

# TE Vwgh Erkenntnis 2013/4/24 2011/17/0293

JUSLINE Entscheidung

🕒 Veröffentlicht am 24.04.2013

## Index

E000 EU- Recht allgemein;  
E3L E13206000;  
E3L E13309900;  
E3L E15201000;  
E3L E16200000;  
E3L E19400000;  
10/07 Verwaltungsgerichtshof;  
10/10 Grundrechte;  
20/06 Konsumentenschutz;  
41/01 Sicherheitsrecht;

## Norm

31995L0046 Datenschutz-RL Art28 Abs1;  
31995L0046 Datenschutz-RL Art3 Abs2;  
32002L0058 Datenschutz-RL Art1 Abs3;  
ECG 2001 §18 Abs1;  
EURallg;  
SPG 1991 §53 Abs3a idF 2007/I/114;  
SPG 1991 §53 Abs3a Z2 idF 2007/I/114;  
StGG Art10a;  
VwGG §13 Abs1 Z1;  
VwGG §42 Abs2 Z2;  
1. StGG Art. 10a heute  
2. StGG Art. 10a gültig ab 01.01.1975 zuletzt geändert durch BGBl. Nr. 8/1974  
1. VwGG § 13 heute  
2. VwGG § 13 gültig ab 01.03.2013 zuletzt geändert durch BGBl. I Nr. 33/2013  
3. VwGG § 13 gültig von 22.07.1995 bis 28.02.2013 zuletzt geändert durch BGBl. Nr. 470/1995  
4. VwGG § 13 gültig von 05.01.1985 bis 21.07.1995  
1. VwGG § 42 heute  
2. VwGG § 42 gültig ab 01.01.2014 zuletzt geändert durch BGBl. I Nr. 33/2013  
3. VwGG § 42 gültig von 01.07.2012 bis 31.12.2013 zuletzt geändert durch BGBl. I Nr. 51/2012

4. VwGG § 42 gültig von 01.07.2008 bis 30.06.2012 zuletzt geändert durch BGBl. I Nr. 4/2008
5. VwGG § 42 gültig von 01.01.1991 bis 30.06.2008 zuletzt geändert durch BGBl. Nr. 330/1990
6. VwGG § 42 gültig von 05.01.1985 bis 31.12.1990

### **Betreff**

Der Verwaltungsgerichtshof hat durch den Vorsitzenden Senatspräsident Dr. Höfinger, die Hofräte Dr. Holeschofsky und Dr. Köhler sowie die Hofrätinnen Dr. Zehetner und Mag. Nussbaumer-Hinterauer als Richter, im Beisein der Schriftführerin Mag. Fries, über die Beschwerde des J A G in W, vertreten durch Dr. Helmut Graupner, Rechtsanwalt in 1130 Wien, Maxingstraße 22-24/4/9, gegen den Bescheid der Datenschutzkommission beim Bundeskanzleramt vom 20. Juli 2011, Zl. DSK-K121.697/0008-DSK/2011, betreffend Geheimhaltung schutzwürdiger personenbezogener Daten, zu Recht erkannt:

### **Spruch**

Die Beschwerde wird als unbegründet abgewiesen.

Der Beschwerdeführer hat dem Bund Aufwendungen in der Höhe von EUR 610,60 binnen zwei Wochen bei sonstiger Exekution zu ersetzen.

### **Begründung**

1.1. Unbestritten war der Beschwerdeführer mit seinem privaten PC am 11. November 2009 im Internet eingeloggt und nützte eine im angefochtenen Bescheid näher genannte IP-Adresse, die ihm von seinem Zugangsprovider zugewiesen worden war. Von 14.40 Uhr bis jedenfalls gegen 19.40 Uhr war er im Chatroom einer näher genannten Website eingeloggt. Dabei handelte es sich beim Inhaber der URL und Diensteanbieter um ein Unternehmen, das seinen Usern unter anderem Schreibforen und Chatrooms zur Vereinbarung sexueller Kontakte sowie zum Austausch einschlägiger Informationen und Phantasien zur Verfügung stellte. Im Chat erweckte der Beschwerdeführer, der dort unter einem Nickname als Frau auftrat, den Eindruck, er wäre bereit, sexuelle Handlungen mit Unmündigen, nämlich "mit 7 - 11jährigen, oder wenn gewünscht auch jünger" zu vermitteln, möglich wäre dies bereits am 14. November 2009. Von diesem Sachverhalt wurde das Landeskriminalamt Wien unter Bekanntgabe der Internetseite und des vom Beschwerdeführer verwendeten Nicknames offenbar von einem Kommunikationspartner im Chatroom informiert. Die befassten Beamten der Bundespolizeidirektion Wien gingen von einer konkret und unmittelbar drohenden Gefahr für die Sicherheit Unmündiger aus und ermittelten zunächst auf Grundlage des § 53 Abs. 3a Z. 2 SPG im Wege einer sogenannten "Whois-Abfrage" beim Domaininhaber die Website, sodann anhand dieser und des Nicknames über den technischen Betreiber des Chatserver die konkrete IP-Adresse des Endgerätes, von dem aus die Nachricht versendet wurde, samt Login-Zeitpunkt. Auf Grund dieser Daten konnte gemäß § 53 Abs. 3a Z. 3 SPG im Wege einer weiteren Abfrage der Provider, dem die IP-Adresse (innerhalb eines Adressenblocks) zugeordnet war, und über diesen schließlich Namen und Adresse des Beschwerdeführers (als Anschlussinhaber und Benutzer) ausgeforscht werden. Er und eine Reihe weiterer Personen wurden wegen des Verdachts der versuchten Bestimmung zum schweren sexuellen Missbrauch von Unmündigen sowie zur entgeltlichen Förderung fremder Unzucht bei der Staatsanwaltschaft Wien zur Anzeige gebracht.

1.1. Unbestritten war der Beschwerdeführer mit seinem privaten PC am 11. November 2009 im Internet eingeloggt und nützte eine im angefochtenen Bescheid näher genannte IP-Adresse, die ihm von seinem Zugangsprovider zugewiesen worden war. Von 14.40 Uhr bis jedenfalls gegen 19.40 Uhr war er im Chatroom einer näher genannten Website eingeloggt. Dabei handelte es sich beim Inhaber der URL und Diensteanbieter um ein Unternehmen, das seinen Usern unter anderem Schreibforen und Chatrooms zur Vereinbarung sexueller Kontakte sowie zum Austausch einschlägiger Informationen und Phantasien zur Verfügung stellte. Im Chat erweckte der Beschwerdeführer, der dort unter einem Nickname als Frau auftrat, den Eindruck, er wäre bereit, sexuelle Handlungen mit Unmündigen, nämlich "mit 7 - 11jährigen, oder wenn gewünscht auch jünger" zu vermitteln, möglich wäre dies bereits am 14. November 2009. Von diesem Sachverhalt wurde das Landeskriminalamt Wien unter Bekanntgabe der Internetseite und des vom Beschwerdeführer verwendeten Nicknames offenbar von einem Kommunikationspartner im Chatroom informiert. Die befassten Beamten der Bundespolizeidirektion Wien gingen von einer konkret und unmittelbar drohenden Gefahr für die Sicherheit Unmündiger aus und ermittelten zunächst auf Grundlage des Paragraph 53, Absatz 3 a, Ziffer 2, SPG im Wege einer sogenannten "Whois-Abfrage" beim Domaininhaber die Website, sodann anhand dieser und des Nicknames über den technischen Betreiber des Chatserver die konkrete IP-Adresse des Endgerätes, von dem aus die Nachricht versendet wurde, samt Login-Zeitpunkt. Auf Grund dieser Daten konnte

gemäß Paragraph 53, Absatz 3 a, Ziffer 3, SPG im Wege einer weiteren Abfrage der Provider, dem die IP-Adresse (innerhalb eines Adressenblocks) zugeordnet war, und über diesen schließlich Namen und Adresse des Beschwerdeführers (als Anschlussinhaber und Benutzer) ausgeforscht werden. Er und eine Reihe weiterer Personen wurden wegen des Verdachts der versuchten Bestimmung zum schweren sexuellen Missbrauch von Unmündigen sowie zur entgeltlichen Förderung fremder Unzucht bei der Staatsanwaltschaft Wien zur Anzeige gebracht.

1.2. Der Beschwerdeführer erhob in der Folge gegen die Bundespolizeidirektion Wien und gegen das Landespolizeikommando Wien bei der belangten Behörde Administrativbeschwerde unter anderem wegen Verletzung im Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten. In dieser rügte er vor allem die fehlende richterliche Bewilligung des seiner Ansicht nach vorliegenden Eingriffs in das gemäß Art. 10a StGG verfassungsgesetzlich geschützte Fernmeldegeheimnis; bei einem verfassungskonformen Verständnis des § 53 Abs. 3a Z. 2 SPG (bzw. unter Berücksichtigung des § 18 Abs. 1 E-Commerce-Gesetz) sei diese gerichtliche Bewilligung erforderlich. 1.2. Der Beschwerdeführer erhob in der Folge gegen die Bundespolizeidirektion Wien und gegen das Landespolizeikommando Wien bei der belangten Behörde Administrativbeschwerde unter anderem wegen Verletzung im Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten. In dieser rügte er vor allem die fehlende richterliche Bewilligung des seiner Ansicht nach vorliegenden Eingriffs in das gemäß Artikel 10 a, StGG verfassungsgesetzlich geschützte Fernmeldegeheimnis; bei einem verfassungskonformen Verständnis des Paragraph 53, Absatz 3 a, Ziffer 2, SPG (bzw. unter Berücksichtigung des Paragraph 18, Absatz eins, E-Commerce-Gesetz) sei diese gerichtliche Bewilligung erforderlich.

1.3. Die belangte Behörde wies mit dem vor dem Verwaltungsgerichtshof angefochtenen Bescheid - soweit für das Verfahren vor diesem noch von Bedeutung - die Administrativbeschwerde gegen die Bundespolizeidirektion Wien ab (Spruchpunkt 1). Begründend führte sie zusammengefasst aus, dass sämtliche Voraussetzungen zur Ausforschung der Daten im Sinne der nicht unter Richtervorbehalt stehenden Bestimmungen des § 53 Abs. 3a Z. 2 und 3 SPG vorgelegen seien: Das Verhalten des Beschwerdeführers habe eine Gefahrenlage im Sinne des § 21 Abs. 2 SPG befürchten lassen, bei den Auskunft erteilenden Unternehmen habe es sich um Diensteanbieter im Sinne des § 92 Abs. 3 Z. 1 Telekommunikationsgesetz 2003 (in der Folge: TKG) bzw. § 3 Abs. 2 E-Commerce-Gesetz gehandelt, der Eingriff sei auch verhältnismäßig gewesen. § 53 Abs. 3a SPG gehe dem (unter Richtervorbehalt stehenden) § 18 Abs. 2 E-Commerce-Gesetz zufolge § 18 Abs. 5 E-Commerce-Gesetz vor. Die Prüfung der angewendeten Vorschriften auf ihre Verfassungskonformität liege außerhalb der Befugnisse der belangten Behörde. 1.3. Die belangte Behörde wies mit dem vor dem Verwaltungsgerichtshof angefochtenen Bescheid - soweit für das Verfahren vor diesem noch von Bedeutung - die Administrativbeschwerde gegen die Bundespolizeidirektion Wien ab (Spruchpunkt 1). Begründend führte sie zusammengefasst aus, dass sämtliche Voraussetzungen zur Ausforschung der Daten im Sinne der nicht unter Richtervorbehalt stehenden Bestimmungen des Paragraph 53, Absatz 3 a, Ziffer 2, und 3 SPG vorgelegen seien: Das Verhalten des Beschwerdeführers habe eine Gefahrenlage im Sinne des Paragraph 21, Absatz 2, SPG befürchten lassen, bei den Auskunft erteilenden Unternehmen habe es sich um Diensteanbieter im Sinne des Paragraph 92, Absatz 3, Ziffer eins, Telekommunikationsgesetz 2003 (in der Folge: TKG) bzw. Paragraph 3, Absatz 2, E-Commerce-Gesetz gehandelt, der Eingriff sei auch verhältnismäßig gewesen. Paragraph 53, Absatz 3 a, SPG gehe dem (unter Richtervorbehalt stehenden) Paragraph 18, Absatz 2, E-Commerce-Gesetz zufolge Paragraph 18, Absatz 5, E-Commerce-Gesetz vor. Die Prüfung der angewendeten Vorschriften auf ihre Verfassungskonformität liege außerhalb der Befugnisse der belangten Behörde.

1.4. Der Beschwerdeführer bekämpft diesen Bescheid vor dem Verwaltungsgerichtshof wegen Rechtswidrigkeit seines Inhaltes sowie wegen Rechtswidrigkeit infolge Verletzung von Verfahrensvorschriften, führt den zuletzt genannten Beschwerdegrund jedoch nicht näher aus.

Die belangte Behörde hat die Akten des Verwaltungsverfahrens vorgelegt und eine Gegenschrift mit dem Antrag erstattet, die Beschwerde als unbegründet kostenpflichtig abzuweisen.

2.0. Der Verwaltungsgerichtshof hat erwogen:

2.1. Noch vor Eingehen auf das konkrete Vorbringen des Beschwerdeführers im hier zu beurteilenden Fall ist im Hinblick auf das Urteil des Gerichtshofs der Europäischen Union vom 16. Oktober 2012 in der Rechtssache C-614/10, Kommission/Österreich, die Frage der Zuständigkeit der belangten Behörde zu prüfen (vgl. das hg. Erkenntnis vom heutigen Tag, Zl. 2011/17/0156, auf das auch hinsichtlich der Darstellung der anzuwendenden Rechtslage gemäß § 43

Abs. 2 VwGG verwiesen wird). 2.1. Noch vor Eingehen auf das konkrete Vorbringen des Beschwerdeführers im hier zu beurteilenden Fall ist im Hinblick auf das Urteil des Gerichtshofs der Europäischen Union vom 16. Oktober 2012 in der Rechtssache C-614/10, Kommission/Österreich, die Frage der Zuständigkeit der belangten Behörde zu prüfen vergleiche , das hg. Erkenntnis vom heutigen Tag, Zl. 2011/17/0156, auf das auch hinsichtlich der Darstellung der anzuwendenden Rechtslage gemäß Paragraph 43, Absatz 2, VwGG verwiesen wird).

Im Hinblick auf den hier zu entscheidenden Beschwerdefall geht der Verwaltungsgerichtshof im gegenständlichen Verfahren davon aus, dass eine Tätigkeit des Staates im strafrechtlichen Bereich zu beurteilen ist. Es liegt somit eine der in Art. 3 Abs. 2 der 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 (ABl. L 281, Seite 31 ff) erwähnten Ausnahmen vom Anwendungsbereich dieser Richtlinie vor (vgl. auch Art. 1 Abs. 3 der 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), ABl. L 201 vom 31. Juli 2002, Seite 37 ff: Im Hinblick auf den hier zu entscheidenden Beschwerdefall geht der Verwaltungsgerichtshof im gegenständlichen Verfahren davon aus, dass eine Tätigkeit des Staates im strafrechtlichen Bereich zu beurteilen ist. Es liegt somit eine der in Artikel 3, Absatz 2, der 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 Amtsblatt , L 281, Seite 31 ff) erwähnten Ausnahmen vom Anwendungsbereich dieser Richtlinie vor vergleiche , auch Artikel eins, Absatz 3, der 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), Amtsblatt , L 201 vom 31. Juli 2002, Seite 37 ff:

"(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, ..., und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates ... und die Tätigkeiten des Staates im strafrechtlichen Bereich."). Die mangelhafte Umsetzung der Richtlinie 95/46/EG im Hinblick auf die dort in Art. 28 Abs. 1 Unterabs. 2 angesprochene Kontrollstelle für den Schutz personenbezogener Daten, die die ihr zugewiesene Aufgabe "in völliger Unabhängigkeit" wahrzunehmen habe, führt daher - infolge der Nichtanwendbarkeit der Richtlinie - nicht zur Unzuständigkeit der belangten Behörde (vgl. dazu näher das bereits erwähnte hg. Erkenntnis vom heutigen Tag, Zl. 2011/17/0156)."(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des Vertrags zur Gründung der Europäischen Gemeinschaft fallen, ..., und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates ... und die Tätigkeiten des Staates im strafrechtlichen Bereich."). Die mangelhafte Umsetzung der Richtlinie 95/46/EG im Hinblick auf die dort in Artikel 28, Absatz eins, Unterabs. 2 angesprochene Kontrollstelle für den Schutz personenbezogener Daten, die die ihr zugewiesene Aufgabe "in völliger Unabhängigkeit" wahrzunehmen habe, führt daher - infolge der Nichtanwendbarkeit der Richtlinie - nicht zur Unzuständigkeit der belangten Behörde vergleiche , dazu näher das bereits erwähnte hg. Erkenntnis vom heutigen Tag, Zl. 2011/17/0156).

2.2. Das Beschwerdevorbringen lässt sich dahin zusammenfassen, dass der Beschwerdeführer die Rechtswidrigkeit des angefochtenen Bescheides darin erblickt, dass die belangte Behörde zu Unrecht - gestützt auf Rechtsprechung des Obersten Gerichtshofes - davon ausgegangen sei, dass im Beschwerdefall die Befassung eines unabhängigen Richters nicht erforderlich gewesen sei; das Fernmeldegeheimnis des Art. 10a StGG erfordere eine diesbezügliche Auslegung.

2.2. Das Beschwerdevorbringen lässt sich dahin zusammenfassen, dass der Beschwerdeführer die Rechtswidrigkeit des angefochtenen Bescheides darin erblickt, dass die belangte Behörde zu Unrecht - gestützt auf Rechtsprechung des Obersten Gerichtshofes - davon ausgegangen sei, dass im Beschwerdefall die Befassung eines unabhängigen Richters nicht erforderlich gewesen sei; das Fernmeldegeheimnis des Artikel 10 a, StGG erfordere eine diesbezügliche Auslegung.

2.3. Der Verfassungsgerichtshof hat in seinem Erkenntnis vom 29. Juni 2012, B 1031/11 = VfSlg. 19.657, mit dem er über die Parallelbeschwerde gegen den auch hier angefochtenen Bescheid der belangten Behörde absprach, zu dieser Frage Stellung genommen. Er hat dabei - wobei hinsichtlich der zugrunde zu legenden Rechtsvorschriften auf deren Wiedergabe in dem erwähnten Erkenntnis vom 29. Juni 2012 verwiesen werden kann - unter anderem wie folgt ausgeführt:

"2. Gegen die Vorschriften des § 53 Abs 3a Z 2 und 3 SPG sind vor dem Hintergrund des Falles keine verfassungsrechtlichen Bedenken entstanden. "2. Gegen die Vorschriften des Paragraph 53, Absatz 3 a, Ziffer 2, und 3 SPG sind vor dem Hintergrund des Falles keine verfassungsrechtlichen Bedenken entstanden.

3. Die in Rede stehenden Bestimmungen greifen aus folgenden Gründen nicht in den Schutz des Fernmeldegeheimnisses iSd Art 10a StGG ein: 3. Die in Rede stehenden Bestimmungen greifen aus folgenden Gründen nicht in den Schutz des Fernmeldegeheimnisses iSd Artikel 10 a, StGG ein:

3.1. Die Verfassungsnorm des Art 10a StGG wurde durch BGBl. 8/1974 in das StGG eingefügt; ihr zufolge darf das Fernmeldegeheimnis nicht verletzt werden (Abs 1), Ausnahmen sind nur auf Grund eines richterlichen Befehls in Gemäßheit der bestehenden Gesetze zulässig (Abs 2). 3.1. Die Verfassungsnorm des Artikel 10 a, StGG wurde durch Bundesgesetzblatt 8 aus 1974, in das StGG eingefügt; ihr zufolge darf das Fernmeldegeheimnis nicht verletzt werden (Absatz eins,), Ausnahmen sind nur auf Grund eines richterlichen Befehls in Gemäßheit der bestehenden Gesetze zulässig (Absatz 2,).

3.1.1. Beim Fernmeldegeheimnis handelt es sich nach den Gesetzesmaterialien um ein dem Briefgeheimnis 'verwandtes Recht', das (wie Art 10 StGG) die Vertraulichkeit aller 'nicht für die Öffentlichkeit bestimmten, im Wege des Fernmeldeverkehrs übermittelten Nachrichten oder Mitteilungen' schützt (AB 960 BlgNR 13. GP, 2). Dabei kommt es auf die Bestimmung der Information für 'eine konkrete Person' an, und nicht darauf, ob die Nachricht allgemein bekannt (geworden) ist. 'Maßnahmen der rein technischen Überwachung des Fernmeldeverkehrs' stellen nach den zitierten Materialien keine Eingriffe in das Fernmeldegeheimnis dar, weil 'ein geordneter und sicher funktionierender Fernmeldeverkehr ohne entsprechende betriebliche und technische Aufsicht nicht denkbar' sei. Dem Schutz unterliegt daher - wie beim Briefgeheimnis, das die Vertraulichkeit des Briefinhaltes (nicht allfällige Informationen auf dem Kuvert) garantiert - der weitergegebene Gedankeninhalt, ohne äußere Gesprächsdaten (zB Telefonnummern) zu erfassen. 3.1.1. Beim Fernmeldegeheimnis handelt es sich nach den Gesetzesmaterialien um ein dem Briefgeheimnis 'verwandtes Recht', das (wie Artikel 10, StGG) die Vertraulichkeit aller 'nicht für die Öffentlichkeit bestimmten, im Wege des Fernmeldeverkehrs übermittelten Nachrichten oder Mitteilungen' schützt Ausschussbericht 960, BlgNR 13. GP, 2). Dabei kommt es auf die Bestimmung der Information für 'eine konkrete Person' an, und nicht darauf, ob die Nachricht allgemein bekannt (geworden) ist. 'Maßnahmen der rein technischen Überwachung des Fernmeldeverkehrs' stellen nach den zitierten Materialien keine Eingriffe in das Fernmeldegeheimnis dar, weil 'ein geordneter und sicher funktionierender Fernmeldeverkehr ohne entsprechende betriebliche und technische Aufsicht nicht denkbar' sei. Dem Schutz unterliegt daher - wie beim Briefgeheimnis, das die Vertraulichkeit des Briefinhaltes (nicht allfällige Informationen auf dem Kuvert) garantiert - der weitergegebene Gedankeninhalt, ohne äußere Gesprächsdaten (zB Telefonnummern) zu erfassen.

3.1.2. Art 10a StGG war bei seiner Einfügung in das Staatsgrundgesetz im Jahr 1974 primär auf den Telegraphen- und Fernmeldeverkehr ausgerichtet. Der Schutz ist nach herrschender Auffassung inzwischen nicht auf Telefonate und Telegramme beschränkt, sondern bezieht sich nunmehr - nicht zuletzt vor dem Hintergrund des dem Begriff 'Fernmeldegeheimnis' bereits vom historischen Verfassungsgesetzgeber unterlegten weiten Verständnisses (AB 960 BlgNR 13. GP, 2) - auf alle Arten der Telekommunikation, einschließlich des Nachrichtenaustausches über das Internet (inklusive geschlossener Internetforen - Chat-Foren; ...) 3.1.2. Artikel 10 a, StGG war bei seiner Einfügung in das Staatsgrundgesetz im Jahr 1974 primär auf den Telegraphen- und Fernmeldeverkehr ausgerichtet. Der Schutz ist nach herrschender Auffassung inzwischen nicht auf Telefonate und Telegramme beschränkt, sondern bezieht sich nunmehr - nicht zuletzt vor dem Hintergrund des dem Begriff 'Fernmeldegeheimnis' bereits vom historischen Verfassungsgesetzgeber unterlegten weiten Verständnisses Ausschussbericht 960, BlgNR 13. GP, 2) - auf alle Arten der Telekommunikation, einschließlich des Nachrichtenaustausches über das Internet (inklusive geschlossener Internetforen - Chat-Foren; ...)

Ob eine im Wege des Internets übermittelte Nachricht vom Schutzbereich des Art 10a StGG erfasst ist, hängt also davon ab, ob es sich um eine Kommunikation handelt, die dem Telegraphen- und Fernmeldeverkehr entspricht. Der Nachrichtenaustausch ist daher jedenfalls dann geschützt, wenn bestimmte Teilnehmer miteinander kommunizieren wollen und die Nachricht jeweils nur für diese Teilnehmer bestimmt ist (es sich nach den Ausführungen der Bundesministerin für Inneres also um eine sogenannte geschlossene Kommunikation - wie etwa beim E-Mail-Verkehr - handelt). Ob eine im Wege des Internets übermittelte Nachricht vom Schutzbereich des Artikel 10 a, StGG erfasst ist, hängt also davon ab, ob es sich um eine Kommunikation handelt, die dem Telegraphen- und Fernmeldeverkehr

entspricht. Der Nachrichtenaustausch ist daher jedenfalls dann geschützt, wenn bestimmte Teilnehmer miteinander kommunizieren wollen und die Nachricht jeweils nur für diese Teilnehmer bestimmt ist (es sich nach den Ausführungen der Bundesministerin für Inneres also um eine sogenannte geschlossene Kommunikation - wie etwa beim E-Mail-Verkehr - handelt).

3.1.3. Art 10a StGG gewährleistet somit die Vertraulichkeit der Telekommunikation, schützt also jedenfalls den Inhalt einer auf diesem Weg weitergegebenen Nachricht, nicht aber sämtliche anderen damit zusammenhängenden Daten; Gegenstand des Fernmeldegeheimnisses sind somit alle Inhaltsdaten, nicht aber der gesamte Telekommunikationsverkehr schlechthin ... 3.1.3. Artikel 10 a, StGG gewährleistet somit die Vertraulichkeit der Telekommunikation, schützt also jedenfalls den Inhalt einer auf diesem Weg weitergegebenen Nachricht, nicht aber sämtliche anderen damit zusammenhängenden Daten; Gegenstand des Fernmeldegeheimnisses sind somit alle Inhaltsdaten, nicht aber der gesamte Telekommunikationsverkehr schlechthin ...

3.2. Seit Inkrafttreten der SPG-Novelle BGBl. I 114/2007 (mit 1. Jänner 2008) sind die Sicherheitsbehörden gemäß § 53 Abs 3a SPG ermächtigt, auf Basis einer bestimmten Nachricht die dazugehörige (statische oder dynamische) IP-Adresse samt deren Verwendungszeit (Z 2) sowie anhand einer bestimmten IP-Adresse Namen und Anschrift des Nutzers des Endgerätes, dem die IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war (Z 3), zu ermitteln. 3.2. Seit Inkrafttreten der SPG-Novelle Bundesgesetzblatt Teil eins, 114 aus 2007, (mit 1. Jänner 2008) sind die Sicherheitsbehörden gemäß Paragraph 53, Absatz 3 a, SPG ermächtigt, auf Basis einer bestimmten Nachricht die dazugehörige (statische oder dynamische) IP-Adresse samt deren Verwendungszeit (Ziffer 2,) sowie anhand einer bestimmten IP-Adresse Namen und Anschrift des Nutzers des Endgerätes, dem die IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war (Ziffer 3,), zu ermitteln.

3.2.1. ...

3.2.2. Nach dem Wortlaut der Regelungen des § 53 Abs 3a Z 2 und 3 SPG ist die Auskunftserteilung auf die einer bestimmten (der Sicherheitsbehörde zur Kenntnis gelangten) Nachricht zuzuordnende IP-Adresse bzw. auf Namen und Anschrift des Inhabers des zu einer bestimmten IP-Adresse gehörigen Endgerätes beschränkt, weshalb nur diese Daten seitens der Sicherheitsbehörde beim Betreiber oder sonstigen Diensteanbieter ermittelt werden dürfen. 3.2.2. Nach dem Wortlaut der Regelungen des Paragraph 53, Absatz 3 a, Ziffer 2, und 3 SPG ist die Auskunftserteilung auf die einer bestimmten (der Sicherheitsbehörde zur Kenntnis gelangten) Nachricht zuzuordnende IP-Adresse bzw. auf Namen und Anschrift des Inhabers des zu einer bestimmten IP-Adresse gehörigen Endgerätes beschränkt, weshalb nur diese Daten seitens der Sicherheitsbehörde beim Betreiber oder sonstigen Diensteanbieter ermittelt werden dürfen.

Für die Erlangung anderer Daten bzw. Datenkategorien, insbesondere solcher, die über die schon bekannte Nachricht hinausgehende (durch Art 10a StGG geschützte) Kommunikationsinhalte betreffen, enthält § 53 Abs 3a SPG hingegen keine Ermächtigung. Für die Erlangung anderer Daten bzw. Datenkategorien, insbesondere solcher, die über die schon bekannte Nachricht hinausgehende (durch Artikel 10 a, StGG geschützte) Kommunikationsinhalte betreffen, enthält Paragraph 53, Absatz 3 a, SPG hingegen keine Ermächtigung.

3.2.3. § 53 Abs 3a Z 2 SPG erlaubt den Sicherheitsbehörden die Ausforschung einer IP-Adresse ausschließlich auf Grund einer bestimmten, ihnen (wie hier) durch Mitteilung eines Kommunikationspartners oder durch offene (jedermann zugängliche) Internetkommunikation bekannt gewordenen Nachricht. 3.2.3. Paragraph 53, Absatz 3 a, Ziffer 2, SPG erlaubt den Sicherheitsbehörden die Ausforschung einer IP-Adresse ausschließlich auf Grund einer bestimmten, ihnen (wie hier) durch Mitteilung eines Kommunikationspartners oder durch offene (jedermann zugängliche) Internetkommunikation bekannt gewordenen Nachricht.

Die anhand einer solchen Nachricht unter den sonstigen Voraussetzungen des § 53 Abs 3a Z 2 und 3 SPG seitens der Sicherheitsbehörde ermittelten (Einzel-)Daten sind daher nicht vom Schutzbereich des Art 10a StGG erfasst. Die anhand einer solchen Nachricht unter den sonstigen Voraussetzungen des Paragraph 53, Absatz 3 a, Ziffer 2, und 3 SPG seitens der Sicherheitsbehörde ermittelten (Einzel-)Daten sind daher nicht vom Schutzbereich des Artikel 10 a, StGG erfasst.

3.2.4. Sobald also der Inhalt einer solchen Nachricht von den Sicherheitsbehörden aus einer offenen Kommunikation rechtmäßig ermittelt wurde oder aus einer geschlossenen Kommunikation von einem der Teilnehmer der Sicherheitsbehörde zugänglich gemacht wurde, steht sie daher nicht unter dem Schutz des Art 10a StGG, sodass die Übermittlung der Verkehrsdaten, die in weiterer Folge die Ermittlung jener Personen, die an dem Nachrichtenverkehr

teilgenommen haben, ermöglicht, nicht als Eingriff in das Fernmeldegeheimnis zu qualifizieren ist. 3.2.4. Sobald also der Inhalt einer solchen Nachricht von den Sicherheitsbehörden aus einer offenen Kommunikation rechtmäßig ermittelt wurde oder aus einer geschlossenen Kommunikation von einem der Teilnehmer der Sicherheitsbehörde zugänglich gemacht wurde, steht sie daher nicht unter dem Schutz des Artikel 10 a, StGG, sodass die Übermittlung der Verkehrsdaten, die in weiterer Folge die Ermittlung jener Personen, die an dem Nachrichtenverkehr teilgenommen haben, ermöglicht, nicht als Eingriff in das Fernmeldegeheimnis zu qualifizieren ist.

3.2.5. Die Vorschriften des § 53 Abs 3a Z 2 und 3 SPG gestatten Sicherheitsbehörden somit von vornherein weder die geheime Überwachung des Internetverkehrs oder den Zugang zu einer Nachricht aus einem geschlossenen Internetforum noch ermächtigen sie zur vorsorglichen anlasslosen Speicherung oder zur systematischen (etwa die Erstellung von Persönlichkeitsprofilen ermöglichende) Verknüpfung von Datensträngen, unabhängig davon, ob diese Daten auch dem Schutzbereich des Art 10a StGG unterliegen ... 3.2.5. Die Vorschriften des Paragraph 53, Absatz 3 a, Ziffer 2, und 3 SPG gestatten Sicherheitsbehörden somit von vornherein weder die geheime Überwachung des Internetverkehrs oder den Zugang zu einer Nachricht aus einem geschlossenen Internetforum noch ermächtigen sie zur vorsorglichen anlasslosen Speicherung oder zur systematischen (etwa die Erstellung von Persönlichkeitsprofilen ermöglichende) Verknüpfung von Datensträngen, unabhängig davon, ob diese Daten auch dem Schutzbereich des Artikel 10 a, StGG unterliegen ...

3.2.6. Der Sicherheitsbehörde dürfen vom Betreiber vielmehr bloß punktuelle Auskünfte erteilt werden, die keinen Rückschluss auf andere (nicht bereits bekannte) Inhalte erlauben.

3.2.7. Die Auskunftspflichtung des Betreibers setzt überdies voraus, dass dieser überhaupt (noch) über gespeicherte Daten verfügt; eine über die Speicherverpflichtungen nach dem TKG (insbesondere zu Verrechnungszwecken gemäß § 99 Abs 2 TKG 2003) hinausgehende Pflicht zur Speicherung von Verkehrsdaten enthält § 53 Abs 3a SPG nicht ... 3.2.7. Die Auskunftspflichtung des Betreibers setzt überdies voraus, dass dieser überhaupt (noch) über gespeicherte Daten verfügt; eine über die Speicherverpflichtungen nach dem TKG (insbesondere zu Verrechnungszwecken gemäß Paragraph 99, Absatz 2, TKG 2003) hinausgehende Pflicht zur Speicherung von Verkehrsdaten enthält Paragraph 53, Absatz 3 a, SPG nicht ...

3.3. Entgegen der Ansicht des Beschwerdeführers bieten die von der belangten Behörde im gegebenen Zusammenhang angewendeten Bestimmungen des § 53 Abs 3a Z 2 und 3 SPG idF BGBl. I 114/2007 mithin keine Basis für die Ermittlung von Inhaltsdaten iSd Art 10a StGG ... 3.3. Entgegen der Ansicht des Beschwerdeführers bieten die von der belangten Behörde im gegebenen Zusammenhang angewendeten Bestimmungen des Paragraph 53, Absatz 3 a, Ziffer 2, und 3 SPG in der Fassung Bundesgesetzblatt Teil eins, 114 aus 2007, mithin keine Basis für die Ermittlung von Inhaltsdaten iSd Artikel 10 a, StGG ...

4. Hingegen greift die Bestimmung des § 53 Abs 3a SPG in das verfassungsgesetzlich gewährleistete Recht auf Datenschutz gemäß § 1 Abs 1 DSG 2000 iVm Art 8 EMRK ein, verletzt dieses jedoch aus folgenden Gründen nicht: 4. Hingegen greift die Bestimmung des Paragraph 53, Absatz 3 a, SPG in das verfassungsgesetzlich gewährleistete Recht auf Datenschutz gemäß Paragraph eins, Absatz eins, DSG 2000 in Verbindung mit Artikel 8, EMRK ein, verletzt dieses jedoch aus folgenden Gründen nicht:

4.1. Nach § 1 Abs 1 DSG 2000 hat jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf die Achtung des Privat- und Familienlebens, hat. 4.1. Nach Paragraph eins, Absatz eins, DSG 2000 hat jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf die Achtung des Privat- und Familienlebens, hat.

4.2. Beschränkungen dieses Grundrechts sind nach dem Gesetzesvorbehalt des § 1 Abs 2 DSG 2000 (abgesehen von lebenswichtigen Interessen des Betroffenen an der Verwendung personenbezogener Daten oder seiner Zustimmung hiezu) bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen zulässig, die aus den in Art 8 Abs 2 EMRK genannten Gründen notwendig sind und die ausreichend präzise, also für jedermann vorhersehbar regeln, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung personenbezogener Daten für die Wahrnehmung konkreter Verwaltungsaufgaben erlaubt ist ... Der jeweilige Gesetzgeber muss somit nach den Vorgaben des § 1 Abs 2 DSG 2000 ... eine materienspezifische Regelung in dem Sinn vorsehen, dass die Fälle zulässiger Eingriffe in das Grundrecht auf Datenschutz konkretisiert und begrenzt werden ... 4.2. Beschränkungen dieses Grundrechts sind nach

dem Gesetzesvorbehalt des Paragraph eins, Absatz 2, DSG 2000 (abgesehen von lebenswichtigen Interessen des Betroffenen an der Verwendung personenbezogener Daten oder seiner Zustimmung hiezu) bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen zulässig, die aus den in Artikel 8, Absatz 2, EMRK genannten Gründen notwendig sind und die ausreichend präzise, also für jedermann vorhersehbar regeln, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung personenbezogener Daten für die Wahrnehmung konkreter Verwaltungsaufgaben erlaubt ist ... Der jeweilige Gesetzgeber muss somit nach den Vorgaben des Paragraph eins, Absatz 2, DSG 2000 ... eine materienspezifische Regelung in dem Sinn vorsehen, dass die Fälle zulässiger Eingriffe in das Grundrecht auf Datenschutz konkretisiert und begrenzt werden ...

4.3. Eine solche ausdrückliche gesetzliche Ermächtigung zur Ermittlung der IP-Adresse sowie von Namen und Anschrift des Benutzers des Endgerätes, dem eine bestimmte IP-Adresse zugeordnet ist, enthält § 53 Abs 3a Z 2 und 3 SPG. Der Eingriff ist auf die bloße Auskunftserteilung über die erfragten Daten beschränkt. Angesichts des im öffentlichen Interesse gelegenen Aufgabengebietes der Sicherheitsbehörden betreffend die Abwehr gefährlicher Angriffe, insbesondere iZm der Verhinderung der Verwirklichung unmittelbar bevorstehender Vorsatztaten nach dem StGB, dem Verbotsgesetz, dem Fremdenpolizeigesetz und dem Suchtmittelgesetz (§§ 16 Abs 2 und 3, 21 Abs 2 SPG), ist es auch nicht unverhältnismäßig, den Sicherheitsbehörden bei Vorliegen einer bestimmten Nachricht, welche die Annahme einer konkreten Gefahrensituation rechtfertigt, die Ermittlung der in Rede stehenden Daten im Wege des Betreibers oder sonstigen Diensteanbieters gemäß § 53 Abs 3a Z 2 und 3 SPG (unter den Kautelen des kommissarischen Rechtsschutzes durch den weisungsfreien Rechtsschutzbeauftragten ... sowie konkreter Lösungsverpflichtungen ...) zu ermöglichen.

4.3. Eine solche ausdrückliche gesetzliche Ermächtigung zur Ermittlung der IP-Adresse sowie von Namen und Anschrift des Benutzers des Endgerätes, dem eine bestimmte IP-Adresse zugeordnet ist, enthält Paragraph 53, Absatz 3 a, Ziffer 2, und 3 SPG. Der Eingriff ist auf die bloße Auskunftserteilung über die erfragten Daten beschränkt. Angesichts des im öffentlichen Interesse gelegenen Aufgabengebietes der Sicherheitsbehörden betreffend die Abwehr gefährlicher Angriffe, insbesondere iZm der Verhinderung der Verwirklichung unmittelbar bevorstehender Vorsatztaten nach dem StGB, dem Verbotsgesetz, dem Fremdenpolizeigesetz und dem Suchtmittelgesetz (Paragraphen 16, Absatz 2, und 3, 21 Absatz 2, SPG), ist es auch nicht unverhältnismäßig, den Sicherheitsbehörden bei Vorliegen einer bestimmten Nachricht, welche die Annahme einer konkreten Gefahrensituation rechtfertigt, die Ermittlung der in Rede stehenden Daten im Wege des Betreibers oder sonstigen Diensteanbieters gemäß Paragraph 53, Absatz 3 a, Ziffer 2, und 3 SPG (unter den Kautelen des kommissarischen Rechtsschutzes durch den weisungsfreien Rechtsschutzbeauftragten ... sowie konkreter Lösungsverpflichtungen ...) zu ermöglichen.

4.4. Im Übrigen ist eine richterliche Genehmigung staatlicher Überwachungsmaßnahmen durch Art 8 EMRK nicht geboten ... 4.4. Im Übrigen ist eine richterliche Genehmigung staatlicher Überwachungsmaßnahmen durch Artikel 8, EMRK nicht geboten ...

5. Der Beschwerdeführer ist daher durch den angefochtenen Bescheid nicht in Rechten wegen Anwendung eines von ihm als verfassungswidrig angesehenen Gesetzes verletzt worden. ...

6.2. Ausgehend vom plausibel festgestellten (unbestrittenen) Sachverhalt, wonach der Beschwerdeführer im Rahmen seines von einem Dritten offenbarten Internetauftritts bei der Sicherheitsbehörde den Eindruck erweckte, Unmündige im zeitlichen Konnex zu Sexualkontakten zu vermitteln, ist die Annahme der belangten Behörde, dass die gesetzlichen Voraussetzungen des § 53 Abs 3a SPG für die getroffenen Maßnahmen (iSd Vorliegens einer auf Grund bestimmter Tatsachen indizierten Gefahrensituation sowie der Notwendigkeit der Datenermittlung als Voraussetzung für die Erfüllung sicherheitsbehördlicher Aufgaben) gegeben waren, verfassungsrechtlich nicht zu beanstanden. ..." 6.2. Ausgehend vom plausibel festgestellten (unbestrittenen) Sachverhalt, wonach der Beschwerdeführer im Rahmen seines von einem Dritten offenbarten Internetauftritts bei der Sicherheitsbehörde den Eindruck erweckte, Unmündige im zeitlichen Konnex zu Sexualkontakten zu vermitteln, ist die Annahme der belangten Behörde, dass die gesetzlichen Voraussetzungen des Paragraph 53, Absatz 3 a, SPG für die getroffenen Maßnahmen (iSd Vorliegens einer auf Grund bestimmter Tatsachen indizierten Gefahrensituation sowie der Notwendigkeit der Datenermittlung als Voraussetzung für die Erfüllung sicherheitsbehördlicher Aufgaben) gegeben waren, verfassungsrechtlich nicht zu beanstanden. ..."

Der Verwaltungsgerichtshof schließt sich hinsichtlich der in der Beschwerde aufgeworfenen Rechtsfragen (vgl. auch die Darstellung oben in Punkt 1.2.) der eben dargestellten rechtlichen Beurteilung durch den Verfassungsgerichtshof an. Der Verwaltungsgerichtshof schließt sich hinsichtlich der in der Beschwerde aufgeworfenen Rechtsfragen vergleiche



, auch die Darstellung oben in Punkt 1.2.) der eben dargestellten rechtlichen Beurteilung durch den Verfassungsgerichtshof an.

Zum Unterschied zur Rechtslage vor Inkrafttreten der SPG-Novelle BGBl. I Nr. 114/2007 (zur alten Rechtslage vgl. das hg. Erkenntnis vom 27. Mai 2009, Zl. 2007/05/0280), mit 1. Jänner 2008 sind die Sicherheitsbehörden ermächtigt, (nicht nur) von Betreibern öffentlicher Telekommunikationsdienste (sondern auch) von sonstigen Diensteanbietern die in § 53 Abs. 3a SPG näher umschriebenen Auskünfte zu verlangen. Damit sind auch die Diensteanbieter hinsichtlich eines Chatrooms erfasst (vgl. Thanner/Vogl, SPG2 (2013) 512 Anm 34 ff.) Zum Unterschied zur Rechtslage vor Inkrafttreten der SPG-Novelle Bundesgesetzblatt Teil eins, Nr. 114 aus 2007, (zur alten Rechtslage vergleiche , das hg. Erkenntnis vom 27. Mai 2009, Zl. 2007/05/0280), mit 1. Jänner 2008 sind die Sicherheitsbehörden ermächtigt, (nicht nur) von Betreibern öffentlicher Telekommunikationsdienste (sondern auch) von sonstigen Diensteanbietern die in Paragraph 53, Absatz 3 a, SPG näher umschriebenen Auskünfte zu verlangen. Damit sind auch die Diensteanbieter hinsichtlich eines Chatrooms erfasst vergleiche , Thanner/Vogl, SPG2 (2013) 512 Anmerkung 34, ff).

2.4. Aus den dargelegten Erwägungen ergibt sich, dass der Beschwerdeführer durch den angefochtenen Bescheid weder wegen der geltend gemachten noch wegen einer vom Verwaltungsgerichtshof aus Eigenem aufzugreifenden Rechtswidrigkeit verletzt worden ist.

Die Beschwerde war infolge dessen gemäß § 42 Abs. 1 VwGG als unbegründet abzuweisen. Die Beschwerde war infolge dessen gemäß Paragraph 42, Absatz eins, VwGG als unbegründet abzuweisen.

2.5. Die vorliegende Entscheidung bedurfte schon deshalb keiner Beschlussfassung in einem verstärkten Senat, weil der Verwaltungsgerichtshof hier eine gegenüber der Vorjudikatur (vgl. das hg. Erkenntnis vom 27. Mai 2009, Zl. 2007/05/0280) durch das Inkrafttreten der SPG-Novelle BGBl. I Nr. 114/2007 (mit 1. Jänner 2008) hinsichtlich der datenschutzrechtlichen Befugnisse der Sicherheitsbehörden geänderte Rechtslage zu beurteilen hatte. 2.5. Die vorliegende Entscheidung bedurfte schon deshalb keiner Beschlussfassung in einem verstärkten Senat, weil der Verwaltungsgerichtshof hier eine gegenüber der Vorjudikatur vergleiche , das hg. Erkenntnis vom 27. Mai 2009, Zl. 2007/05/0280) durch das Inkrafttreten der SPG-Novelle Bundesgesetzblatt Teil eins, Nr. 114 aus 2007, (mit 1. Jänner 2008) hinsichtlich der datenschutzrechtlichen Befugnisse der Sicherheitsbehörden geänderte Rechtslage zu beurteilen hatte.

2.6. Die Entscheidung über die Kosten beruht auf den §§ 47 ff VwGG in Verbindung mit der VwGH-Aufwandersatzverordnung 2008, BGBl. II Nr. 455. 2.6. Die Entscheidung über die Kosten beruht auf den Paragraphen 47, ff VwGG in Verbindung mit der VwGH-Aufwandersatzverordnung 2008, Bundesgesetzblatt , II Nr. 455.

Wien, am 24. April 2013

### **Schlagworte**

Gemeinschaftsrecht Richtlinie Umsetzungspflicht EURallg4/2

### **European Case Law Identifier (ECLI)**

ECLI:AT:VWGH:2013:2011170293.X00

### **Im RIS seit**

24.05.2013

### **Zuletzt aktualisiert am**

05.10.2017

**Quelle:** Verwaltungsgerichtshof VwGH, <http://www.vwgh.gv.at>