Sachverhalt

Schweizer Strafverfolgungsbehörden führten im Jahr 2006 eine Überwachung von Nutzern des Internetnetzwerkes »Razorback« durch und konnten feststellen, dass mehrere von ihnen kinderpornographisches Material in der Form von Bildern oder Videos besaßen und austauschten.

Auf Basis dieser von der Schweizer Polizei erhaltenen Daten ersuchte die slowenische Polizei am 7.8.2006 das Unternehmen S. (ein slowenischer Internetdienstanbieter – in der Folge »IDA«) ohne vorher eine gerichtliche Genehmigung einzuholen, Daten betreffend den Nutzer offenzulegen, dem zu einer bestimmten Zeit am 20.2.2006 eine bestimmte IP-Adresse zugewiesen gewesen war. Die Polizei stützte sich dabei auf § 149b Abs. 3 StPO, der die Betreiber von elektronischen Kommunikationsnetzwerken dazu verpflichtete, der Polizei Informationen zu den Eigentümern oder Nutzern bestimmter Mittel zur elektronischen Kommunikation offenzulegen. Am 10.8.2006 übermittelte der IDA der Polizei Namen und Adresse des Vaters des Bf., welcher der Abonnent des mit der betreffenden IP-Adresse verbundenen Internetdienstes war.

Im Dezember 2006 ersuchte die Polizei den IDA nach Einholung einer gerichtlichen Anordnung darum, die persönlichen Daten des Teilnehmers und mit der fraglichen IP-Adresse in Verbindung stehende Verkehrsdaten offenzulegen. Der IDA übermittelte der Polizei die verlangten Daten.

Daraufhin wurde eine Durchsuchung des Familienwohnsitzes des Bf. angeordnet, wobei sein Vater als Verdächtiger angegeben war. Es wurden vier Computer beschlagnahmt. Auf den Festplatten wurde kinderpornographisches Material gefunden. In weiterer Folge wurde der Bf. selbst als Verdächtiger geführt und eine strafrechtliche Untersuchung gegen ihn eingeleitet. Am 29.5.2008 wurde Anklage gegen ihn erhoben.

Mit Urteil vom 5.12.2008 befand das BG Kranj den Bf. des Besitzes und der Verbreitung von kinderpornographischem Material für schuldig und verurteilte ihn zu einer bedingten Freiheitsstrafe von acht Monaten, die vom Berufungsgericht später in eine unbedingte Strafe von sechs Monaten umgewandelt wurde. Das Urteil des Berufungsgerichts wurde vom Obersten Gericht am 20.1.2011 bestätigt. Die Gerichte wiesen den Ein-

wand des Bf. zurück, die slowenische Polizei hätte die Teilnehmerinformationen unrechtmäßig erlangt, da sie vorab keine gerichtliche Anordnung eingeholt hätte. Das Verfassungsgericht wies am 13.2.2014 eine Beschwerde des Bf. ab, da es zu keiner Verletzung seiner verfassungsmäßig gewährleisteten Rechte gekommen wäre. Insbesondere hätte der Bf. die IP-Adresse, mit der er Zugang zum Internet erhalten hatte, nicht verborgen und sich somit bewusst der Öffentlichkeit ausgesetzt. Er könne somit keine berechtigte Erwartung von Privatsphäre haben. Daher wären die Daten betreffend die Identität des Nutzers der IP-Adresse nicht nach Art. 37 der Verfassung (Schutz der Vertraulichkeit der Kommunikation), sondern nur nach Art. 38 der Verfassung (Schutz personenbezogener Daten) geschützt. Da Letzterer für die Vornahme eines Eingriffs jedoch keine gerichtliche Anordnung erforderte, wäre eine solche auch für die Offenlegung der Daten im Fall des Bf. nicht nötig gewesen.

Rechtsausführungen

Der Bf. behauptete eine Verletzung von Art. 8 EMRK (hier: *Recht auf Achtung des Privatlebens*), weil der IDA seine persönlichen Daten unrechtmäßig gespeichert und die Polizei Teilnehmerdaten in Verbindung mit seiner dynamischen IP-Adresse und in der Folge seine Identität willkürlich und ohne gerichtliche Anordnung erlangt hätte.

I. Zulässigkeit

1. Betreffend die angeblich unrechtmäßige Speicherung von persönlichen Daten durch den IDA

(74) Die Regierung behauptete, der Bf. habe es verabsäumt, sich vor den innerstaatlichen Gerichten über die unrechtmäßige Speicherung seiner persönlichen Daten durch den IDA zu beschweren. […] Sie brachte weiter vor, der IDA wäre eine private Einrichtung und der Bf. hätte ihn daher auch im Zivilverfahren auf Schadenersatz verklagen können. Jedenfalls sei dieser Teil der Beschwerde ihrer Ansicht nach wegen Nichterschöpfung des innerstaatlichen Instanzenzugs für unzulässig zu erklären.

(79) Im vorliegenden Fall rügte der Bf. in seiner Beschwerde an den GH die Speicherung seiner angeblichen persönlichen Daten durch den IDA. Er verabsäumte es diesbezüglich jedoch, die innerstaatlichen Rechtsbehelfe zu erschöpfen, da er diese Rüge nicht zumindest der Sache nach im innerstaatlichen Verfahren erhoben hat.

(80) Folglich muss dieser Teil der Beschwerde […] für **unzulässig** erklärt werden (mehrheitlich).

2. Betreffend die Offenlegung der Teilnehmerinformationen

(81) Die Regierung rügte, der Bf. könne nicht behaupten, Opfer [der gerügten Konventionsverletzung] zu sein, da die Teilnehmerinformationen, die vom IDA offengelegt worden waren, seinen Vater betroffen hätten.

(83) Der GH hält fest, dass diese Frage in engem Zusammenhang mit dem Inhalt der Beschwerde steht und verbindet die Einrede der Regierung daher mit der Entscheidung in der Sache (6:1 Stimmen; *abweichendes Sondervotum von Richter Vehabović*).

(84) Diese Rüge ist nicht offensichtlich unbegründet […] und auch aus keinem anderen Grund unzulässig und daher für **zulässig** zu erklären (mehrheitlich; *abweichendes Sondervotum von Richter Vehabović*).

II. In der Sache

1. Vorbemerkungen und Umfang der Prüfung des GH

(96) Der GH bemerkt […], dass eine IP-Adresse eine einzigartige Nummer ist, die jedem Netzwerkgerät zugewiesen ist. Dadurch wird den Geräten erlaubt, miteinander zu kommunizieren. Anders als eine statische IP-Adresse, die einer bestimmten Netzwerkschnittstelle eines speziellen Geräts permanent zugewiesen ist, wird eine dynamische IP-Adresse einem Gerät durch den IDA vorübergehend zugewiesen, nämlich typischerweise zu jedem Zeitpunkt, zu dem sich das Gerät mit dem Internet verbindet. Die IP-Adresse alleine ermöglicht es, gewisse Details, wie den IDA, mit dem der Nutzer verbunden ist, sowie im Groben einen physischen Standort – am wahrscheinlichsten den Standort des IDA – zu bestimmen. Die meisten dynamischen IP-Adressen können somit zum IDA zurückverfolgt werden und nicht zu einem speziellen Computer. Um den Namen und die Adresse des Teilnehmers zu erhalten, der eine dynamische IP-Adresse verwendet, ist es normalerweise erforderlich, dass der IDA diese Informationen eruiert und zu diesem Zwecke die relevanten Verbindungsdaten seiner Teilnehmer prüft.

(97) Im vorliegenden Fall wurden die Informationen über die dynamische IP-Adresse und die Zeit, zu der sie zugewiesen worden war, durch die Schweizer Polizei gesammelt. Diese hatte eine Überwachung von Nutzern eines speziellen Internetnetzwerks, das kinderpornographisches Material umfasste, durchgeführt. Sie übergab die Informationen an die slowenische Polizei, die vom IDA Name und Adresse des mit der fraglichen dynamischen IP-Adresse in Verbindung stehenden Teilnehmers – des Vaters des Bf. – erlangte.

(98) Die Regierung brachte vor, Art. 8 EMRK würde in diesem Fall keine Anwendung finden, weil der Bf. von der strittigen Maßnahme nicht direkt betroffen gewesen

sei und selbst wenn dies der Fall gewesen wäre, er freiwillig auf sein Recht auf Privatsphäre verzichtet hätte, indem er die fraglichen Dateien öffentlich ausgetauscht hätte. Um diese Fragen zu beantworten, muss der GH prüfen, ob der Bf. oder irgendein anderer Internetnutzer eine angemessene Erwartung hatte, dass seine ansonsten öffentliche Online-Aktivität anonym bleiben würde.

(99) Der GH wiederholt in diesem Zusammenhang, dass sexueller Missbrauch unzweifelhaft eine abscheuliche Verfehlung mit lähmenden Auswirkungen auf die Opfer ist. Kinder und andere verwundbare Individuen haben das Recht auf staatlichen Schutz vor solchen schweren Eingriffen in wesentliche Aspekte ihres Privatlebens, und zwar in der Form von wirksamer Abschreckung. Dieser Schutz umfasst ein Bedürfnis, die Straftäter zu identifizieren und sie zur Rechenschaft zu ziehen. Die von der Regierung aufgeworfenen Fragen betreffend die Anwendbarkeit von Art. 8 EMRK müssen jedoch unabhängig vom legalen oder illegalen Charakter der fraglichen Aktivität und ebenso unbeschadet der Anforderung aus der Konvention beantwortet werden, dass von den Mitgliedstaaten Schutz für verwundbare Individuen gewährt werden muss [...].

2. Anwendbarkeit von Art. 8 EMRK

(101) Für die Überlegung, ob das Privatleben einer Person von Maßnahmen außerhalb ihres Zuhauses oder ihrer privaten Räumlichkeiten betroffen ist, sind eine Reihe von Elementen relevant. Um zu ermitteln, ob die Begriffe von »Privatleben« und »Korrespondenz« anwendbar sind, hat der GH bei mehreren Gelegenheiten geprüft, ob Individuen eine angemessene Erwartung hatten, dass ihre Privatsphäre geachtet und geschützt würde. In diesem Zusammenhang hat er festgehalten, dass eine angemessene Erwartung von Privatsphäre ein bedeutender, wenn auch nicht unbedingt entscheidender Faktor ist.

(102) Im Kontext von persönlichen Daten hat der GH darauf hingewiesen, dass der Begriff des »Privatlebens« nicht restriktiv interpretiert werden darf. Er hat festgestellt, dass die weite Auslegung jener des Übereinkommen von 1981[1] entspricht [...]. Solche persönlichen Daten werden definiert als »jede Information über eine bestimmte oder bestimmbare natürliche Person« (Art. 2).

(103) Ferner geht aus der gefestigten Rechtsprechung hervor, dass Fragen im Hinblick auf das Privatleben auftreten, wenn Daten über ein spezielles Individuum erhoben, verarbeitet oder verwendet werden oder das betroffene Material auf eine Weise oder in einem Maß veröffentlicht wird, die bzw. das über das normalerweise Vorhersehbare hinausgehen. [...]

a. Natur der berührten Interessen

(107) Die Regierung hat nicht bestritten, dass die Teilnehmerinformationen grundsätzlich persönliche Daten darstellen. Eine solche Schlussfolgerung lässt sich auch aus den Definitionen in der Konvention von 1981, der Gesetzgebung der EU sowie der innerstaatlichen Gesetzgebung, die deren Umsetzung dient, ableiten.

(108) Zusätzlich bemerkt der GH, dass die mit zu bestimmten Zeiten zugewiesenen speziellen dynamischen IP-Adressen verbundenen Teilnehmerinformationen nicht öffentlich verfügbar waren und deshalb nicht mit den Informationen verglichen werden können, die im traditionellen Telefonbuch oder der öffentlichen Datenbank für Fahrzeugkennzeichen auffindbar sind, auf welche die Regierung verwies. Tatsächlich scheint es, dass der IDA, um einen Teilnehmer zu identifizieren, dem zu einer bestimmten Zeit eine spezielle IP-Adresse zugewiesen wurde, Zugang zu gespeicherten Daten betreffend spezielle Telekommunikationen nehmen muss. Die Verwendung solcher gespeicherter Daten kann für sich bereits Überlegungen im Hinblick auf das Privatleben verlangen.

(109) Zudem ist es dem GH unmöglich, den speziellen Kontext zu ignorieren, in dem im vorliegenden Fall um die Teilnehmerinformationen angesucht wurde. Der einzige Zweck für die Erlangung der Teilnehmerinformationen war es, eine spezielle Person hinter den unabhängig davon gesammelten Inhaltsdaten zu identifizieren [...]. Der GH bemerkt in diesem Zusammenhang, dass es einen Bereich der Interaktion einer Person mit anderen gibt, der in den Anwendungsbereich des »Privatlebens« fällt. Informationen über derartige Aktivitäten betreffen den Aspekt der Privatsphäre ab dem Moment, wo sie mit einer identifzierten oder identifizierbaren Einzelperson verbunden sind oder dieser zugewiesen werden [...]. Was daher von der Polizei gesuchte periphere Informationen zu sein scheinen, nämlich der Name und die Adresse eines Teilnehmers, muss in Situationen wie jener des vorliegenden Falles als untrennbar mit den relevanten, zuvor vorhandenen Inhaltsdaten in Verbindung stehend behandelt werden [...]. Es anders zu sehen würde bedeuten, Informationen den notwendigen Schutz zu verweigern, die sehr viel über die Online-Aktivitäten eines Individuums enthüllen können, einschließlich sensibler Details über dessen Interessen, Überzeugungen und privaten Lebensstil.

(110) Angesichts der obigen Überlegungen kommt der GH zum Schluss, dass der vorliegende Fall Fragen der Privatsphäre betrifft, die geeignet sind, den Schutz von Art. 8 EMRK zu aktivieren.

1 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (SEV Nr. 108), BGBl. 1988/317.

b. Wurde der Bf. durch die strittige Maßnahme identifiziert?

(111) Der GH muss sich zunächst mit dem Argument der Regierung befassen, dass die von der Polizei erlangten Teilnehmerinformationen nur den Namen und die Adresse des Vaters des Bf. enthüllten und nicht des Bf. selbst. In diesem Zusammenhang hält der GH fest, dass allgemein akzeptiert wurde, dass die Definition von persönlichen Daten sich nicht nur auf Informationen betreffend identifizierte, sondern auch betreffend identifizierbare Individuen bezieht.

(112) Im vorliegenden Kontext war der Bf. ohne Zweifel Nutzer des fraglichen Internetdienstes und es war seine Online-Aktivität, die von der Polizei überwacht wurde. Der GH beobachtet weiter, dass der Bf. das Internet dem Anschein nach über seinen eigenen Computer in seinem eigenen Zuhause nutzte. Es hat wenig Aussagekraft, dass der Name des Bf. in den von der Polizei erlangten Teilnehmerinformationen nicht genannt wurde. Tatsächlich ist es nicht ungewöhnlich, dass ein Haushalt ein einziges Abonnement für einen Internetdienst hat, das von mehreren Familienmitgliedern genutzt wird. Der Umstand, dass sie den Internetdienst nicht persönlich abonniert haben, hat keine Auswirkungen auf ihre Erwartungen von Privatsphäre, die indirekt zum Tragen kommen, sobald die Teilnehmerinformationen betreffend ihre private Nutzung des Internets enthüllt werden.

(113) Es ist klar, dass der Zweck der strittigen Maßnahme, nämlich die Erlangung von Teilnehmerinformationen in Verbindung mit der dynamischen IP-Adresse [...] durch die Polizei ohne gerichtliche Anordnung, darin lag, die Computernutzung mit einem Standort und womöglich einer Person zu verknüpfen. Die Teilnehmerinformationen, die auch die Adresse enthielten, erlaubten es der Polizei, das Zuhause zu identifizieren, von dem aus die fragliche Internetverbindung aufgebaut worden war. Das führte dazu, dass sie den Bf. als mutmaßlichen User des »Razorback«-Netzwerks identifizierte.

(114) Angesichts des Vorgesagten und unter Berücksichtigung dessen, dass die innerstaatlichen Gerichte den Fall nicht aus dem Grund abwiesen, dass der Bf. nicht der Abonnent des fraglichen Internetdienstes gewesen war, kommt der GH zum Schluss, dass dieser Umstand im vorliegenden Fall nicht als Hindernis für die Anwendung von Art. 8 EMRK gesehen werden kann. Er weist die Einrede der Regierung betreffend das angebliche Fehlen des Opferstatus daher zurück (6:1 Stimmen; *abweichendes Sondervotum von Richter Vehabović*).

c. Hatte der Bf. eine angemessene Erwartung von Privatsphäre?

(115) Um festzustellen, ob der Begriff des »Privatlebens« auf den vorliegenden Fall anwendbar ist, muss der GH prüfen, ob der Bf. angesichts der öffentlichen Zugänglichkeit des fraglichen Netzwerks eine angemessene Erwartung hatte, dass seine Privatsphäre respektiert und geschützt würde. In diesem Zusammenhang befanden das Verfassungsgericht und die belangte Regierung [...], dass er seine Online-Aktivität und zugehörige dynamische IP-Adresse bewusst der Öffentlichkeit preisgegeben habe. Daher sei seine Erwartung von Privatsphäre ihrer Ansicht nach nicht berechtigt gewesen und müsse zudem davon ausgegangen werden, dass er darauf verzichtet habe.

(116) Der GH akzeptiert [...], dass der Bf., als er Dateien mit pornographischem Material über das »Razorback«-Netzwerk austauschte, aus seiner subjektiven Sicht erwartete, dass diese Aktivität privat bleiben und seine Identität nicht offengelegt werden würde [...]. Anders als das Verfassungsgericht befindet der GH jedoch, dass der Umstand, dass er seine dynamische IP-Adresse nicht verbarg – unter der Annahme, dass dies möglich ist –, bei der Beurteilung nicht entscheidend sein kann, ob seine Erwartung von Privatsphäre von einem objektiven Standpunkt aus gesehen angemessen war. In diesem Zusammenhang bemerkt er, dass sich eindeutig nicht die Frage stellt, ob der Bf. in angemessener Weise erwarten konnte, seine dynamische IP-Adresse geheim zu halten, sondern ob er in angemessener Weise Privatsphäre im Hinblick auf seine Identität erwarten konnte.

(117) Der GH hat den Anonymitätsaspekt von Online-Privatsphäre bereits anerkannt [...], der mit der Natur der Online-Aktivität in Verbindung steht, an der sich die Nutzer beteiligen, ohne unbedingt identifizierbar zu sein. Dieses Anonymitätskonzept der Privatsphäre muss bei der gegenständlichen Beurteilung als wesentlicher Faktor berücksichtigt werden. Insbesondere wurde nicht vorgebracht, dass der Bf. seine Identität im Hinblick auf die fragliche Online-Aktivität je enthüllt hätte [...] oder dass er etwa durch den speziellen Anbieter der Seite über ein Konto oder Kontaktdaten identifizierbar gewesen wäre. Seine Online-Aktivität brachte daher einen hohen Grad an Anonymität mit sich, was durch den Umstand bestätigt wird, dass die zugewiesene dynamische IP-Adresse – selbst wenn sie für die Nutzer des Netzwerks sichtbar war – nicht zum konkreten Computer zurückverfolgt werden konnte, ohne dass die Daten vom IDA nach einem Ersuchen der Polizei verifiziert wurden.

(118) Letztlich hält der GH fest, dass der anwendbare rechtliche Rahmen ebenso ein relevanter – wenn auch nicht unbedingt ein entscheidender – Faktor bei der Beurteilung der angemessenen Erwartung von Privatsphäre sein kann. Im vorliegenden Fall legte keine der Parteien Informationen betreffend die Vertragsbestimmungen vor, auf der Basis welcher der Internetdienst dem Vater des Bf. angeboten worden war. Was den gesetzlichen Rahmen anbelangt, erachtet es der GH für ausreichend festzuhalten, dass Art. 37 der Verfassung die Privatheit der Korrespondenz und Kommunikation

garantierte und verlangte, dass jeder Eingriff in dieses Recht auf eine gerichtliche Anordnung gestützt wurde. Daher kann auch aus Sicht der zur betreffenden Zeit in Kraft stehenden Gesetzgebung nicht gesagt werden, dass die Erwartung des Bf. von Privatsphäre im Hinblick auf seine Online-Aktivität als unberechtigt oder unangemessen angesehen werden konnte.

d. Schlussfolgerung

(119) Aus den oben genannten Gründen kommt der GH zum Schluss, dass das Interesse des Bf. daran, seine Identität im Hinblick auf seine Online-Aktivität geschützt zu bekommen, unter den Begriff des »Privatlebens« fällt und Art. 8 EMRK daher auf diese Beschwerde anwendbar ist.

3. Beachtung von Art. 8 EMRK

a. Lag ein Eingriff vor?

(120) Angesichts der obigen Schlussfolgerung, dass im vorliegenden Fall das Recht des Bf. auf Achtung seines Privatlebens nach Art. 8 Abs. 1 EMRK zur Anwendung kommt, erachtet der GH es weiter für erwiesen, dass die Anfrage an den IDA durch die Polizei und die Verwendung der Teilnehmerinformationen durch diese, die zur Identifikation des Bf. führten, einen Eingriff in dieses Recht begründeten. Angesichts des Vorgesagten hält er es nicht für notwendig zu entscheiden, ob die fragliche Maßnahme auch einen Eingriff in das Recht des Bf. auf Achtung seiner Korrespondenz darstellte.

b. War der Eingriff gesetzlich vorgesehen?

(124) Unter der Annahme, dass die Erlangung der Teilnehmerinformationen in Verbindung mit der fraglichen dynamischen IP-Adresse durch die Polizei eine Grundlage im innerstaatlichen Recht hatte, weil § 149b Abs. 3 der StPO vorsah, dass die Polizei vom IDA Informationen über den Eigentümer oder Nutzer bestimmter Mittel zur elektronischen Kommunikation erlangen konnte, muss der GH im vorliegenden Fall prüfen, ob diese Bestimmung zugänglich, vorhersehbar und mit der Rechtsstaatlichkeit vereinbar war.

(125) Er hält fest, dass der vorliegende Fall keine Frage im Hinblick auf die Zugänglichkeit des Rechts aufwirft. Zu den übrigen Erfordernissen wiederholt der GH, dass eine Bestimmung »vorhersehbar« ist, wenn sie ausreichend präzise definiert ist, um es einem Individuum zu ermöglichen – und sei es unter Einholung eines angemessenen Rates –, sein Verhalten zu regulieren […]. Die Vereinbarkeit mit der Rechtsstaatlichkeit verlangt zudem, dass das innerstaatliche Recht einen angemessenen Schutz gegen willkürliche Eingriffe in Rechte nach Art. 8 EMRK vorsieht. Der GH muss daher auch überzeugt sein, dass angemessene und wirksame Garantien gegen Missbrauch bestehen. Diese Beurteilung hängt von allen Umständen des Falles ab, wie der Natur, dem Umfang und der Dauer der möglichen Maßnahmen, den Gründen, die für ihre Anordnung verlangt werden, den Behörden, die zuständig sind, um sie zu erlauben, durchzuführen und zu überwachen, und der Art des nach dem nationalen Recht vorgesehenen Rechtsmittels.

(126) Unter Berücksichtigung des speziellen Kontexts des Falles betont der GH, dass die Cybercrime-Konvention[2] die Staaten verpflichtet, den Behörden bei der Bekämpfung von unter anderem Kinderpornographie betreffenden Verbrechen Maßnahmen wie die Echtzeiterfassung von Verkehrsdaten und die Anordnung der Herausgabe verfügbar zu machen. Solche Maßnahmen sind nach Art. 15 dieser Konvention jedoch »Bedingungen und Garantien [des] innerstaatlichen Rechts [der Vertragsparteien] unterworfen« und müssen, »soweit dies in Anbetracht der Art der betreffenden Befugnis oder des betreffenden Verfahrens angebracht ist, unter anderem eine gerichtliche oder sonstige unabhängige Kontrolle, eine Begründung der Anwendung sowie die Begrenzung des Umfangs und der Dauer der Befugnis oder des Verfahrens umfassen«.

(127) Im vorliegenden Fall hält der GH fest, dass § 149b Abs. 3 StPO, auf den sich die innerstaatlichen Behörden stützten, eine Anfrage zu Informationen über den Eigentümer oder Nutzer eines bestimmten Mittels zur elektronischen Kommunikation betraf. Er enthielt keine speziellen Regeln zur Verbindung zwischen der dynamischen IP-Adresse und Teilnehmerinformationen. Der GH bemerkt ferner, dass Art. 37 der Verfassung für jeden Eingriff in die Vertraulichkeit der Kommunikation eine gerichtliche Anordnung verlangte. Zudem sah das Gesetz über die elektronische Kommunikation, das die Geheimhaltung und Vertraulichkeit elektronischer Kommunikation speziell regelte, zur betreffenden Zeit keine Möglichkeit vor, Zugang zu Teilnehmerinformationen und verbundenen Verkehrsdaten zu erlangen und diese für die Zwecke von Strafverfahren zu übermitteln. Es sah vor, dass elektronische Kommunikation einschließlich der verbundenen Verkehrsdaten vertraulich war und als solche durch den IDA geschützt werden musste. Es bestimmte ferner, dass der IDA die Verkehrsdaten nicht an andere übermitteln durfte, außer dies war für die Erbringung des Dienstes notwendig – es sei denn, von der zuständigen Behörde war die rechtmäßige Überwachung der Kommunikation angeordnet worden. Daher war die Gesetzgebung im Hinblick auf das Schutzniveau, welches für die Privatsphäre des Bf. gewährt wurde, zumindest nicht einheitlich.

2 Übereinkommen über Computerkriminalität vom 23.11.2001 (SEV Nr. 185), BGBl. III 2012/140.

(128) Dies vorausgeschickt, würde der GH die Funktion der nationalen Gerichte an sich ziehen, wenn er versuchen würde, eine verbindliche Aussage dahingehend zu treffen, welche Bestimmungen im vorliegenden Fall Vorrang haben hätten sollen. Er muss sich stattdessen der Begründung durch die innerstaatlichen Gerichte zuwenden. In diesem Zusammenhang befand das Verfassungsgericht, dass die »Identität der kommunizierenden Individuen einer der wichtigen Aspekte der Vertraulichkeit der Kommunikation [war]« und ihre Offenlegung nach Art. 37 Abs. 2 der Verfassung eine gerichtliche Anordnung verlangte […]. Genauer gesagt verlangte die Offenlegung von Teilnehmerinformationen in Verbindung mit einer bestimmten dynamischen IP-Adresse nach der Auslegung des Verfassungsgerichts, die mit seiner früheren Rechtsprechung in Einklang stand, wonach die Verkehrsdaten iSd. Definition nach innerstaatlichem Recht unter den Schutz von Art. 37 der Verfassung fielen, grundsätzlich eine gerichtliche Anordnung und konnte nicht durch eine einfache schriftliche Anfrage der Polizei erlangt werden.

(129) Der GH hält fest, dass der einzige Grund für das Verfassungsgericht, die Beschwerde des Bf. abzuweisen – also die Offenlegung der Teilnehmerinformationen ohne eine gerichtliche Anordnung zu billigen –, tatsächlich die Annahme war, der Bf. hätte »auf die berechtigte Erwartung von Privatsphäre verzichtet« […]. Unter Berücksichtigung seiner Feststellungen im Zusammenhang mit der Anwendbarkeit von Art. 8 EMRK erachtet der GH die Position des Verfassungsgerichts in dieser Frage jedoch nicht als mit dem Anwendungsbereich des Rechts auf Privatsphäre nach der Konvention vereinbar. Eingedenk der Feststellung des Verfassungsgerichts, dass die »Identität des kommunizierenden Individuums« in den Anwendungsbereich des Schutzes von Art. 37 der Verfassung fiel, und der Schlussfolgerung des GH, wonach der Bf. eine angemessene Erwartung hatte, dass seine Identität im Hinblick auf seine Online-Aktivität geheim bleiben würde, war im vorliegenden Fall eine gerichtliche Anordnung notwendig. Zudem hinderte das innerstaatliche Recht die Polizei nicht daran, diese einzuholen, berücksichtigt man die Tatsache, dass sie wenige Monate nach der Erlangung der Teilnehmerinformationen, während welcher Zeit im Fall offenkundig keine Ermittlungsschritte gesetzt worden waren, für anscheinend zumindest teilweise gleiche Informationen wie jene, die sich bereits in ihrem Besitz befanden, um eine gerichtliche Anordnung ansuchte und diese auch erhielt. Die Berufung der innerstaatlichen Behörden auf § 149b Abs. 3 StPO war deshalb offensichtlich unangemessen und bot darüber hinaus praktisch keinen Schutz vor einem willkürlichen Eingriff.

(130) In diesem Zusammenhang bemerkt der GH, dass zur betreffenden Zeit keine Bestimmungen existiert zu haben scheinen, welche die Voraussetzungen für die Speicherung von gemäß § 149b Abs. 3 StPO erlangten Daten konkretisierten, und ebensowenig Garantien gegen einen Missbrauch durch Beamte im Verfahren betreffend den Zugang und die Übermittlung solcher Daten. Was Letzteres angeht, hätte die Polizei, die über Informationen betreffend eine spezielle Online-Aktivität verfügte, einen Urheber rein durch ein Ersuchen an den IDA identifizieren können, diese Information zu eruieren. Zudem konnte nicht gezeigt werden, dass zur betreffenden Zeit eine unabhängige Überwachung des Gebrauchs dieser polizeilichen Befugnisse existierte, obwohl diese Befugnisse, so wie sie von den innerstaatlichen Gerichten interpretiert wurden, den IDA dazu zwangen, die gespeicherten Verbindungsdaten abzurufen, und es der Polizei ermöglichten, viele Informationen betreffend Online-Aktivitäten ohne dessen Zustimmung mit einem bestimmten Individuum in Verbindung zu bringen.

(132) In Anbetracht des oben Gesagten ist der GH der Ansicht, dass es den Bestimmungen, auf welche die strittige Maßnahme […] gestützt wurde, und der Art und Weise, wie sie von den innerstaatlichen Gerichten angewendet wurden, an Klarheit fehlte und keine ausreichenden Garantien gegen einen willkürlichen Eingriff in die Rechte nach Art. 8 EMRK geboten wurden.

(133) Unter diesen Umständen befindet der GH, dass der Eingriff in das Recht des Bf. auf Achtung seines Privatlebens nicht wie von Art. 8 Abs. 2 EMRK gefordert »gesetzlich vorgesehen« war. Daher braucht der GH nicht zu prüfen, ob die strittige Maßnahme ein legitimes Ziel verfolgte und verhältnismäßig war.

(134) […] Der GH kommt zum Schluss, dass eine **Verletzung** von **Art. 8 EMRK** erfolgt ist (6:1 Stimmen; *abweichendes Sondervotum von Richter Vehabović; im Ergebnis übereinstimmendes Sondervotum von Richterin Yudkivska, gefolgt von Richter Bošnjak*).

III. Entschädigung nach Art. 41 EMRK

Die Feststellung einer Verletzung stellt für sich eine ausreichende Entschädigung für den vom Bf. erlittenen immateriellen Schaden dar (einstimmig). € 3.522,– für Kosten und Auslagen (6:1 Stimmen).