztes Verfahren reichen, bei dem ein Gericht bei entsprechender Verdachtslage anordnet, bestimmte Daten von bestimmten Teilnehmern "einzufrieren" (sog. "**Quick-Freeze**") Siehe dazu die **Cybercrime Konvention**, der Österreich zwar beigetreten ist (23.11.2001), welche aber nach mehr als 10 Jahren noch immer nicht ratifiziert ist – gar so dringend scheint die Verfolgung und der Datenbedarf also gar nicht zu sein. Laut (inoffiziellen) Aussagen von Polizisten scheint es insbesondere ein praktisches Problem zu sein, an benötigte Daten in anderen Ländern heranzukommen (sind diese vorhanden und ist die Auskunftserteilung legal etc). Es läge daher näher, das bereits bestehende „Arsenal" effektiv (bzw überhaupt) zu nutzen, bevor neue (weitere Daten) gesammelt werden.

III.4.4 Die VDS steht selbst dann, wenn man sie als das gelindeste, noch zum Ziel der Kriminalitätsbekämpfung führende Mittel ansieht, in keinem angemessenen Verhältnis zum Nachteil für die Einzelnen sowie die Gesellschaft

Je fragwürdiger die Eignung und die Notwendigkeit (im Sinne des gelindesten Mittels) erscheinen, desto höher sind die Anforderungen an die Verhältnismäßigkeit des Eingriffs. Die Güterabwägung zeigt - wenn überhaupt - nur einen geringen positiven Effekt in wenigen Einzelfällen gegenüber einem schweren Eingriff in die Privatsphäre praktisch der gesamten Bevölkerung.

III.4.5 Normierte Zwecke

Falls die VDS nicht schon dem Grunde nach als unverhältnismäßig gesehen wird, ergibt sich die mangelnde Verhältnismäßigkeit daraus, dass die Verwendungszwecke („Ermittlung, Feststellung und Verfolgung schwerer Straftaten") viel zu vage und zu weit gefasst sind. **Was „schwere Straftaten" sind, wird in der Richtlinie 2006/24/EG nicht gar nicht definiert.**

Im Falle der Verhütung künftiger Straftaten kann nicht an dieselben Kriterien angeknüpft werden, die für die Gefahrenabwehr oder die Verfolgung begangener Straftaten entwickelt worden sind.

Maßnahmen der **Gefahrenabwehr** setzen eine **konkrete aktuelle Gefahrenlage** voraus, während die **Strafverfolgung** an den Verdacht einer **schon verwirklichten Straftat** anknüpft. Bei der Vorverlagerung des Eingriffs in eine Phase, in der sich noch kein konkreter Straftatbestand abzeichnet, besteht das Risiko, dass der Eingriff lediglich an ein noch schwer(er) fassbares Geschehen anknüpft.

Da der Eingriff sich auf mögliche zukünftige Aktivitäten bezieht, kann er sich häufig nur auf Tatsachen stützen, bei denen noch offen ist, ob sie sich zu einer Rechtsgutverletzung weiterentwickeln (Vgl BVerfGE 110, 33 (59)).

Man sondiert Kommunikationsvorgänge, bei denen nicht unbedingt klar sein muss, ob sie überhaupt mit einer Rechtsverletzung in Verbindung stehen. Sieht der Gesetzgeber in solchen Situationen Grundrechtseingriffe vor, so hat er die den Anlass bildenden Straftaten sowie die Anforderungen an Tatsachen, die auf die künftige Begehung hindeuten, derart bestimmt zu umschreiben, dass das besonders hohe Risiko einer Fehlprognose noch innerhalb des verfassungsrechtlichen Rahmens bleibt. Die Norm muss handlungsbegrenzende Tatbestandselemente enthalten, die einen Standard an Vorhersehbarkeit und Kontrollierbarkeit vergleichbar dem schaffen, der für die Aufgaben der Gefahrenabwehr und Strafverfolgung rechtsstaatlich geboten ist (Vgl BVerfGE 110, 33 (56)). Es muss den Betroffenen vorhersehbar und kontrollierbar (d.h. einsehbar) sein, aufgrund welcher ihrer Handlungen ihre Vorratsdaten von den Behörden verwendet werden.

III.4.6 Anforderungen an die gesetzlichen Grundlagen

III.4.6.1 Eingriffe in den Schutzbereich des Art 8 EMRK bedürfen einer Rechtfertigung.

Gemäß Art. 8 Abs. 2 EMRK ist zunächst eine gesetzliche Grundlage für Eingriffe erforderlich. Nach dem Urteil des EGMR im Fall ***Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien*** vom 28.6.2007 (siehe insbesondere § 71 mit Hinweisen auf ***Malone gg. das Vereinigte Königreich, Kruslin gg. Frankreich***, § 27; ***Huvig gg. Frankreich***, § 26; ***Kopp gg. die Schweiz,*** § 55, und ***Amann gg. die Schweiz***, § 50) verlangt der Ausdruck „gesetzlich vorgesehen", wie er in Art. 8 Abs. 2 EMRK verwendet wird, nicht nur, dass die angefochtene Maßnahme eine Grundlage im innerstaatlichen Recht hat. Er bezieht sich darüber hinaus auch auf die Qualität dieses Gesetzes und verlangt, dass es für die betroffenen Personen zugänglich sein muss und diese im Einklang mit dem Rechtsstaatsprinzip auch in der Lage sind, die Konsequenzen vorherzusehen.

III.4.6.2 Aus dem Erfordernis einer gesetzlichen Grundlage in Verbindung mit dem in der Präambel der EMRK verankerten Rechtsstaatsprinzip leitet der EGMR zudem ab, dass das eingreifende innerstaatliche Recht hinreichend bestimmt und für den Bürger zugänglich sein muss (EGMR, ***Lambert gg. Frankreich***, 24.08.1998). Dem Einzelnen müsse es möglich sein, sein Verhalten den Vorschriften entsprechend einzurichten, was ein – gemessen an der Schwere des Eingriffs – hinreichendes Maß an Vorhersehbarkeit voraussetze.

Räumt das nationale Recht der Exekutive oder dem zuständigen Richter bei der Durchführung bzw Anordnung von Maßnahmen Ermessen ein, dann verlangt das Bestimmtheitserfordernis – auch und gerade bei geheimen Maßnahmen –, dass der zulässige Zweck der Maßnahme, die Reichweite und Grenzen des Ermessens sowie die Kriterien, nach denen es auszuüben ist, hinreichend erkennbar sind, insbesondere, dass vorhersehbar ist, unter welchen Umständen Eingriffe zulässig sind (EGMR, ***Malone gg. Großbritannien***, 27.06. 1984; EGMR, ***Kopp gg. die Schweiz,*** 25.03. 1998).

Die **Anforderungen an die Vorhersehbarkeit im Einzelnen** hängen von der **Eingriffstiefe** der jeweiligen Maßnahme ab, sodass schwerwiegende Eingriffe eine besonders präzise gesetzliche Regelung erforderlich machen.

Für den Fall einer Informationssammlung und -speicherung durch einen Geheimdienst wurde etwa entschieden, dass das nationale Recht detailliert festlegen muss, welche Arten von Informationen gespeichert werden dürfen, gegenüber welchen Personengruppen Überwachungsmaßnahmen ergriffen werden dürfen, unter welchen Umständen Informationen gesammelt werden dürfen, welches Verfahren dabei einzuhalten ist, nach welcher Zeitdauer erlangte Informationen zu löschen sind, welche Personen auf den Datenbestand zugreifen dürfen, die Art und Weise der Speicherung, das Verfahren des Informationsabrufs sowie die zulässigen Verwendungszwecke für die abgerufenen Informationen (EGMR, ***Rotaru gg. Rumänien***, 29.03.2000).

Zum Schutz vor Missbrauch durch Telefonüberwachung ohne Wissen des Betroffenen hat der EGMR die detaillierte Festlegung der folgenden Umstände durch das nationale Recht gefordert:

Gegen welche Personen und bei welchen Straftaten das Instrument der Telefonüberwachung eingesetzt werden darf, die maximale Dauer der Überwachungsmaßnahme, das Verfahren, in welchem Abhörprotokolle erstellt werden, die Sicherungsmaßnahmen dafür, dass die Originalbänder intakt und in ihrer Gesamtheit erhalten bleiben, damit sie vom Richter und dem Verteidiger des Beschuldigten untersucht werden können, sowie Fristen für die Löschung der erlangten Informationen (EGMR, ***Kruslin gg. Frankreich***, 27.03.1990). Für den Fall, dass unbeteiligte Dritte von einer Überwachungsmaßnahme betroffen sind (z.B. als Gesprächspartner eines Verdächtigen), müssen Sicherungsvorkehrungen in Bezug auf deren Daten vorgesehen werden (EGMR, ***Amann gg. die Schweiz***, 12.01.2000).

III.4.6.3 Auch wenn Strafverfolgungsorgane um die Herausgabe von Daten „bitten", ohne dass Telekommunikationsunternehmen dazu zu verpflichtet sind, ist es erforderlich, dass die freiwillige Übermittlung der angeforderten Daten nach innerstaatlichem Recht rechtmäßig und die Befugnis der Strafverfolgungsorgane zur Anforderung solcher Daten detailliert geregelt ist (EGMR, ***Malone gg. Großbritannien***, 27.06. 1984). In jedem Fall muss der Staat angemessene Maßnahmen ergreifen, um zu verhindern, dass Dritte unbefugt Kenntnis von überwachten Telekommunikationsinhalten erlangen (EGMR, ***Craxi gg. Italien***, 26.06.2003).

III.4.6.4 Vor allem in Bezug auf § 99 Abs 5 Z 3 und 4 des österreichischen Telekommunikationsgesetzes („TKG") iVm § 53 Abs 3a und 3b des österreichischen Sicherheitspolizeigesetzes („SPG") ist der Rechtsschutz äußerst mangelhaft, weil die Auskünfte keine Einschränkungen auf den Schutz höherrangiger Rechtsgüter (z.B. Leben, Gesundheit oder Freiheit eines Menschen) vorsehen, sondern Auskünfte allgemein zur Abwehr gefährlicher Angriffe (§ 16 SPG) zulassen.

Ebenso wenig vorgesehen ist eine vorherige Genehmigung im Sinne eines Vier-Augen-Prinzips, eine unabhängige richterliche Kontrolle ist dem SPG insgesamt fremd.

Ebenso ist für Datenauskünfte gemäß § 99 Abs 5 Z 2 TKG iVm § 76a Abs 2 der österreichischen Strafprozessordnung („StPO") kein Richtervorbehalt vorgesehen, und auch hier gibt es keine Einschränkung auf „schwere Straftaten" mit einem bestimmten Mindestmaß an Strafdrohung.

Trotz Richtervorbehalts ist aber auch die Grundregel zur Verwendung von Vorratsdaten in § 102b TKG iVm § 135 Abs 2a StPO zu weit gehend, weil die Delikte, für deren Aufklärung eine Auskunft zulässig ist, lediglich eine Höchststrafdrohung von mehr als einem Jahr Freiheitsstrafe beinhalten müssen. Eine Durchsicht des StGB zeigt, dass hier Delikte erfasst sind, die doch weit entfernt von der ursprünglichen Rechtfertigung der VDS – Bekämpfung von organisierter Kriminalität und Terrorismus – erscheinen, beispielsweise § 123 StGB (Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses, Strafdrohung bis 2 Jahre Freiheitsstrafe).

III.4.7 Sonderproblem IP-Adressen:

Ermittlungsrelevante IP-Adressen „fallen nicht vom Himmel", sondern man kommt an sie nur (außer: Verschlüsselung) heran, **wenn man vorher den Inhalt einer Kommunikation (= aufgerufener Dienst, besuchte Website, etc) kennt** und von dort die IP-Adresse eines Nutzers erfährt. Sie können daher nicht einfach als „harmlose Zugangsdaten" angesehen werden, da mit ihnen immer ein Zusammenhang zwischen Inhalt und Person hergestellt wird. Die Auskunft über Zugangsdaten ist immer erst ein weiterer Ermittlungsschritt, bei dem eine inhaltlich bestimmte Kommunikation auf einen bestimmten Teilnehmer zurückgeführt werden soll.

Anschaulich lässt sich eine IP-Adresse als eine Art KFZ-Kennzeichen auf dem „Datenhighway" beschreiben. Vielfach wird daher eine Art „IT-Lenkererhebung" erforderlich sein, um Aussagekraft und Zuverlässigkeit der ermittelten Daten beurteilen zu können; denn eine reine Gefährdungshaftung für Inhaber von Internet- oder Telefonanschlüssen ist der österreichischen Rechtsordnung bislang nicht bekannt. Der Aussagekraft und mit ihr verbunden dem tatsächlichen Nutzen der Daten für den angestrebten Zweck kommen für die Verhältnismäßigkeit der behördlichen Befugnisse entscheidende Bedeutung zu, die bereits abstrakt in jeden Abwägungsvorgang mit einzubeziehen sind.

Problematisch ist auch, dass die IP-Adressen sich oft **lange nicht ändern** (statische sowieso nicht, aber auch dynamische): Die Polizei kann also eine **„Registratur"** für die Zukunft aufbauen, da es **keine klare Bestimmungen gibt, die Daten nachher zu löschen**, solange nicht völlig eindeutig ist, dass die Daten für die Strafverfolgung oder Gefahrenabwehr unbrauchbar sind (dies wird aber sehr selten zu argumentieren sein, vor allem im Zusammenhang mit Ermittlungen im Umfeld von organisierter Kriminalität.)

III.4.8 Die Praxis der VDS und die Verletzung materieller Grundrechte

III.4.8.1 Verletzung des Rechts auf Datenschutz gemäß **Artikel 7 GRC** durch die VDS.

Mittels elektronischer Datenverarbeitung sind Einzelangaben über persönliche oder sachliche Verhältnisse einer Person unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar.

Sie können darüber hinaus **mit anderen Datensammlungen zusammengefügt** werden, wodurch vielfältige Nutzungs- und Verknüpfungsmöglichkeiten entstehen. **Dadurch können weitere Informationen erzeugt und Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch anschließende Eingriffe in seine Privatsphäre nach sich ziehen können**.

Eine weitere Besonderheit des Eingriffspotentials von Maßnahmen der elektronischen Datenverarbeitung liegt in der **Menge** der potentiell verarbeitbaren Daten, die auf konventionellem Wege nicht bewältigt werden könnten. Der mit solchen technischen Möglichkeiten einhergehenden **gesteigerten Gefährdungslage** entspricht der **Steigerung des Bedürfnisses nach einem hierauf bezogenen, verbesserten Grundrechtsschutz**.

Mit in den Blick zu nehmen ist zum anderen auch die Persönlichkeitsrelevanz **der Informationen, die durch eine weitergehende Verarbeitung und Verknüpfung der erfassten Informationen gewonnen werden sollen** oder auch nur können. Ferner ist bedeutsam, ob der Betroffene, etwa durch eine Rechtsverletzung, einen ihm zurechenbaren **Anlass** für eine Datenerhebung geschaffen hat oder ob die Erhebung **anlasslos** erfolgt und damit praktisch auch jeden anderen hätte treffen können. Informationserhebungen gegenüber Personen, die den Eingriff durch ihr Verhalten nicht veranlasst haben, sind grundsätzlich **von höherer Eingriffsintensität als anlassbezogene**.

Werden Personen, die keinen Erhebungsanlass gegeben haben, in großer Zahl in den Wirkungsbereich einer Maßnahme einbezogen, können von ihr auch allgemeine **Einschüchterungseffekte** ausgehen, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können (Vgl BVerfGE 65, 1 (42); 113, 29 (46)). Die Unbefangenheit des Verhaltens wird insbesondere gefährdet, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass **Risiken des Missbrauchs** und ein diffuses **Gefühl der ständigen Überwachung** entstehen.

III.4.8.2 Aus der Judikatur des EGMR ergibt sich explizit, dass auch „äußere Gesprächsdaten", also gewählte Nummer, Zeitpunkt und Dauer, vom Schutzbereich des Art 8 Abs 1 EMRK umfasst sind und ein Eingriff in dieses Grundrecht insbesondere auch dann vorliegt, wenn solche Daten **ohne Zustimmung des Betroffenen** an staatliche Behörden übermittelt werden (EGMR, *Malone gg. Großbritannien*, 27.06. 1984. Abs. 83f.)

Der EGMR selbst hat im Zusammenhang mit ähnlich gelagerten Fällen bereits mehrfach ausgesprochen, dass schon das bloße Bestehen eines Gesetzes, das eine geheime Überwachung der Telekommunikation erlaubt, für alle Personen, auf die es Anwendung findet, die Gefahr der Überwachung mit sich bringt. Diese Gefahr greife notwendigerweise in die Freiheit der Kommunikation zwischen Benützern von Telekommunikationseinrichtungen ein und stelle daher unabhängig von irgendwelchen tatsächlich gegen sie ergriffenen Maßnahmen einen Eingriff in die durch Art 8 EMRK geschützten Rechte dar (EGMR, ***Weber und Saravia gg. Deutschland***, App. Nr. 54934/00, Abs 78 mit Hinweisen auf frühere Rechtsprechung in Klass, Malone).

III.4.9 Eingriffe in den Schutzbereich

Im Urteil ***Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien*** entschied der EGMR im Hinblick auf Entscheidungen in anderen Fällen (siehe ***Klass u.a. gg. Deutschland***, § 41; ***Malone gg. das Vereinigte Königreich***, § 64; ***Weber und Saravia gg. Deutschland***, §§ 77-79), dass das Bestehen von Rechtsvorschriften, die eine geheime Überwachung erlauben, selbst einen Eingriff in das Recht nach Art 8 EMRK darstellt.

Im Urteil ***Copland gg. das Vereinigte Königreich*** entschied der Gerichtshof überdies, dass die Erhebung von Verbindungsdaten ohne Einwilligung des Betroffenen einen Eingriff in dessen Rechte auf Achtung des Privatlebens und des Briefverkehrs darstellt. Dies gilt neben Telefonaten auch für die Erhebung von näheren Umständen der E-Mail-Nutzung und der Internetnutzung (EGMR Urteil ***Copland gg. das Vereinigte Königreich)***. Sowohl in der Erhebung wie auch in der Speicherung dieser Daten liegt ein Grundrechtseingriff, selbst wenn die Daten auf legalem Wege erlangt werden. (EGMR Urteil ***Rotaru gg. Rumänien)***.

Es lässt sich also festhalten, dass jede staatliche Verwendung (Erhebung, Speicherung, Verarbeitung und Weitergabe) von personenbezogenen Informationen einen Eingriff in Art. 8 EMRK darstellt. Der EGMR entschied ebenso bereits wiederholt, dass auch Telefongespräche als „Briefverkehr/Korrespondenz" iSd Art. 8 EMRK anzusehen sind (EGMR Urteil ***Niemietz gg. Deutschland)***. Art. 8 EMRK schützt dabei sowohl geschäftliche als auch private Kommunikation (EGMR Urteil ***Leander gg. Schweden***, 25.02.1987*)*. Eine Subsumtion unter den Begriff des „Privatlebens" fällt insofern leichter, als der Gerichtshof unter Bezugnahme auf die Europäische Datenschutzkonvention (EGMR Urteil ***Silver gg. Großbritannien***, 25.02.1983) allgemein anerkennt, dass die Sammlung und Speicherung personenbezogener Daten einen Eingriff in das Privatleben des Einzelnen darstellt (EGMR Urteil ***Leander gg. Schweden***, 25.02.1987), ebenso wie die Verwendung solcher Daten und die Verweigerung ihrer Löschung.

Dass sich der Staat zur Speicherung solcher Daten privater Unternehmen bedient, kann keinen Unterschied machen, wenn er sich gleichzeitig selbst Zugriff auf die gespeicherten Daten eröffnet. **Andernfalls könnte der Staat seine Grundrechtsbindung durch ein bloßes „Outsourcing" von Maßnahmen umgehen**.

Die Inanspruchnahme Privater erhöht das Gewicht des Eingriffs sogar noch, da sich der Kreis von – weitgehend ohne Schuld – beeinträchtigten Personen durch den zusätzlichen Eingriff entsprechend vergrößert. Zudem ist das Risiko, dass gespeicherte Daten missbraucht werden, durch eine Vielzahl von Daten erfassende Privatunternehmen erheblich höher einzuschätzen als im Fall einer Speicherung durch staatliche Stellen.

In einer demokratischen Gesellschaft ist eine Maßnahme nur erforderlich, wenn ein in Anbetracht des Stellenwerts des garantierten Freiheitsrechts hinreichend dringendes soziales Bedürfnis nach ihr besteht, sie einen legitimen Zweck verfolgt und ihre Belastungsintensität nicht außer Verhältnis zu dem Gewicht des Zwecks steht (EGMR Urteil ***Silver gg. Großbritannien***, 25.02.1983). Der EGMR hat dazu eindeutig erklärt, dass das Interesse des Staates gegenüber den Interessen des Einzelnen an der Achtung seiner Privatsphäre abgewogen werden müsse (EGMR Urteil ***Leander gg. Schweden***, 25.02.1987). Eingriffe sind zwar nicht auf das unerlässliche Maß beschränkt, aber ein bloßes Nützlichsein oder Wünschenswertsein genügt nicht (EGMR Urteil, ***Silver gg. Großbritannien***, 25.02.1983). Sind die genannten Kriterien erfüllt, dann liegt keine Verletzung von Art 8 EMRK vor.

In Bezug auf die Vorratsdatenspeicherung von Telekommunikationsdaten ist die Rechtsprechung des EGMR so zu interpretieren, dass jede Form einer groß angelegten, allgemeinen oder sondierenden elektronischen Überwachung unzulässig ist, insbesondere, wenn nicht wegen einer bestimmten Tat oder Gefahr ermittelt wird, sondern nach möglichen Taten oder Gefährdungen gesucht werden soll.

V.4.10 Unverhältnismäßigkeit

Eine Beschränkung von Grundrechten ist nur insoweit zulässig, als sie zur Erreichung des angestrebten Zweckes geeignet und erforderlich ist und der mit ihr verbundene Eingriff seiner Intensität nach nicht außer Verhältnis zur Bedeutung der Sache und den von den Betroffenen hinzunehmenden Einbußen steht. Einbußen an grundrechtlich geschützter Freiheit dürfen nicht in unangemessenem Verhältnis zu den Zwecken stehen, denen die Grundrechtsbeschränkung dient.

Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person führen zwar dazu, dass der Einzelne Einschränkungen seiner Grundrechte hinzunehmen hat, wenn überwiegende Allgemeininteressen dies rechtfertigen. Der Gesetzgeber muss aber zwischen Allgemein- und Individualinteressen einen angemessenen Ausgleich herstellen. Dabei spielt auf grundrechtlicher Seite eine Rolle, unter welchen Voraussetzungen welche und wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind. Maßgebend sind also insbesondere die Gestaltung der Einschreitschwellen, die Zahl der Betroffenen und die Intensität der Beeinträchtigungen.

Im **Bereich der Telekommunikationsüberwachung** ist von Bedeutung, ob die Betroffenen als Personen anonym bleiben, welche Informationen erfasst werden können und welche Nachteile den Grundrechtsträgern aufgrund der Überwachungsmaßnahme drohen. Auf Seiten der mit dem Eingriff verfolgten Zwecke ist das Gewicht der Ziele maßgeblich, denen die Telekommunikationsüberwachung dient. Es hängt unter anderem davon ab, wie bedeutsam die Rechtsgüter sind, die mit Hilfe der Maßnahme geschützt werden sollen und wie wahrscheinlich der Eintritt einer Rechtsgutverletzung ist [vgl BVerfGE 100, 313 (375f.)].

Die Ermächtigung zur Speicherung und in der Folge zur Überwachung der Telekommunikation zwecks Vorsorge für die Verfolgung und die Verhütung der in Bezug genommenen Straftaten genügt den Anforderungen der Verhältnismäßigkeit im engeren Sinne nicht.

Die Standortkennung eingeschalteter Mobilfunkendeinrichtungen kann zur **Erstellung eines Bewegungsbildes** führen, über das gegebenenfalls auf **Gewohnheiten der betroffenen Personen oder auf Abweichungen hiervon** geschlossen werden kann. Schließlich ist zu bedenken, dass die Zuordnung von Verbindungs- und Bestanddaten, insbesondere von IP-Adressen, zu einer bestimmten Person selbst keine Rückschlüsse darüber zulässt, ob diese Person auch am interessierenden Kommunikationsvorgang beteiligt war. Hierzu bedarf es weiterer konkretisierender Indizien, welche gerade bei der Erforschung von Kommunikationsvorgängen im Internet häufig nur schwer fassbar sind.

Grundrechtlich bedeutsam ist ferner die große Streubreite der möglichen Eingriffe. Die Erhebung von Verbindungsdaten kann eine große Zahl von Personen treffen. Erfasst werden nicht nur potenzielle Straftäter, sondern auch sämtliche Personen, mit denen diese im betreffenden Zeitraum Telekommunikationsverbindungen nutzen. Dazu können etwa auch Personen gehören, die in keiner Beziehung zu einer möglicherweise zu verhütenden oder später zu verfolgenden Straftat stehen, wie etwa Kontakt- und Begleitpersonen oder gänzlich unbeteiligte Dritte.

Eingriffe dieser Art bergen darüber hinaus auch deshalb hohe Risiken für die Rechte der Betroffenen in sich. Gegen die angesprochenen Maßnahmen können Betroffene frühestens dann mit rechtlichen Mitteln vorgehen, wenn die Maßnahmen bereits vollzogen sind und sie über die Tatsache, dass solche Maßnahmen getroffen wurden, informiert wurden oder davon auf andere Weise Kenntnis erlangen konnten. Bei Maßnahmen der Vorfeldermittlung ist aufgrund der Ungewissheit, ob und wann Straftaten begangen werden, regelmäßig mit einer längeren Zeitdauer bis zu einer (allfälligen) Unterrichtung zu rechnen als bei sonstigen Überwachungsmaßnahmen.

Die Verwertung in anderen Zusammenhängen ist ein eigenständiger Eingriff. Die Datenerhebung im Vorfeld der Begehung von Straftaten kann aufgrund der fehlenden Begrenzung auf eine konkret in Verwirklichung begriffene oder schon begangene Straftat vielfältig nutzbare Informationen ergeben.

Die Bindung an den Zweck, den das zur Kenntnisnahme der Daten ermächtigende Gesetz festgelegt hat, wird bei der weiteren Verwertung der erlangten Informationen praktisch kaum haltbar sein.

Die Möglichkeit der Verwendung der erhobenen Daten zu unbestimmten oder noch nicht bestimmbaren Zwecken erhöht damit die Schwere des Eingriffs schon in der Phase der Erhebung.

Das Urteil EGMR *S. und Marper vs UK* ist im vorliegenden Zusammenhang von besonderem Gewicht, weil selbst die Speicherung personenbezogener Daten von Personen, die einmal im Verdacht standen, eine strafbare Handlung begangen zu haben, vom EGMR als Verletzung des Art. 8 EMRK betrachtet wird. Umso mehr wirft die völlig verdachtsunabhängige Speicherung von Vorratsdaten die Frage nach einer Verletzung dieses Konventionsrechts auf.

VI. Anstelle einer Zusammenfassung

Würden die Antragsteller/innen sich selbst in die Sklaverei verkaufen, wäre ein solcher Vertrag ohne jeden Zweifel in jeder Rechtsordnung jedes Mitgliedsstaates der Europäischen Union nichtig. Auch das hier angerufene Gericht würde – so eine derartige Fragestellung an den EuGH herangetragen würde – in diesem Sinne entscheiden. Schon die rechtliche Eröffnung einer solchen Möglichkeit wäre zweifellos verfassungswidrig und eine Verletzung der GRC.

Die Menschen Europas wurden nicht gefragt, ob sie – um Benjamin FRANKLIN zu paraphrasieren – bereit sind, fundamentale Freiheit zu opfern, um kurzfristig ein wenig vermeintliche Sicherheit zu erkaufen.

Der Paradigmenwechsel von einer Politik der Freiheit zu einer Politik der (Staats-) Sicherheit beinhaltet das Problem, dass hier nicht von demokratisch legitimierten Gesetzgebern „Feinabstimmungen" zwischen Freiheit und Sicherheit durch Grundrechtseingriffe im Gefüge des demokratischen Gemeinwesens vorgenommen werden.

Tatsächlich resultiert ein nicht unerheblicher Anteil massiv freiheitsgefährdender Gesetze der letzten 20 Jahre aus „Empfehlungen" von Gruppen oder „informellen", zur Gesetzgebung nicht berufenen, demokratisch von niemandem legitimierten Institutionen, wie z.B. der FATF (Financial Action Task Force on Money Laundering), der auch die Europäische Union selbst beigetreten ist.

Die – verdachtsunabhängige – Vorratsdatenspeicherung ist eine „Einstiegsdroge" in den Sicherheits- und Überwachungsstaat, der die Abschaffung des Bargeldes folgen und an dessen Ende „der subkutane Chip für alle" stehen wird.

Die Vorratsdatenspeicherung wird zunächst das Bunte, Kreative, Anarchische, Individualistische in Europa – sohin alle unsere Stärken – nachhaltig beschädigen, ihren vorgeblichen Zweck – mehr Sicherheit für alle – wird sie hingegen nicht erfüllen. Am Ende der (befürchteten) Entwicklung werden wir (vielleicht) noch Menschen sein, aber keine freien Menschen. Der Europäischen Union als „Raum der Sicherheit, des Wohlstands, des Rechts und der Freiheit" wird dann etwas fehlen.

Und das Argument, man könne der Europäischen Union und ihren Mitgliedstaaten bzw. ganz allgemein den **Institutionen** nicht „auf Vorrat" Missbrauch unterstellen, ist Unsinn – die Geschichte, insbesondere auch die Geschichte Europas, beweist, dass Unrecht und Rechtsstaat einander nicht ausschließen. Außerdem: Über die Vorratsdatenspeicherung wird den **Menschen** verdachtsunabhängig und „auf Vorrat" der Missbrauch ihrer Freiheit, ihrer unveräußerlichen Rechte unterstellt.

Bei einem Paradigmenwechsel von einer Politik der Freiheit zu einer Politik der (nationalen, europäischen oder sonstigen) Sicherheit ist größtes Misstrauen und größte Vorsicht geboten.
Die Vorratsdatenspeicherung erweist sich als Einstieg in den „permanenten Ausnahmezustand".

„*Souverän ist, wer über den Ausnahmezustand entscheidet*" (Carl SCHMITT).

Wien, am 29. März 2013 für die Antragsteller/innen