

**Club Sozialdemokratischer Rechtsanwältinnen
und Rechtsanwälte im BSA**



Stellungnahme zu 325/ME und 326/ME XXV. GP

Nein zu einer sachlich nicht indizierten und vorschnellen Beeinträchtigung der Grundrechte österreichischer BürgerInnen

Der Club Sozialdemokratischer RechtsanwältInnen ist als Sektion der Vereinigung Sozialdemokratischer JuristInnen Teil des Bundes Sozialdemokratischer AkademikerInnen, Intellektueller und KünstlerInnen (BSA). Wir erstatten nachfolgende Stellungnahme zu den Ministerialentwürfen 325/ME und 326/ME XXV. GP aus rechtsanwaltlicher Sicht:

Zusammenfassung

Auf Grundlage der Prinzipien von Gerechtigkeit, Gleichheit, Freiheit, und Solidarität ist uns das Funktionieren des Österreichischen Staatswesens einschließlich der **Gerichtsbarkeit** und einer **effizienten Strafverfolgung** ein wesentliches Anliegen. Dies darf aber nicht auf Kosten der Grundrechte aller österreichischen BürgerInnen gehen.

Die vorliegenden Ministerialentwürfe 325/ME und 326/ME XXV. GP sind unseres Erachtens **als Einheit zu sehen**. Das gemeinsame Thema dieser Entwürfe ist der Ausbau staatlicher Überwachung der österreichischen BürgerInnen einschließlich der Einführung des „**Bundestrojaners“ und der Vorratsdatenspeicherung in neuem Gewand**. Die Ausarbeitung der Entwürfe ist zum Teil sogar bedenklicher, als der letzte Versuch derselben Ministerien in gleicher Richtung, welcher nach dem Begutachtungsverfahren im März 2016 nach zahlreicher Kritik zurückgenommen wurde.¹

Zusammenfassend enthalten beide Entwürfe sachlich nicht gerechtfertigte Grundrechts-eingriffe. Besonders schwer wiegen dabei Eingriffe in die **Sicherheit von Mandanten-Daten bei den österreichischen RechtsanwältInnen**. Menschen, die sich zu einer Beratung an österreichische RechtsanwältInnen wenden, müssen stets sicher sein können, dass diese vertrauliche Kommunikation geschützt bleibt. Es drohen weitere Verurteilungen Österreichs

¹ 192/ME 25. GP

Club Sozialdemokratischer Rechtsanwältinnen und Rechtsanwälte im BSA



vor dem Europäischen Gerichtshof für Menschenrechte (EGMR) wegen Verletzung der Grundrechte seiner BürgerInnen in dieser Hinsicht.²

Die vorliegenden Entwürfe zerstören nicht nur die **Integrität des Anwalts-Mandanten-Verhältnisses**, sondern setzen – in der derzeitigen Fassung – zahllose Unbeteiligte einer Einbeziehung in polizeiliche und strafrechtliche Ermittlungen aus. Durch die Entwürfe wird auch das **Briefgeheimnis** (vgl Art 10 Staatsgrundgesetz, StGG, und Art 8 der Europäischen Menschenrechtskonvention, EMRK) sowie das Gesetz vom 27.10.1862 zum Schutz des **Hausrechtes** schwer beeinträchtigt. Die Bestimmungen sind dabei teilweise zu unbestimmt, um überhaupt als gesetzliche Ausnahmen Bestand haben zu können.³

Die Notwendigkeit der vorgeschlagenen Grundrechtseingriffe ist auch **nicht objektiv mit statistischen Daten untermauert**. Die Kriminalstatistik und die Statistik des Justizministeriums zeigen, dass Österreich im internationalen Vergleich eine geringe Verbrechensrate mit relativ hoher Aufklärungsquote aufweist. Diese positiven Ergebnisse wurden von den österreichischen Sicherheits- und Justizbehörden mit den derzeit bereits zur Verfügung stehenden Ermittlungsmaßnahmen erzielt.

Engpässe erwiesen sich in der Vergangenheit vorwiegend beim Personal. Dies wird sich durch die gegenständliche Novelle in keiner Weise verbessern. Wenn der Wille besteht, ab 2018 pro Jahr im Schnitt EUR 10 Mio mehr an Mitteln für Justiz und Sicherheit auszugeben, so würde vielmehr die **Einstellung weiterer Ermittlungsbeamter sowie weitere Planstellen in den Kriminalbehörden und der Staatsanwaltschaft** benötigt.

Die Überwachung verschlüsselter Nachrichten in der vorgesehenen Form birgt auch ein **hohes Sicherheitsrisiko**. Die nach den vorliegenden Entwürfen beabsichtigte Art der Überwachung erfolgt im Wege des Hackings privater Computersysteme zur Installation von Schadsoftware. Diese erfordert unabdingbar die Bezahlung von privaten (zumindest dubiosen, wenn nicht kriminellen) Organisationen zum Erwerb von Sicherheitslücken, verbunden mit deren Interesse diese Sicherheitslücken auch offenzuhalten. Beeinträchtigt werden dadurch die wichtigen Cyberkriminalitäts-Initiativen der Bundesregierung.⁴

² EGMR, Wieser und Bicos Beteiligungen GmbH gg. Österreich, Antrag Nr. 74336/01; Robathin gg. Österreich, Antrag Nr. 30457/06

³ zB EGMR, *Sorvistogg. Finnland*, Antrag Nr. 19348/04

⁴ Siehe zB <https://www.onlinesicherheit.gv.at/>

Club Sozialdemokratischer Rechtsanwältinnen und Rechtsanwälte im BSA



Die Entwürfe bewirken somit auch eine **Förderung der Cyberkriminalität**, und damit gerade der einzigen Kriminalitätsform, die in den letzten Jahren ein konstantes Wachstum erlebte.

Wir empfehlen dringend:

- die Gesetzgebungsvorhaben **zurückzustellen**,
- ausgewählte Bereiche erst dann wieder vorzulegen, wenn überhaupt **stichhaltige statistische Daten** über die Notwendigkeit der angedachten Grundrechtseingriffe vorliegen,
- die Ausgestaltung so zu wählen, dass die **Maßnahmen grundrechtskonform** sind und zu keinen weiteren Verfahren vor dem Verfassungsgerichtshof (VfGH) und dem Europäischen Gerichtshof für Menschenrechte (EGMR) führen,⁵
- jede Überwachung erst dann zu ermöglichen, wenn sichergestellt ist, dass auch bei richterlicher Bewilligung technisch **ausschließlich eine spezifische Kommunikationsform** erfasst, nicht eine pauschale elektronische Durchsuchung erlaubt und die Beeinträchtigung Unbeteigter so weit wie möglich vermieden wird,⁶
- jedenfalls **keine routinemäßige und großflächige Speicherung von Überwachungsdaten** aus privater und öffentlicher Video- und/oder Tonüberwachung einzuführen,
- zu gewährleisten, dass die Sicherheitsbehörden bekannt gewordene **Sicherheitslücken umgehend schließen** bzw deren Schließung veranlassen und keine staatlichen Gelder in Kanäle fließen, die – wenn auch nur mittelbar – die Cyberkriminalität fördern,
- und nicht zuletzt das **Anwaltsgeheimnis und das Anwalts-Mandanten-Verhältnis ohne Vorbehalte zu schützen**.⁷

⁵ Vgl bisher EGMR, Wieser und Bicos Beteiligungen GmbH gg. Österreich, Antrag Nr. 74336/01; Robathin gg. Österreich, Antrag Nr. 30457/06

⁶Vgl EGMR, *Iliya Steffanov gg. Bulgarien*, Antrag Nr. 65755/01; *Robathin gg. Österreich*, Antrag Nr. 30457/06

⁷ § 9 Abs 2 und 3 Rechtsanwaltsordnung (RAO), §§ 144, 157 Strafprozeßordnung (StPO)

Detailanalyse

Sicherheitspolizeigesetz (SPG, inkl Sicherheitsforen):

Der Entwurf enthält für die neu eingefügten polizeilichen Befugnisse überhaupt keine entsprechenden Rechtsschutzmaßnahmen. Vollkommen abzulehnen ist auch die Errichtung von Sicherheitsforen (§ 56 SPG-neu), welche ohne Publizitätsbestimmungen die Einrichtung von geschlossenen und vertraulichen Gremien ermöglicht, die sowohl bei eigentlich polizeilichen Sicherheitsaufgaben bis hin zu simplen Streitschlichtungen ohne Wissen und Willen der betroffenen BürgerInnen mit deren personenbezogenen Daten versorgt werden. Der Entwurf sieht keinerlei demokratische Legitimierung dieser Gremien vor. Auch eine spezifische richterliche Kontrolle – über eine Maßnahmenbeschwerde hinaus – ist nicht vorgesehen. Eine Privatisierung von hoheitlichem Handeln außerhalb eines ordentlichen Verfahrens und abseits der kontrollierenden Öffentlichkeit ist abzulehnen.

§ 53 SPG-neu (Videoüberwachung):

Diese Bestimmung würde den Zugriff auf sämtliche Daten der öffentlichen und privaten Videoüberwachung für die Sicherheitsbehörden eröffnen. Bereits die „*Vorbeugung wahrscheinlicher [sic!] oder Abwehr gefährlicher Angriffe gegen Leben, Gesundheit, sexuelle Integrität und Selbstbestimmung, Freiheit oder Vermögen, der Abwehr krimineller Verbindungen*“ sei ausreichend für die Sicherheitsbehörden, um die entsprechenden Daten, quasi auf Zuruf, zu erhalten. Dies entspricht in keiner Weise den geltenden Grundrechtsstandards.

§ 54 SPG-neu und § 99 Telekommunikationsgesetz-neu (TKG-neu, verpflichtende Datenaufbewahrung):

§ 54 Abs 4b SPG-neu ermöglicht die *de facto* uneingeschränkte Nutzung der Daten von Section Control und Verkehrsüberwachung für die Sicherheitsbehörden. Auch hier zeigt sich deutlich, dass die regelmäßig von Datenschützern geäußerten Bedenken, dass bereits die Erlaubnis der Sammlung von Daten in der Folge auch zu einer weitergehenden Verwendung der Daten führt, mehr als berechtigt sind. Bei Einführung der Section Control wurde mehrfach zugesichert, dass diese Daten ausschließlich für die Einhaltung der Höchstgeschwindigkeit verwendet würden, nunmehr sollen diese Daten ebenfalls für die „Abwehr und Aufklärung gefährlicher Angriffe“ verwendet werden dürfen, was in Wahrheit kaum eine Einschränkung bedeutet. Neben der Tatsache, dass dieser Eingriff daher abzulehnen ist, kann dies als warnendes Beispiel für alle

Club Sozialdemokratischer Rechtsanwältinnen und Rechtsanwälte im BSA



weiteren versuchten schrittweisen Grundrechtseinschränkungen in dem Gesetzesvorhaben gelten.

Durch § 99 TKG-neu wird über die Hintertüre der Ausnahme der Löschungsverpflichtung die Vorratsdatenspeicherung wiedereingeführt. Die entsprechenden Regelungen wecken aber dieselben Bedenken, wie dies bereits bei den durch den VfGH aufgehobenen Bestimmungen schon der Fall war.⁸

§ 134 StPO-neu (pauschale Erfassung jeglicher Datenübertragung)

Es wäre zu begrüßen, wenn tatsächlich eine vom TKG losgelöste und klar eingegrenzte Begriffsdefinition des Terminus „Überwachung von Nachrichten“ geschaffen würde. Dies erfolgt aber gerade nicht. Unter „Überwachung von Nachrichten“ fällt nach den vorgeschlagenen Begriffsdefinitionen nämlich nicht mehr bloß die Ermittlung des Inhalts konkreter Kommunikationsvorgänge im klassischen Sinne, sondern die Übertragung jeglicher Informationen in jeder beliebigen elektronischen Form, also Inhalte von Homepages, Beiträge in Newsgroups, Informationen über Bestellvorgänge, aber auch selbst der Vorgang des Speicherns von allgemeinen Daten auf einem externen Server (i.e. „Cloud“). Dass dies beabsichtigt ist, wird in den erläuternden Bemerkungen auch zugestanden.⁹

Die Überwachung sowohl unverschlüsselter als auch verschlüsselter „Nachrichten“ nähert sich daher in Wahrheit der elektronischen Durchsuchung an, ohne dass dies den BürgerInnen im Gesetzestext selbst zugänglich gemacht würde. Der juristische Laie versteht unter Terminus „Nachricht“ wohl etwas deutlich enger Gefasstes. Eine umfassende elektronische Durchsuchung, in der vorgesehenen Form ist auch eine Verletzung des Art 8 EMRK. Der Entwurf ist in diesem Punkt nicht einmal ausreichend klar und vorhersehbar, um überhaupt als zulässige gesetzliche Ausnahme in Betracht zu kommen.¹⁰ Im Zweifel ist die bisherige Formulierung beizubehalten.

Die im Entwurf gewählte schwammige Formulierung mag ihren Grund darin haben, dass die technische Möglichkeit einer grundrechtskonformen Überwachung zweifelhaft ist. ZB wurde in Deutschland bereits 2007/2008 das in manchen Punkten vergleichbare Verfassungsschutzgesetz Nordrhein-Westfalen (VSG NRW) vom deutschen Bundesverfassungsgericht

⁸ VfGH G 47/2012 ua

⁹ zu Z 10, 11, 16, 25 und 26 der Erl

¹⁰ zB EGMR, *Sorvistogg. Finnland*, Antrag Nr. 19348/04

Club Sozialdemokratischer Rechtsanwältinnen und Rechtsanwälte im BSA



(BVerfG) überprüft.¹¹ Dabei beschäftigte sich das BVerfG mit der Online-Durchsuchung. Expertenstellungen dort und auch solche aus jüngster Vergangenheit kamen dabei zum Ergebnis, dass es technisch nicht möglich ist, eine Software, die nur auf laufende Kommunikation zugreift, zu erstellen. Mit ihr ist es immer auch möglich, auf andere Daten zuzugreifen.¹² Selbst wenn sich die im Entwurf vorgesehene Maßnahme daher juristisch von einer "*Online-Durchsuchung abgrenzen*"¹³ lässt, ist eine solche Trennung technisch nicht möglich. Das hohe Missbrauchspotenzial, das mit der Online-Durchsuchung einhergeht, wird daher auch bei den geplanten Maßnahmen vorliegen.

Ist eine grundrechtskonform eingegrenzte Nachrichtenüberwachung technisch nicht möglich, so hat diese bis zur Weiterentwicklung der technischen Möglichkeiten zu unterbleiben. Nicht die Grundrechte sind staatlichen Begehrlichkeiten anzupassen, sondern staatliche Eingriffe haben sich im Rahmen der Grundrechte zu halten.

§ 135 und 137 StPO-neu (Briefgeheimnis)

Mit der Bestimmung des § 135 Abs 1 StPO-neu würde das Briefgeheimnis weitgehend aufgehoben. Es entfällt die Voraussetzung der Haft bzw des Haftbefehls für die Beschlagnahme von Postsendungen, ohne dass aber besondere sonstige Voraussetzungen zumindest in jenem Umfang eingeführt werden, wie sie bisher bei der Nachrichtenüberwachung bestanden (§ 136 StPO). Die Öffnung von Briefen und Postsendungen steht daher in Zukunft gänzlich im Ermessen der Behörden. Allein aufgrund des Vorbringens der erläuternden Bemerkungen, wonach es „in der Praxis immer wieder vorkommt „dass zB Suchtmittel im Wege von Brief- oder Postsendungen zugestellt werden“¹⁴, ist ein Eingriff in dieser Art und Schwere in keiner Weise zu rechtfertigen.

Die vorgeschlagene Fassung verletzt mit hoher Wahrscheinlichkeit Art 10 Staatsgrundgesetz (StGG) und Art 8 der Europäischen Menschenrechtskonvention (EMRK). Die letztgenannte Bestimmung schützt dabei neben dem Briefgeheimnis im engeren Sinne auch den Anspruch

¹¹ BVerfG 1 BvR 370/07 und 1 BvR 595/07

¹² Freiling, Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07, 27.9.2007, S. 6; Bogk, Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07, 23.9.2007, S. 13-15. Siehe auch jüngst Chaos Computer Club, Stellungnahme zur „Quellen-TKÜ“, 9.8.2016. Vgl dazu ausführlich auch Pichler, Online Durchsuchung in junger Prozessrechtswissenschaftler (2018, in Druck).

¹³ Erl 325/ME 2

¹⁴ Z 13der ErlB

Club Sozialdemokratischer Rechtsanwältinnen und Rechtsanwälte im BSA



auf Achtung des Privatlebens als Schutz vor Zugriff auf sonstige Gegenstände. Mit anderen Worten wird durch das Recht auf Achtung des Privatlebens nach Art 8 Abs 1 EMRK ein umfangreiches informationelles Selbstbestimmungsrecht und ein Recht auf Freiheit von Datensammlungen gesichert, wenn eine besondere Nähe zum privaten oder familiären Lebensbereich besteht und es sich um staatliche Eingriffe handelt.¹⁵ Zwar können Maßnahmen mit dem Ziel einer späteren Strafverfolgung gerechtfertigt sein, dabei muss aber die Verhältnismäßigkeit gewahrt bleiben.

Aus anwaltlicher Sicht wird dies dadurch verschlimmert, dass durch den Fall des § 137 Abs 2 StPO die Versiegelung anwaltlicher Korrespondenzstücke und der Widerspruch gegen deren Beschlagnahme nicht mehr möglich sind. Geradezu zynisch sind die Hinweise in den erläuternden Bemerkungen zu diesem Punkt, dass ohnedies die Strafverfolgungsbehörde den Inhalt der Schriftstücke prüft und nur aktenrelevante Schriftstücke zum Akt nimmt bzw selbst anwaltliche Schriftstücke vor der Hauptverhandlung aussortiert.¹⁶ Gerade vor derartigen Eingriffen soll das Recht der anwaltlichen Verschwiegenheit schützen. Es ist hier klar zu sagen, dass in Zukunft jeder brieflich erteilte anwaltliche Ratschlag den Ermittlungsbehörden zur Kenntnis gelangen könnte.

§ 135a StPO-neu (Überwachung verschlüsselter Nachrichten)

Entsprechend der oben diskutierten Definition von „Nachrichten“ ist auch mit verschlüsselten Nachrichten (in diesem Sinne irreführend) jede Form der Datenübertragung gleich zu welchem Zweck erfasst und einer elektronischen Durchsuchung angenähert. Es gelten dieselben Bedenken. Verstärkt werden diese Bedenken, durch die ausdrücklich im Gesetzesentwurf genannten Mittel der Überwachung.

Der Kreis der in die Überwachung einzubeziehenden Personen wird zunächst weit über den unter Verdacht stehenden Täterkreis hinaus erweitert. Ausreichend ist, dass der Verdächtige mit einem fremden Computer „eine Verbindung“ herstellen werde können (das sind daher alle Verwandten, Bekannten, Freunde, Dienstgeber, Dienstnehmer, Geschäftspartner etc. des Verdächtigen).

¹⁵ Brunst, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen (Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht 2009) 288; Wildhaber, in: IntKomm EMRK, Art 8 Rn 336

¹⁶ zu Z 19 und 24 der ErlB

Club Sozialdemokratischer Rechtsanwältinnen und Rechtsanwälte im BSA



Im Grunde wird dabei die Installation einer Schadsoftware in einem privaten Computersystem (sohin eines „Bundestrojaners“) erlaubt. Die Methode der Überwachung ist nicht eingeschränkt, sodass insbesondere auch generelle Aufzeichnungsmethoden, zum Beispiel Keylogger, als zulässig erscheinen würden. Es ist nach dem Entwurf daher in keiner Weise sichergestellt, dass eine Maßnahme immer ausschließlich für eine bestimmte elektronische Kommunikationsform (Programm) angeordnet wird. Dies wäre allerdings unabdingbare Voraussetzung, um die Ermittlungsmaßnahmen überhaupt grundrechtskonform zu machen. Der Entwurf verwirklicht vielmehr die oben bereits beschriebene Gefahr einer pauschalen elektronischen Durchsuchung. Besonders besorgniserregend sind nach der Rechtsprechung des EGMR Maßnahmen, welche den Exekutivbeamten entweder ein weites Ermessen in der Durchführung zugestehen¹⁷ oder sachlich nicht begrenzte Sicherstellungen im großen Umfang bzw hinsichtlich ganzer EDV-Systeme anordnen¹⁸.

Zusätzlich ermöglicht der Entwurf das Eindringen in eine Wohnung oder in andere durch das Hausrecht geschützte Räumlichkeiten zur Installation des „Bundestrojaners“ und dies sogar mit Durchsuchung von Behältnissen und Überwindung spezifischer Sicherheitsvorkehrungen! Dies geht sogar über die bisherigen Bestimmungen der optischen und akustischen Überwachung nach § 136 StGB weit hinaus. Hinzu tritt, dass diese Maßnahmen betreffend verschlüsselter Informationen – in einem groben Wertungswiderspruch im Vergleich zur optischen und akustischen Überwachung – nicht erst bei schweren Straftaten mit mehr als zehn Jahren Freiheitsstrafe zulässig sein sollen, sondern für jedes beliebige Schöffenvorfahren, sohin im Regelfall für Straftaten ab fünf Jahren Freiheitsstrafe. Mit dem Entwurf findet eine materielle Aushöhlung des Gesetzes vom 27.10.1862 zum Schutz des Hausrechtes und Art 8 EMRK statt und sind die vorgesehenen Befugnisse weit überschießend und eines Rechtsstaates europäischer Prägung unwürdig.

Berührt eine derartige Überwachung den Lebens- und Arbeitsbereich eines Rechtsanwalts, werden diese Probleme noch potenziert. In einer Anwaltskanzlei, bzw in der EDV-Einrichtung einer Anwaltskanzlei selbst, werden üblicherweise eine Vielzahl von Akten verwahrt. Neben der Frage, ob Aktenstücke eines konkreten Mandates sichergestellt werden dürfen, stellt sich daher immer die Frage des Schutzes des Eingriffes in Angelegenheiten unbeteiligter Mandanten. Es ist daher bei der Überwachung verschlüsselter Nachrichten in der

¹⁷ EGMR, Niemitz gg. Deutschland, Antrag Nr. 13710/88; Yuditskaya ua gg. Russland, Antrag Nr. 5678/06

¹⁸ EGMR, Iliya Steffanov gg. Bulgarien, Antrag Nr. 65755/01; Robathin gg. Österreich, Antrag Nr. 30457/06

Club Sozialdemokratischer Rechtsanwältinnen und Rechtsanwälte im BSA



vorgeschlagenen weiten Form kein Anwendungsfall denkbar, in welchem ein im Gesetz vorgesehenes unüberwachtes Eindringen in eine Anwaltskanzlei und deren EDV-System als zulässig angesehen werden könnte. Die Anwendung derartiger Maßnahmen ist daher für den Fall der Rechtsanwälte vollständig auszuschließen; ein Verweis auf das Umgehungsverbot nach § 144 StPO ist unzureichend.

§§ 144 und 145 StPO-neu (Rechtsschutz der anwaltlichen Verschwiegenheit)

Der Schutz der anwaltlichen Verschwiegenheit ist nicht bloß in § 9 Abs 2 und 3 RAO gewährleistet, sondern ist auch Teil des Grundrechts des Art 8 Abs 1 EMRK.¹⁹ Bereits in der Vergangenheit hat die Ausgestaltung der weiten Ermittlungsmöglichkeiten nach der StPO insbesondere hinsichtlich der Sicherstellung elektronischer Daten im Anwaltsbereich zu Verurteilungen der Republik Österreich vor dem EGMR geführt.²⁰ Eine Beeinträchtigung der anwaltlichen Verschwiegenheit beeinträchtigt auch das Funktionieren des Rechtsstaates im Sinne des Art 6 EMRK.²¹ Bei einem Eingriff in eine Rechtsanwaltskanzlei ist die Anwesenheit eines unabhängigen Beobachters notwendig, wobei der EGMR in der Vergangenheit stets betreffend Österreich die Anwesenheit eines Vertreters der Rechtsanwaltskammer als positiv angesehen hat.²²

Hinsichtlich der über die formale Hausdurchsuchung hinausgehenden Ermittlungsmaßnahmen war schon bisher der Schutz der anwaltlichen Verschwiegenheit mangelhaft. Nur bei einer gewöhnlichen Hausdurchsuchung ist ein Schutz unbeteiligter Mandanten insoweit gegeben, als neben dem vertretenen Rechtsanwalt auch ein Vertreter der zuständigen Rechtsanwaltskammer Kenntnis von der Maßnahme hat und zur Durchsuchung beigezogen wird. Bereits in der bisherigen Form der optischen und akustischen Überwachung nach § 136 StPO sehen wir den Rechtsschutz durch den Rechtsschutzbeauftragten nach § 91a SPG unzureichend.

¹⁹ EGMR, *Niemitz gg. Deutschland*, Antrag Nr. 13710/88; *Robathin gg. Österreich*, Antrag Nr. 30457/06; *Iliya Steffanov gg. Bulgarien*, Antrag Nr. 65755/01; uva

²⁰ EGMR, Wieser und Bicos Beteiligungen GmbH gg. Österreich, Antrag Nr. 74336/01; Robathin gg. Österreich, Antrag Nr. 30457/06

²¹ vgl bereits EGMR, *Niemitz gg. Deutschland*, Antrag Nr. 13710/88 zur Bedeutung der rechtanwaltlichen Verschwiegenheit

²² EGMR, Wieser und Bicos Beteiligungen GmbH gg. Österreich, Antrag Nr. 74336/01; Robathin gg. Österreich, Antrag Nr. 30457/06

**Club Sozialdemokratischer Rechtsanwältinnen
und Rechtsanwälte im BSA**

Erschwerend tritt hinzu, dass der Rechtsschutzbeauftragte gemäß § 147 Abs 3a StPO-neu der Ermittlung nicht zwingend beizuziehen ist, sondern ihm bloß „Gelegenheit zu geben“ ist, sich einen persönlichen Eindruck zu verschaffen. Zu allem Überfluss sieht keiner der vorliegenden Gesetzesentwürfe eine höhere finanzielle Dotierung des Rechtsschutzbeauftragten für den durch diese Novelle verursachten Mehraufwand vor. Es wird daher zu erwarten sein, dass der Rechtsschutzbeauftragte angesichts des vermehrten Aktenaufwandes eine sorgfältige Prüfung der Maßnahmen nicht mehr gewährleisten kann oder generell überfordert wäre.