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

Verfassungsgerichtshof
Freyung 8
1010 Wien

Per webERV

140509 Äußerung/Individualantrag/1/cms/sg
G 47/2012-23, G 59/2012-12
G 62/2012-17, G 70/2012-12
G 71/2012-8

Antragsteller:

1. **Ing. Dr. Christof TSCHOHL,** [redacted]
   Jurist, Ludwig Boltzmann Institut für Menschenrechte
   [redacted]
2. **Mag. Andreas KRISCH,** geb. [redacted]
   Consultant, Obmann Arbeitskreis Vorratsdatenspeicherung
   [redacted]
3. **Mag. Albert STEINHAUSER,** [redacted]
   Nationalratsabgeordneter, Justizsprecher der „Grünen"
   [redacted]
4. **Jana HERWIG, MA,** [redacted] Medienwissenschafterin,
   [redacted]
5. **Sigrid MAURER,** [redacted] Nationalratsabgeordnete
   [redacted]
6. **Mag. DDr. Erich SCHWEIGHOFER,** [redacted]
   Ao. Univ. Prof. Universität Wien,
   Leiter der Arbeitsgruppe Rechtsinformatik,
   [redacted]
7. **Dr. Hannes TRETTER,** [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,** [redacted] Richterin,
[redacted]
10. **Philipp SCHMUCK,** [redacted] Student,
[redacted]
11. **Dr. Stefan PROCHASKA,** [redacted] Rechtsanwalt
Vizepräsident der Rechtsanwaltskammer Wien
Geschäftsführer PHH Rechtsanwälte GmbH
1010 Wien, Julius-Raab Platz 4

12. **bis 11.130. Antragsteller/in gemäß vorgelegter CD**

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

(Vollmachten gem. § 8 RAO erteilt)

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

wegen: §§ 102a, 102b, 102c, 99, 92 – 94, 98, 109 TKG 2003,
§ 76a Abs 2 StPO, § 53 Abs 3a, 3b SPG

Äußerung
zum Urteil der Großen Kammer
des Gerichtshofes der Europäischen Union vom 08.04.2014

1-fach
1 Anlage (einfach)

In umseits bezeichneter Rechtssache übermittelte der Verfassungsgerichtshof mit Schreiben vom 09.04.2014, den Antragstellerinnen und Antragstellern zugestellt am 11.04.2014, das Urteil der Großen Kammer des Gerichtshofes der Europäischen Union vom 08.04.2014 (nachfolgend kurz: „Urteil") zu den verbundenen Rechtssachen C-293/12 und C-594/12, verbunden mit der Aufforderung, innerhalb von vier Wochen hierzu eine Äußerung zu erstatten.

In Entsprechung dieser Aufforderung ergeht durch die Antragstellerinnen und Antragstellern sohin binnen offener Frist nachstehende

ÄUßERUNG:

1. Rechtslage nach der Aufhebung der Richtlinie

Nach der Aufhebung der Richtlinie 2006/24/EG durch das Urteil ist aus Sicht der Antragsteller/innen als entscheidende Vorfrage zunächst zu klären, ob und wie weit ein Spielraum für eine Vorratsdatenspeicherung („VDS") auf rein nationaler Ebene verbleibt.

Zunächst bewirkt die Aufhebung der Richtlinie 2006/24/EG auch den Wegfall der mit dieser RL bewirkten Änderung der „Datenschutz-Richtlinie für elektronische Kommunikationsdienste" 2002/58/EG.[1] Das bedeutet, dass das Gebot gemäß Art 6 Abs 1 RL 2002/58/EG auch für die in § 102a TKG aufgezählten Datenkategorien (wieder) gilt, wonach Verkehrsdaten *„zu löschen oder zu anonymisieren [sind], sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden"*. Allerdings normiert Art 15 Abs 1 RL 2002/58/EG ausdrücklich den Spielraum der Mitgliedstaaten, von dieser Löschungsverpflichtung ua für Zwecke der nationalen Sicherheit sowie der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten gesetzliche Ausnahmen vorzusehen und eine Speicherung von Verkehrsdaten für die genannten Zwecke für eine begrenzte Zeit vorzuschreiben.

Auch eine solche nationale Vorratsdatenspeicherung muss nach Art 15 Abs 1 letzter Satz RL 2002/58/EG den *„in Artikel 6 Absätze 1 und 2 des Vertrags über die Europäische Union niedergelegten Grundsätzen"* entsprechen. Zu diesen Grundsätzen zählen seit dem Inkrafttreten des Vertrags von Lissabon insbesondere die EU Grundrechtecharta und deren Auslegung durch den EuGH. Die durch den EuGH im Urteil 08.04.2014 aufgestellten Determinanten wirken daher auch auf eine nationale VDS, gestützt auf die Ausnahme des Art 15 Abs 1 RL 2002/58/EG, zurück. Die Gestaltung der Regelung des Art 15 Abs 1 RL 2002/58/EG als materielle Determinierung eines Spielraums für Regelungen durch die Mitgliedsstaaten zeigt außerdem auch ohne den Verweis auf

[1] Im Detail ist die Gestaltung sehr verschachtelt, weil durch RL 2006/24/EG ein Abs 1a) in Art 15 RL 2002/58/EG eingefügt wurde, der die Ausnahme des Art 15 Abs 1 2002/58/EG in Bezug auf Daten, die der Vorratsdatenspeicherung nach der RL 2006/24/EG unterliegen, für unanwendbar erklärt.

Art 6 EUV, dass eine rein nationale VDS im Anwendungsbereich des Unionsrechts liegt[2] und daher die im Primärrecht verankerte EU Grundrechtecharta und ihre Interpretation durch den EuGH zu beachten ist.

In der Entscheidung vom 14.03.2012 zu U 466/11 ua. hat der Verfassungsgerichtshof entschieden, dass er im Anwendungsbereich des Unionsrechts die von der EU Grundrechtecharta garantierten Rechte äquivalent zu den verfassungsgesetzlich gewährleistete Rechte iSd Art 144 bzw. Art 144a B-VG sieht, die daher einen Prüfungsmaßstab in Verfahren der generellen Normenkontrolle nach Art 139 und Art 140 B-VG darstellen. Daraus folgt, dass jedenfalls jene im Rahmen der Individualanträge relevierten Normen durch den Verfassungsgerichtshof als verfassungswidrig aufzuheben sind, die mit Anforderungen aus dem EuGH Urteil zum Vorabentscheidungsverfahren unvereinbar sind. Darüber hinaus liegt es (nunmehr) im nationalen Ermessen des Verfassungsgerichtshofes, durchaus einen Maßstab zu setzen, der im Vergleich zu den Unionsgrundrechten einen günstigeren Grundrechtsschutz bewirkt. Dem steht nach der Aufhebung der Richtlinie 2006/24/EG auch kein Anwendungsvorrang des Unionsrechts entgegen, weil es nunmehr kein Gebot für eine Vorratsdatenspeicherung im Unionsrecht gibt.

2. Materielle Determinanten aus dem EuGH Urteil

Nach Auffassung der Antragsteller/innen gebietet das Urteil eine Aufhebung des §102a TKG, welcher die Vorratsspeicherung vorschreibt und daher die zentrale Norm zur österreichischen Umsetzung der Vorratsdatenspeicherung bildet. Im Falle der Aufhebung dieser Norm durch den Verfassungsgerichtshof sind auch alle Normen aufzuheben, die Aufgrund formeller oder materieller Verweisungen in untrennbarem Zusammenhang stehen oder sonst keinen Sinn mehr ergeben würden. Die entsprechenden Zusammenhänge haben die Antragsteller/innen im verfahrenseinleitenden Schriftsatz (Kapitel III, Seite 12 ff) detailliert dargestellt und im Rahmen der Anträge (Kapitel VI.1., Seite 45 f) formal berücksichtigt.

Im Hinblick auf die einleitende Darstellung ist theoretisch denkbar, dass die im Urteil festgestellten Mängel der nun aufgehobenen Richtlinie im Zuge der innerstaatlichen Umsetzung auf nationaler Ebene „repariert" wurden. Nachfolgend werden daher spezifische Aspekte aus dem Urteil hervorgehoben, die nach Auffassung der Antragsteller/innen zeigen, dass auch die österreichische Umsetzung der VDS die Grundrechtsverletzungen durch die aufgehobene Richtlinie nicht kompensiert. Ganz allgemein ist vorwegzuschicken: Auch die tendenziell eher zurückhaltende Umsetzung der Richtlinie 2006/24/EG in Österreich erfolgte innerhalb der Determinanten dieser Richtlinie. Da die Richtlinie in vielen verschiedenen Aspekten als

---

[2] Vgl. EuGH 18.06.1991, Rs. C-260/89, ERT. Aus EuGH 26.02.2013, Rs. C-617/10, Fransson ergibt sich, dass die ERT-Judikatur auch für die Frage gilt, wann eine Grundrechtsbeschränkung in „Durchführung des Unionsrechts" stattfindet.

unverhältnismäßig erkannt wurde, ist indiziert, dass jede Umsetzung innerhalb dieser Determinanten ebenso überschießend und damit grundrechtswidrig ist.

a.) Zur Zulässigkeit

Der EuGH stellt fest, *„dass die den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste und den Betreibern eines öffentlichen Kommunikationsnetzes durch die Art. 3 und 6 der Richtlinie 2006/24 auferlegte Pflicht, die in Art. 5 dieser Richtlinie aufgeführten Daten über das Privatleben einer Person und ihre Kommunikationsvorgänge während eines bestimmten Zeitraums auf Vorrat zu speichern, als solche einen Eingriff in die durch Art. 7 der Charta garantierten Rechte darstellt“* [3]. In der Folge differenziert der EuGH zwischen der Speicherung der Verkehrsdaten und dem Zugang nationaler Behörden zu den Daten und bezeichnet letzteres als *„zusätzlichen Eingriff in dieses Grundrecht“*[4]. In derselben Weise (*„desgleichen“*) bewirke die Richtlinie einen Eingriff in das Datenschutzgrundrecht gemäß Art 8 EU Grundrechtecharta[5].

Diese Differenzierung ist im Hinblick auf die (bisher nur vorläufig angenommene) Zulässigkeit des gegenständlichen Individualantrags gemäß Art 140 B-VG von Bedeutung. Damit wird nämlich die Argumentation der Antragsteller/innen zur Zulässigkeit (Verfahrenseinleitender Schriftsatz Kapitel IV, Seite 22 ff) der Anträge gestützt, wonach die unmittelbare und aktuelle rechtliche Betroffenheit schon aus der Speicherung der Daten resultiert und ein allfälliger Zugriff durch berechtigte Behörden einen weiteren, zusätzlichen Grundrechtseingriff darstellt.

b.) Erforderlichkeit und Verhältnismäßigkeit

Das Urteil formuliert als zentrale Kritik, *„dass sich die Richtlinie 2006/24 generell auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstreckt, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des Ziels der Bekämpfung schwerer Straftaten vorzusehen*[6]*. Die Richtlinie 2006/24 betrifft nämlich zum einen in umfassender Weise alle Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich jedoch die Personen, deren Daten auf Vorrat gespeichert werden, auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte*[7]*.“* Weiters kritisiert der EuGH, dass die *„Vorratsspeicherung weder auf die Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat*

---

[3] Urteil Rn 34

[4] Urteil Rn 35

[5] Urteil Rn 36

[6] Urteil Rn 57.

[7] Urteil Rn 58.

gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten"[8], eingeschränkt ist.

Dieses Problem liegt im Wesen der durch die Richtlinie normierten Vorratsdatenspeicherung und konnte schon deshalb im Zuge der innerstaatlichen Umsetzung nicht beseitigt werden, weil ansonsten wohl das Vertragsverletzungsverfahren gegen Österreich wegen mangelnder Umsetzung der Richtlinie fortgeführt worden wäre. Aus den oben zitierten Ausführungen des EuGH geht hervor, dass das bisherige Konzept einer anlasslosen, verdachtsunabhängigen und flächendeckenden Speicherung mit Art 7 und 8 EU Grundrechtecharta nicht vereinbar ist.

Besonders schwer wiegt dabei das in Rn 58 des Urteils angesprochene Problem der besonders schutzwürdigen Kommunikation von Berufsgeheimnisträgern, welches daher gesondert in Punkt 3. dieser Stellungnahme behandelt wird.

Zum Zugang nationaler Behörden zu den gespeicherten Daten kritisiert der EuGH, zusätzlich *„zu diesem generellen Fehlen von Einschränkungen", „...dass die Richtlinie 2006/24 kein objektives Kriterium vorsieht, das es ermöglicht, den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung zwecks Verhütung, Feststellung oder strafrechtlicher Verfolgung auf Straftaten zu beschränken, die im Hinblick auf das Ausmaß und die Schwere des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte als hinreichend schwer angesehen werden können, um einen solchen Eingriff zu rechtfertigen. Die Richtlinie 2006/24 nimmt im Gegenteil in ihrem Art. 1 Abs. 1 lediglich allgemein auf die von jedem Mitgliedstaat in seinem nationalen Recht bestimmten schweren Straftaten Bezug.*"[9]

Zu diesem Kritikpunkt ist zunächst festzuhalten, dass hier die österreichische Umsetzung durchaus eine Entschärfung des Problems bewirkt, gelöst wird es jedoch nicht vollständig. Einerseits ist nämlich in Zweifel zu ziehen, nach der Grundregel des § 135 Abs 2a StPO, wonach die Daten nur zur Aufklärung von Straftaten mit mehr als einem Jahr Freiheitsstrafdrohung verfügbar sind, die aufzuklärenden Straftaten tatsächlich als *„hinreichend schwer"* angesehen werden können, um einen derart schwerwiegenden Grundrechtseingriff zu rechtfertigen. In dieser Hinsicht zeigten bereits die bei der mündlichen Verhandlung vor dem EuGH seitens der Republik Österreich referierten statistischen Daten zur Auskunftspraxis, dass die tatsächlich Zwecke von den propagierten Zielen der Bekämpfung von Terrorismus und organisierter Kriminalität weit weg sind. Demzufolge gab es nämlich in Österreich für den Zeitraum vom 01.04.2012 bis zum 31.03.2013 (also nach einem Jahr Vorratsdatenspeicherung in Österreich) insgesamt 326 Anfragen und in 312 Fällen auch die Auskünfte dazu.

---

[8] Urteil Rn 59 letzter Satz

[9] Urteil Rn 60

Bei 161 erledigten Rechtssachen soll in 71 Fällen die Vorratsdatenspeicherung einen Beitrag zur Aufklärung geleistet haben. Die meisten Abfragen von Vorratsdaten waren dabei nicht auf schwerste Verbrechen, wie Terrorismus oder Mord gerichtet, sondern betrafen Diebstahl (106) oder Stalking.

Bei den mithilfe von Vorratsdaten aufgeklärten Fällen betrafen 16 Fälle Diebstahl, 12 Suchtmitteldelikte, 12 Stalking, 7 Betrug und 7 Raub. Der Rest waren sonstige Delikte.

Bei der mündlichen Verhandlung vor dem EuGH konnte der Vertreter der österreichischen Bundesregierung auf Nachfrage des Gerichtshofs nicht beantworten, ob darunter Fälle schwerer Kriminalität zu finden seien, die Angaben indizieren dies jedenfalls nicht.

Im Hinblick auf eben jene Zugriffsbefugnisse nach § 76a Abs 2 StPO sowie § 53 Abs 3a SPG ist auch für die nationale Umsetzung die Kritik des EuGH gültig, dass „*der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung den Zugang zu den Daten und ihre Nutzung auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken soll und im Anschluss an einen mit Gründen versehenen Antrag der genannten Behörden im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten ergeht*“[10], unterliegt.

Zur Speicherdauer ist festzuhalten, dass auch (die in Österreich festgesetzten) 6 Monate überschießend sind. Wie der EuGH in seinem Urteil zutreffend feststellt, „*… (sind) die Daten für einen Zeitraum von mindestens sechs Monaten auf Vorrat zu speichern (…), ohne dass eine Unterscheidung zwischen den in Art. 5 der Richtlinie genannten Datenkategorien nach Maßgabe ihres etwaigen Nutzens für das verfolgte Ziel oder anhand der betroffenen Personen getroffen wird. Die Speicherfrist liegt zudem wischen mindestens sechs Monaten und höchstens 24 Monaten, ohne dass ihre Festlegung auf objektiven Kriterien beruhen muss, die gewährleisten, dass sie auf das absolut Notwendige beschränkt wird.*“[11] Damit verlässt auch die österreichische Regelung der Speicherdauer von sechs Monaten den Boden einer juristisch (im Sinne von: grundrechtlich) darstellbaren Argumentation (jenseits des Faktums, dass es sich halt um die kürzeste Zeit der Vorgabe gemäß Richtlinie handelt) und rückt bedenklich in die Nähe einer „Glaubensfrage“. Denn ein Argument, wieso sechs Monate zweckentsprechend sind, lässt sich auch den Materialien im österreichischen Umsetzungsprozess nicht entnehmen.

c.) Datensicherheit

Zur Datensicherheit wird seitens der Antragsteller/innen zwar eingeräumt, dass die österreichische Umsetzung eines Datensicherheitskonzepts insbesondere durch die Datensicherheitsverordnung gemäß §§ 94 und 102c TKG (DSVO) ein an sich vorbildliches Datensicherheitskonzept normiert und damit wohl den hierzu aufgestellten Anforderungen des

---

[10] Urteil Rn 62 letzter Satz

[11] Urteil Rn 63 f

EuGH[12] vermutlich weitgehend entspricht. Allerdings fehlt es auch in Österreich an einer Einschränkung, die aufgrund der Richtlinie schlichtweg nicht absehbar war: Es gibt kein Verbot gegenüber den Anbietern iSd TKG, Vorratsdaten außerhalb des Gebiets der Europäischen Union zu speichern[13]. Schon allein aus diesem Mangel ergibt sich, dass die Speicherpflicht nach § 102a TKG aufzuheben ist, weil eine für viele Anbieter wohl tiefgreifende Verpflichtung nicht einfach durch ergänzende Interpretation des § 102c TKG ohne Deckung in dessen Wortlaut gelöst werden darf, ohne das verfassungsrechtliche Bestimmtheitsgebot zu verletzen.

Der Vollständigkeit halber sei angemerkt, dass die Datensicherheitsverordnung ausdrücklich in vielen Regelungsaspekten auch auf „Betriebsdaten" anwendbar ist und daher auch nach einer allfälligen Aufhebung der österreichischen Vorratsdatenspeicherung einen äußerst wichtigen Anwendungsbereich findet.

3. Zum Sonderproblem „Schutz von Berufsgeheimnissen"

Völlig richtig spricht der EuGH das Dilemma der Berufsgeheimnisse in der Vorratsdatenspeicherung an.[14] Dieses Problem war den in Österreich für die Umsetzung der VDS Richtlinie zuständigen Behörden spätestens nach dem Urteil des deutschen Bundesverfassungsgerichts zu BVerfG, 1 BvR 256/08 vom 2.3.2010 bewusst. Das Bundesverfassungsgericht hatte nämlich die Aufhebung der deutschen Umsetzung der Richtlinie 2006/24 unter anderem auch damit begründet, dass eine Ausnahme bei der Erfassung von Kommunikationsvorgängen von Berufsgeheimnisträgern fehle.

Das in Österreich für die Umsetzung primär verantwortliche Bundesministerium für Verkehr, Innovation und Technologie (BMVIT) nahm die Vorgaben des deutschen Bundesverfassungsgerichts sehr ernst und schrieb am 1. April 2010 eine Einladung für einen Stakeholder-Roundtable aus, um das Problem noch im Zuge der laufenden Umsetzung der Richtlinie zu diskutieren. Eingeladen waren: Anwaltskammer, Ärztekammer, Journalistenverbände, Notariatskammer, Arbeiterkammer, Wirtschaftskammer, Internet-Serviceprovider Verband (ISPA), European Digital Rights (EDRi) sowie das Ludwig Boltzmann Institut für Menschenrechte (BIM).[15] Daraufhin fanden am 15. April, am 18. Mai und am 25. Juni 2010 insgesamt drei Round Table Diskussionen zu diesem Thema statt. Der Erstbeschwerdeführer im gegenständlichen Verfahren und Co-Autor dieser Stellungnahme,

---

[12] Urteil Rn 66 ff

[13] dazu Urteil Rn 68

[14] Urteil Rn 58

[15] Zur ausführlicheren Dokumentation des gesamten Prozesses einschließlich der insgesamt 3 Roundtables der „Berufsgeheimnisträger" siehe Tschohl, Datensicherheit TKG Novelle 2010, Studie des Ludwig Boltzmann Institut für Menschenrechte zur Datensicherheit in der TKG Novelle zur Umsetzung der Vorratsdatenspeicherung in Österreich, Seite 75 f; online unter http://bim.lbg.ac.at/files/sites/bim/BIM%20Studie%20Datensicherheit%20TKG%20Novelle%202010_final_online-Publikation.pdf (09.05.2014).

Christof Tschohl, war bei sämtlichen Stakeholder Diskussionen als Vertreter des BIM aktiv eingebunden.

In der Sache wurde diskutiert, warum von Seiten des BIM solche Ausnahmen nicht schon im Ursprünglichen BIM Entwurf zur TKG Novelle enthalten waren und dass hierzu mit Vertretern der Zivilgesellschaft schon früher diskutiert wurde. Dabei ging es primär darum, dass Ausnahmen für Berufsgeheimnisträger schon bei der Speicherung rein technisch vor dem Problem stehen, dass jeder speicherpflichtige Dienstanbieter nicht nur von seinen eigenen Kunden, sondern von sämtlichen Kommunikationsteilnehmern wissen müsste, ob einer der Kommunikationsteilnehmer einem gesetzlich geschützten Berufsgeheimnis unterliegt.

Die einzige Lösungsmöglichkeit wäre eine Art zentrale Filterliste, in der Diskussion „Whitelist" genannt, als notwendige Voraussetzung, um Ausnahmen entweder bei der Speicherung oder zumindest bei der Übermittlung von Verkehrsdaten/Vorratsdaten theoretisch zu ermöglichen. Gleichzeitig wurde festgestellt, dass eine Implementierung der Ausnahme schon bei der Speicherung nur mit einem enormen technischen und administrativen Aufwand verbunden wäre. In diesem Fall müsste die „Whitelist" als Filter nämlich bei jedem einzelnen Anbieter implementiert sein, zugleich aber bundesweit einheitlich, aktuell und in Echtzeit auf Stand gehalten werden.

Angesichts dieser Schwierigkeiten wurde der Vorschlag einer „Clearing-Stelle" als zentrale Plattform zur Übermittlung von Datenauskünften an Sicherheitsbehörden diskutiert. Die Idee war, eine „Whitelist" als eine Art „Filter" zu implementieren, wobei im Ergebnis einer Auskunft ein automatisches „schwärzen" einer „geschützten Person" innerhalb eines Auskunft-Datensatzes realisiert werden könnte. In diesem Zusammenhang wurde zugleich aber festgehalten, dass schon nach derzeitiger Rechtslage eine „Beharrungsmöglichkeit" der Gerichte besteht, wenn Geheimnisträger selbst dringend verdächtig sind, eine Straftat begangen zu haben, die abstrakt eine Auskunft rechtfertigt. Allerdings bedarf eine Auskunft dann, wenn die Gefahr besteht, dass ein Entschlagungsrecht gemäß § 157 Abs. 1 Z 2 bis 4 StPO umgangen werden könnte, gemäß § 144 Abs 3 StPO einer Genehmigung des Rechtsschutzbeauftragten der Justiz.

Für den Fall einer Umgehung des Beweiserhebungsverbots ordnet § 157 Abs 2 StPO die Folge der Nichtigkeit des Verfahrens an (Beweisverwertungsverbot), wobei es sich um einen relativen Nichtigkeitsgrund handelt. Seitens des BIM wurde vor allem darauf hingewiesen, dass dieses Problem – im Hinblick auf die Abfrage betrieblich gespeicherter Daten („Betriebsdaten") – nicht neu sei, durch die Vorratsdatenspeicherung aber potenziert werde.

Der wesentlichste Punkt in der gesamten Debatte ist jedoch die datenschutzrechtliche Einschätzung der „Whitelist" selbst. Eine Liste mit Namen, Anschrift und Teilnehmernummer zu jedem Anschluss von Menschen, die einem gesetzlich geschützten Berufsgeheimnis unterliegen[16], ist datenschutzrechtlich fast schon so bedenklich wie die Vorratsdatenspeicherung selbst. Dazu käme das Problem, dass zur Erstellung dieser List wohl eine Art „opt-in" Verfahren

[16] Auch wenn dieser Kreis weiter ist als jener der Entschlagungsberechtigten gemäß § 157 StPO.

zu finden wäre. Betroffene müssten sich entscheiden, ob sie sich lieber dem datenschutz-Risiko der „Whitelist" oder der Vorratsdatenspeicherung aussetzen würden.

Insgesamt war daher die einhellige Meinung im Kreis der Diskutierenden, dass eine solche Filterliste keinesfalls den Interessen des Datenschutzes förderlich wäre.

Als einzige konkrete Konsequenz der ausführlichen Diskussionen blieb daher schließlich die Zusage von Seiten des BMVIT übrig, den Gesetzesentwurf um eine Schutzbestimmung zu erweitern: Dem Kommunikationsgeheimnis sollte ein ausdrückliches Umgehungsverbot hinzugefügt werden, was mit der Einführung eines neuen Absatz 5 in § 93 TKG schließlich auch erfolgte: *„(5) Das Redaktionsgeheimnis (§ 31 Mediengesetz) sowie sonstige, in anderen Bundesgesetzen normierte Geheimhaltungsverpflichtungen sind nach Maßgabe des Schutzes der geistlichen Amtsverschwiegenheit und von Berufsgeheimnissen sowie das Verbot deren Umgehung gemäß §§ 144 und 157 Abs. 2 StPO zu beachten. Den Anbieter trifft keine entsprechende Prüfpflicht."*

Mit der Widergabe der Diskussionen zum Problem der Berufsgeheimnisträger bei Umsetzung der Vorratsdatenspeicherung soll hier gezeigt werden, dass der EuGH damit wie schon zuvor das deutsche Bundesverfassungsgericht ein Dilemma anspricht, welches im Rahmen des Konzepts einer anlasslosen und Flächendeckenden Datenspeicherung nicht zufriedenstellend aufgelöst werden kann. Die einzige Möglichkeit, den Grundrechtsschutz in dieser speziellen Hinsicht zu wahren, ist die Aufhebung der generellen Speicherverpflichtung nach § 102a TKG.

4. Eine Art „politische Zusammenfassung":

Der EuGH führte in seinem Urteil aus[17]:

„Zur Erforderlichkeit der durch die Richtlinie 2006/24 vorgeschriebene Vorratsspeicherung der Daten ist festzustellen, dass zwar die Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, von größter Bedeutung für die Gewährleistung der öffentlichen Sicherheit ist und dass ihre Wirksamkeit in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen kann. Eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer Speicherungsmaßnahme – wie sie die Richtlinie 2006/24 vorsieht – für die Kriminalitätsbekämpfung nicht rechtfertigen."

Der EuGH erkannte auch, dass die Vorratsdatenspeicherung *„... (...) zu einem Eingriff in die Grundrechte fast der gesamten europäischen Bevölkerung (führt)"*[18].

---

[17] Urteil Rn 51

[18] Urteil Rn 56

Der EuGH schreckte aber offensichtlich vor den zwingenden Konsequenzen seiner eigenen (grundrechtsfreundlichen) Logik zurück. Um diesen Konsequenzen zu entgehen, musste der nicht definierte, letztlich ohne Offenlegung des zugrundeliegenden Menschenbildes gar nicht definierbare „Wesensgehalt" von Grundrechten herhalten[19]:

„Zum Wesensgehalt des Grundrechts auf Achtung des Privatlebens und der übrigen in Art. 7 der Charta verankerten Rechte ist festzustellen, dass die nach der Richtlinie 2006/24 vorgeschriebene Vorratsdatenspeicherung von Daten zwar einen besonders schwerwiegenden Eingriff in diese Rechte darstellt, doch nicht geeignet ist, ihren Wesensgehalt anzutasten, da die Richtlinie, wie sich aus ihrem Art.1 Abs 2 ergibt, die Kenntnisnahme des Inhalts elektronischer Kommunikation als solchen nicht gestattet.

„Die Vorratsdatenspeicherung ist auch nicht geeignet, den Wesensgehalt des in Art. 8 der Charta verankerten Grundrechts auf den Schutz personenbezogener Daten anzutasten…." (usw., usf.).

Wenn die Vorratsdatenspeicherung *„… (…) zu einem Eingriff in die Grundrechte fast der gesamten europäischen Bevölkerung (führt)"*, dann sollten und müssten ebendiese Menschen – die Souveräne jenes (letztlich ebenfalls undefinierbaren) *„Gemeinwohls"* (ein Begriff mit einer zweifelhaften politischen Karriere), das ständig als Rechtfertigung für jede Ausweitung staatlicher Machtbefugnisse herhalten muss – entscheiden, ob sie diesen Eingriff erlauben, ob sie bereit sind, den Preis für die versprochene „Sicherheit" zu bezahlen, ob sie zustimmen, dass der *„Wesensgehalt"* ihrer unveräußerlichen Rechte durch maßlose Eingriffe wie die Vorratsdatenspeicherung *„angetastet"* wird. Denn es handelt sich immerhin – wie vom EuGH selbst ausgeführt – um *„…. die Grundrechte fast der gesamten europäischen Bevölkerung"*.

Wie bereits in den Individualanträgen vom 15.06.2012 ausgeführt wurde, stellen die im hier gegenständlichen Verfahren relevierten Bestimmungen des TKG, der StPO und des SPG, die in Umsetzung der (aufgehobenen) Richtlinie 2006/24/EG geschaffen wurden, für die Antragsteller/innen einen Dammbruch dar, eine Art Quantensprung in den „Überwachungsstaat". Es sei wiederholt: Setzen sich diese Prinzipien durch und fort, ist die auf der Vorstellung von persönlicher Freiheit der Menschen basierende Ordnung westlicher Demokratien am Ende – ungeachtet, wie das Staatswesen formal organisiert und verwaltet wird. Die Vorratsdatenspeicherung ist der Einstieg in den „permanenten Ausnahmezustand".

Zur Verletzung der Privatsphäre durch die „Vorratsdatenspeicherung" hat der EuGH bereits seine Rechtsansicht geäußert, zu Art 11 GRC – zur Meinungsfreiheit – wurde hingegen nur ausgeführt, dass ein Eingriff in den Schutzbereich vorliegt, ohne weitere Beurteilung, ob dieser Eingriff gerechtfertigt ist. Da die Antragsteller/innen aber die Meinung vertreten, dass durch die „Vorratsdatenspeicherung" aus den bereits vorgetragenen Gründen insbesondere auch die Meinungs- und Medienfreiheit einer nachhaltigen Erosion ausgesetzt wird, fordern sie den Verfassungsgerichtshof ausdrücklich auf, in der Begründung der – nach ihrer Meinung

---

[19] Urteil Rn 39f

unausweichlichen – Aufhebung der angefochtenen Bestimmungen klare Worte zum Wert und zur Bedeutung des Grundrechts auf Meinungs- und Medienfreiheit für das Gemeinwohl und eine Gemeinschaft freier Menschen zu finden.

5. Anträge

Aus den oben angeführten Gründen sowie unter Hinweis auf das bisherige Vorbringen (auch in der Stellungnahme im Vorabentscheidungsverfahren gemäß Art. 267 AEUV) halten die Antragsteller/innen die **Anträge vom 15.06.2012 in der Fassung des Schriftsatzes vom 20.06.2012** vollinhaltlich aufrecht.

6. Kosten

Abschließend modifizieren die Antragsteller/innen ihren Antrag auf Kostenzuspruch aus dem Schriftsatz vom 15.06.2012.

Die Antragsteller/innen legen als Anlage ./2 vor ein Kostenverzeichnis auf nachstehender Grundlage bzw. Kriterien:

a.) Für den verfahrenseinleitenden Schriftsatz vom 15.06.2012 (welcher von den Antragsteller/innen als Einheit mit jenen vom 20.06.2012, 05.07.2012 und 08.10.2012 als Einheit bewertet wird) steht ein Pauschalsatz (Grundbetrag) von EUR 2.180,00 zuzüglich 50% Streitgenossenzuschlag (für 11.129 Antragsteller/innen, gedeckelt gemäß § 15 RATG), zuzüglich 20 % USt zuzüglich Eingabengebühren gemäß § 17a Z 1 VfGG in Höhe von EUR 240,00.

b.) Für vom VfGH abverlangte (oder nicht abverlangte) Schriftsätze und für die Teilnahme an Verhandlungen in von Amts wegen eingeleiteten Normprüfungsverfahren und in Zwischenverfahren findet kein weiterer Kostenzuspruch statt.

c.) Im gegenständlichen Fall wurde das Normprüfungsverfahren auf Antrag eingeleitet, wodurch vom VfGH abverlangte (oder nicht abverlangte) Schriftsätze und die Teilnahme an Verhandlungen einem Kostenersatz zugänglich sind.

d.) Der EuGH führt in seinem Urteil aus, dass für die Parteien der Ausgangsverfahren (auch jenem vor dem VfGH) das Verfahren vor dem EuGH einen Zwischenstreit in den Verfahren vor jenen Gerichten darstelle, die Kostenentscheidung daher Sache des VfGH sei.[20]

---

[20] Urteil Rn 73

e.) Da sich dem VfGG keine Bemessungsgrundlage für das hier gegenständliche Verfahren findet, nehmen die Antragsteller/innen Bezug die „Allgemeinen Honorar-Kriterien (AHK 2005) für Rechtsanwälte"; deren § 5 zufolge können als Bemessungsgrundlage für Honoraransätze, soweit sich nicht auf Grund des Interesse des Auftraggebers oder aus der Sache selbst ein anderer Wert ergibt, definierte Beträge als angemessen betrachtet werden.

f.) Für Verwaltungssachen von weitreichender Bedeutung (§ 5 Z 34 c AHK) gilt eine Bemessungsgrundlage von EUR 21.800,00 als angemessen, für gewerblichen Rechtsschutz (§ 5 Z 14 AHK) EUR 36.000,00, für Urheber- und Verlagsrechtssachen (§ 5 Z 29 AHK) ebenfalls EUR 36.000,00, für Kartellsachen (§ 5 Z 18 b AHK) EUR 145.000,00, für Bausachen bei Großprojekten (§ 5 Z 4 lit c AHK) und Gewerbesachen für Großbetriebe (§ 5 Z 13 lit d AHK) jeweils EUR 181.000,00.

g.) Da das hier gegenständliche Verfahren die Grundrechte von zumindest 8 Millionen Menschen in Österreich betrifft und über das im Sinne der Antragsteller/innen erfolgreiche Zwischenverfahren vor dem EuGH indirekt die Grundrechtsinteressen von ca. 350 Millionen Menschen von den Prozessanstrengungen der Antragsteller/innen berührt sind, erscheint „aus der Sache selbst" eine Bemessungsgrundlage von EUR 543.000,00 (sohin der dreifachen Bemessungsgrundlage etwa einer Gewerbesache eines Großbetriebes) angemessen.

h.) Gemäß § 8 Abs 1 AHK können für die Vertretung vor übernationalen Tribunalen (wie dem EuGH) und dem Verfassungsgerichtshof für Beschwerden, Gegenschriften und die Verrichtung von mündlichen Verhandlungen der doppelte Betrag der TP 3C RATG als angemessen betrachtet werden.

Aus der Anwendung der oben skizzierten Kriterien ergibt sich der beantragte Kostenersatz.

Sollte eine der Verfassungsgerichtshof eine mündliche Verhandlung anberaumen, wird ein ergänztes, aktualisiertes Kostenverzeichnis vor Schluss der mündlichen Verhandlung vorgelegt werden.

Wien, am 09. Mai 2014 für die Antragstellerinnen und Antragsteller