Tagungsbericht: Drittes Trierer Forum zum Recht der Inneren Sicherheit

Strafverfolgung im digitalen Zeitalter

Von Ass. iur. **Georg Köpferl**, München/Berkeley

Bereits zum dritten Mal veranstaltete das Institut für Deutsches und Europäisches Strafprozessrecht und Polizeirecht der Universität Trier (ISP) in Kooperation mit dem Landeskriminalamt Rheinland-Pfalz das „Trierer Forum zum Recht der Inneren Sicherheit" (TRIFORIS). In diesem Jahr kamen am 17. Juni 2015 in der Staatskanzlei Rheinland-Pfalz rund 150 Teilnehmer aus Wissenschaft und Praxis zusammen, um unter dem Tagungsthema „Strafverfolgung im digitalen Zeitalter" die Herausforderungen und Gefahren der „mit moderner Infrastruktur agierenden Kriminalitätsstrukturen" zu diskutieren. Die Aktualität dieses Themas wurde dabei erst wenige Tage zuvor durch die Aufdeckung des Angriffs auf das Datennetz des Deutschen Bundestages dokumentiert.

Nach Grußworten von *Randolf Stich* (Ministerialdirektor im Ministerium des Innern, für Sport und Infrastruktur des Landes Rheinland-Pfalz), *Dr. Jürgen Brauer* (Generalstaatsanwalt, Koblenz) und *Johannes Kunz* (Leiter des Landeskriminalamtes Rheinland-Pfalz), in denen die Herausforderungen des digitalen Zeitalters für eine effektive Strafverfolgung beschworen wurden, führte Prof. *Dr. Mark A. Zöller* (Trier) in das Tagungsthema ein. Hierbei wies er einerseits auf die zweistelligen Zuwachsraten im Bereich der „Cybercrimes" hin, die die enorme Herausforderung für die Strafverfolgungsbehörden dokumentierten, andererseits warnte er aber auch vor einer Verschiebung der sensiblen Balance zwischen Freiheit und Sicherheit durch neue Ermittlungsmethoden.

Die Vormittagssitzung eröffnete sodann der ehemalige Präsident des Bundeskriminalamtes *Jörg Ziercke* mit dem Vortrag „Vorratsdatenspeicherung – eine unendliche Geschichte". *Ziercke* malte zunächst ein düsteres Bild: Ohne effektive Überwachung bestehe die Gefahr, dass das Internet zum rechtsfreien Raum werde und damit das staatliche Gewaltmonopol partiell aufgegeben werde. Zur Illustration verwies *Ziercke* auf zwei Beispiele. So sei in 60 % der Fälle von Kinderpornographie eine Speicherung der Verkehrsdaten von mindestens sechs Monaten notwendig, damit überhaupt eine Chance bestehe, die Täter zu ermitteln. Mit gewisser Verwunderung wurde das zweite Beispiel *Zierckes* von einigen Tagungsteilnehmern aufgenommen: So hätte die Verkehrsdatenspeicherung auch zur Aufdeckung des Kommunikationsnetzes des Nationalsozialistischen Untergrundes (NSU) beitragen können. In der Diskussion wurde anschließend auch bezweifelt, ob ausgerechnet vermeintlich fehlende kriminalistische Mittel Ursache für die Schwierigkeiten bei der Aufdeckung des Unterstützernetzwerks seien. Auf der anderen Seite betonte *Ziercke* im Hinblick auf die verfassungsrechtlich garantierten Freiheitsrechte, dass eine wirksame Strafverfolgung und Gefahrenabwehr eben nicht per se eine Gefahr für die Freiheit der Bürger darstelle. In 90 % der Fälle betreffe die Abfrage von Telekommunikationsverkehrsdaten ohnehin nur die Identifizierung des Nutzers einer IP-Adresse und bei den Verkehrsdaten handele es sich nur um Meta- und nicht um Inhaltsdaten. *Ziercke* wies darauf hin, dass das Bundesverfassungsgericht – auf die Rechtsprechung des Europäischen Gerichtshofs ging *Ziercke* nicht ein – die Vorratsdatenspeicherung grundsätzlich als zulässiges Mittel der Strafverfolgung und Gefahrenabwehr anerkannt und dem Gesetzgeber eine „Gebrauchsanleitung" für die verfassungskonforme Ausgestaltung in das Urteil geschrieben habe. Vor diesem Hintergrund sei jedenfalls die geplante Regelung mit dem Grundgesetz vereinbar. Im Gegenteil sei insbesondere im Hinblick auf den Straftatenkatalog die Regelung des § 100g StPO nach der Auffassung *Zierckes* zu restriktiv. Auch wenn eine verfassungskonforme Regelung möglich sei, müsse man den Einsatz einer Ermittlungsmethode aber insbesondere dann überdenken, wenn der nahezu flächendeckende Grundrechtseingriff nur wenig Nutzen für die Strafverfolgung liefere, was *B. Gercke* mit dem Hinweis auf den fehlenden empirischen Nachweis für die Notwendigkeit der Wiedereinführung der Vorratsdatenspeicherung in die Diskussion einbrachte. Die für die nach Einführung der Vorratsdatenspeicherung errechnete Erhöhung der Aufklärungsquote um 0,006 %, die in diesem Zusammenhang immer wieder genannt wird und die auch *B. Gercke* dem Referenten vorhielt, tat *Ziercke* allerdings als „Statistik-Klamotte" ab. Zweifel an der Wirksamkeit der Vorratsdatenspeicherung kamen aber auch deshalb auf, weil *Ziercke* selbst ausdrücklich eingestand, dass professionelle Täter aufgrund des Einsatzes von Anonymisierungsprogrammen für die Strafverfolgungsbehörden nur schwer zu ermitteln seien. Darüber hinaus meldete *B. Gercke* in der Diskussion verfassungsrechtliche Bedenken im Hinblick auf die weiterhin ungeklärte Frage der Datensicherheit an – ein zentraler Argumentationstopos im Urteil des Bundesverfassungsgerichts. Eine Auffassung, die auch *M. Gercke* in der Diskussion zu seinem Vortrag teilte, da auch das neue IT-Sicherheitsgesetz, dessen Regelungen er als „butterweich" qualifizierte, eine ausreichende Datensicherheit nicht gewährleisten würde.

Im Anschluss an *Ziercke* referierte Prof. *Dr. Marco Gercke* (Köln) über „Neue Herausforderungen für das Sicherheitsrecht durch die Informationstechnologie". *M. Gercke* erläuterte zunächst den Hintergrund, vor dem er diese Herausforderungen betrachten wollte, indem er auf den durch die Cyberkriminalität verursachten immensen Schaden einging. Dieser liege zwar laut PKS in Deutschland lediglich bei 50 Mio. Euro im Jahr, er werde anderenorts aber realistischer mit 1,6 % des Bruttoinlandsproduktes angegeben (so die von McAfee in Auftrag gegebene Studie „Net Losses – Estimating the Global Cost of Cybercrime"). Zu erklären sei das nur mit der sehr geringen Anzeigebereitschaft der Geschädigten. Die Einschaltung der Polizei werde meist als letztes Reaktionsinstrument angesehen. Da verwundere es nicht, dass die Unternehmensberatungen derzeit gewaltig in ihre Forensikabteilungen investierten. Als die eigentliche Herausforderung für das sicherheitsrecht benannte *M. Gercke* dann aber den Gesetzgeber. Ein besonderes Übel sei nämlich die schlechte Qualität der Gesetze gerade auch im Bereich der Cybercrime-Bekämpfung. Nach *M. Gercke* liege dies

nicht nur an fehlenden handwerklichen Fertigkeiten in der Ministerialbürokratie, sondern es mangele beim Gesetzgeber oft schon am Interesse, handwerklich einwandfreie Gesetze zu schaffen. Dem Gesetzgeber attestierte er zudem eine gewisse Beratungsresistenz. Es fehle meist an einer ausgearbeiteten Strategie, die in eine entsprechende Politik münde, die wiederum zur Gestaltung entsprechender Gesetze führe. In der Diskussion spitzte *M. Gercke* sein Kritik dann noch zu, indem er behauptete, dass beim Gesetzgeber keine Bereitschaft zu erkennen sei, dogmatische Strukturen zu achten. *M. Gercke* exemplifizierte seine Kritik anhand einiger Beispiele: Bei der Vorratsdatenspeicherung habe man sich nach jahrelanger Kontroverse zur Einführung durchgerungen, ohne dass man über deren Nutzen, den *M. Gercke* angesichts der Anonymisierungsmöglichkeiten selbst für gering hält, wirklich diskutiert habe. Darüber hinaus seien wichtige Bereiche durch das Strafrecht nicht abgedeckt, allem voran der Identitätsdiebstahl. Schließlich würden europäische Vorgaben zum Teil „katastrophal" oder verspätet umgesetzt. Auch *Zöller* stimmte in der Diskussion diesem Befund prinzipiell zu. Ihm blieb lediglich zusammenzufassen: „Wir können und wollen uns die Zeit für gute Gesetze nicht mehr nehmen." Da war ob dieser zum Teil doch scharfen Kritik im Auditorium gar von „Politik-Bashing" die Rede.

Mit einer aktuellen Entwicklung im Bereich der Telekommunikationsüberwachung beschäftigte sich Prof. *Dr. Fredrik Roggan* (Oranienburg) in seinem Vortrag „Das Verbot der ‚Gesetzgebung auf Vorrat' und seine Folgen für die Quellen-TKÜ". *Roggan* stellte zunächst den Streitstand im Hinblick auf die Zulässigkeit der Quellen-TKÜ nach der StPO dar, die insbesondere von Kommentatoren aus der Praxis als von der Rechtsgrundlage des § 100a StPO gedeckt angesehen wird. Kritisch sieht *Roggan* dabei, dass § 100a StPO als „technikoffen" verstanden wird, denn die Technikoffenheit sei in der Strafprozessrechtswissenschaft kein gängiger Argumentationstopos. Ein neues Licht auf diese Auslegung des § 100a StPO werfe das Urteil des Landesverfassungsgerichts Sachsen-Anhalt vom 11.11.2014 (Az. LVG 9/13). Darin hat das Landesverfassungsgericht § 17c des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA), der die Quellen-TKÜ zur Gefahrenabwehr ermöglicht, für verfassungswidrig und nichtig erklärt. Das Landesverfassungsgericht vertritt die Auffassung, dass der Gesetzgeber mit dem Schutz von Leib, Leben oder Freiheit einer Person in Fällen einer gegenwärtigen Gefahr zwar einen legitimen und ausreichend gewichtigen Zweck verfolge, dennoch sei die Regelung unverhältnismäßig. Denn der Gesetzgeber habe keine verantwortliche Abwägungsentscheidung getroffen, weil es noch keine technischen Mittel gebe, um die Norm umzusetzen. Der Gesetzgeber habe demnach die Polizei zu Maßnahmen und zum Einsatz von technischen Instrumenten ermächtigt, die er noch gar nicht kennen und bewerten konnte. Eine – in den Worten *Roggans* – „Gesetzgebung auf Vorrat" sei damit unzulässig. Daraus zog *Roggan* den Schluss, dass auch eine Ermächtigungsgrundlage für die Quellen-TKÜ in der StPO erst dann geschaffen werden könne, wenn ein entsprechendes technisches Mittel vorhanden sei, das der Gesetzgeber bewerten könne. Damit sei es auch nicht möglich, Ermächtigungsgrundlagen der StPO als „technikoffen" zu interpretieren. Hiergegen erhob *Bär* in seinem späteren Vortrag Einspruch. Seiner Auffassung nach sei das Verhältnis genau anders herum: Der Gesetzgeber habe eine Regelung zu schaffen auf deren Grundlage dann die entsprechenden technischen Mittel zu beschaffen seien. Auswirkungen könnte die Entscheidung – so *Roggans* Einschätzung – auch auf das beim Bundesverfassungsgericht anhängige Verfahren zu verschiedenen Vorschriften des BKAG – darunter die TKÜ-Regelung in § 20l BKAG – haben. Denn auch bei Schaffung dieser Vorschrift stand noch keine Software zur Realisierung einer Quellen-TKÜ zur Verfügung. Es bleibt damit abzuwarten, ob das Bundesverfassungsgericht die Argumentation des Landesverfassungsgerichts Sachsen-Anhalt aufgreift und seiner Entscheidung zugrundelegt.

Die Nachmittagssitzung eröffnete *Dr. Wolfgang Bär* (München) mit seinem Vortrag „Aktuelle Entwicklungen im Bereich der Internetkriminalität". *Bär* berichtete hier zunächst von organisatorischen Maßnahmen im Bereich der Cybercrime-Verfolgung, bevor er sich Fragen des materiellen und prozessualen Rechts widmete. So sei mit Beginn des Jahres 2015 auch in Bayern eine Zentralstelle zur Bekämpfung von Cybercrime bei der Generalstaatsanwaltschaft Bamberg eingerichtet worden. Wie bereits in anderen Bundesländern werde nun auch in Bayern durch die Schaffung der Zentralstelle juristisches und technisches Fachwissen zur Cybercrime-Bekämpfung zusammengefasst. *Bär* erläuterte daraufhin einige Felder des materiellen Strafrechts, bei denen er einen Handlungsbedarf sieht. Zum einen müsse der Gesetzgeber bei der Bestrafung der Datenhehlerei aktiv werden. Positiv kommentierte er deshalb den Gesetzentwurf für einen neuen § 202d StGB (BR-Drs. 70/14 und 283/13), der diese Strafbarkeitslücke schließen soll. Die Straffreiheit der mit dem Ankauf sog. Steuer-CDs befassten Beamten werde durch die Vorschrift des § 202d Abs. 3 StGB gewährleistet, worauf auch in der Diskussion nochmals eingegangen wurde. Bei den Tatbeständen der §§ 202a ff. StGB und § 303a StGB ist nach der Auffassung *Bärs* die Einführung einer Versuchsstrafbarkeit sowie die Schaffung von Qualifikationstatbeständen notwendig. Nach *Bär* muss die Schaffung von Qualifikationen auch dazu führen, dass diese in den Katalog des § 100a StPO aufgenommen werden, in dem sich derzeit noch keine Straftatbestände aus dem Bereich der Cybercrimes finden. Mit der Verabschiedung des Gesetzentwurfes zur Steuerhehlerei würde diese Forderung *Bärs* erfüllt, denn der Entwurf sieht auch die Einführung von Qualifikationstatbeständen in die §§ 202a, 202b StGB nebst der Aufnahme dieser Tatbestände in die Kataloge der §§ 100a, 100c StPO vor. Darüber hinaus sprach sich *Bär* für eine strafrechtliche Reaktion auf den „Diebstahl von Rechnerleistung" aus, um angemessen auf die Botnetz-Kriminalität reagieren zu können – ein Thema, das auch jüngst Gegenstand der Justizministerkonferenz in Stuttgart war. Im Bereich des Prozessrechts thematisierte *Bär* zunächst die – seiner Auffassung nach problematische – Zweiteilung zwischen TKG und TMG. Die Trennung sei schwer nachvollziehbar, da sie sich nicht sauber vornehmen lasse. Dies habe auch Konsequenzen für den

strafprozessualen Zugriff auf Bestands- und Verkehrsdaten (TKG) und Nutzungsdaten (TMG), da sich die Einzelermächtigungen der StPO ausschließlich auf Telekommunikationsdaten bezögen. Für die Erhebung von Nutzungsdaten blieben deshalb nur §§ 161, 163 StPO. Zudem ging *Bär* auf die „Beschlagnahme" von E-Mail-Kommunikation in der Phase der Zwischenspeicherung ein. Hier entstehe aufgrund der Rechtsprechung des Bundesverfassungsgerichts, das eine Anwendung des § 94 StPO befürworte, das Problem, dass die Maßnahme gegenüber den Betroffenen offen erfolgen müsse. In Bayern wähle man deshalb den Weg über § 99 StPO. Neue prozessrechtliche Fragestellungen hätten sich jüngst im Hinblick auf Beschlagnahme, Sicherstellung und Einziehung von „Bitcoins" ergeben. Hier sei noch weitgehend ungeklärt, wie mit diesem neuen Phänomen rechtlich umzugehen sei. Zuletzt sprach *Bär* einige Probleme bei der Datensicherung in der Cloud an. Zwar sei mit § 110 Abs. 3 StPO eine Grundlage für den Zugriff auf diese Daten vorhanden, allerdings nur, wenn sich der Server im Inland befinde. Im Falle eines Serverstandorts im Ausland stellten sich nicht nur rechtshilferechtliche Fragen, sondern es bestünde teilweise schon das tatsächliche Problem, zu ermitteln, in welchem Staat sich der Server befinde.

Mit der – wohl rhetorischen – Frage, ob ein Strafverteidiger, der bei der Aufklärung „analoger Straftaten" als bremsende Kraft im Strafverfahren wirke, nicht ein Fremdkörper auf einer Tagung sei, bei der die Effektivität der Strafverfolgung im Mittelpunkt stehe, leitete Prof. *Dr. Rainer Hamm* (Frankfurt a. M.) seinen Vortrag „Strafverteidigung im Zeitalter der Informationstechnologie" ein. Im ersten Teil seines Vortrages äußerte *Hamm* Zweifel an dem in der Einladung zur Tagung gebrauchten Begriff von den „Wettbewerbsnachteilen" der Strafverfolgungsbehörden gegenüber den modernen Kriminalitätsstrukturen. Er halte den Idealfall eines „fairen Wettbewerbs" angesichts der technischen Möglichkeiten, die auch den Strafverfolgungsbehörden zur Verfügung stünden, nicht mehr unbedingt für utopisch, denn der Gesetzgeber habe stets dem Wunsch der Strafverfolger nach neuen Ermittlungsmethoden ohne empirischen Nachweis der Geeignetheit und Notwendigkeit nachgegeben. Der umfangreiche Ermächtigungskatalog der Strafprozessordnung, deren Charakter sich seit dem Volkszählungsurteil von der „Magna Charta des Beschuldigten" zum Ermächtigungskatalog für die Strafverfolgungsbehörden gewandelt habe, zeige dies eindrucksvoll. Von der Vorratsdatenspeicherung über die Auslesung von Facebook-Accounts bis zur mit technischen Befunden verbundenen gefährlichen Illusion absoluter Richtigkeit von Ermittlungsergebnissen – die Informationstechnologie werfe zahlreiche neue normative Probleme auf, die es stets kritisch zu hinterfragen gelte. Strafverteidigung im Informationszeitalter bedeute auch, diese Fragen nachdrücklich zu artikulieren und zur Klärung an die Rechtsmittelgerichte heranzutragen. Abschließend widmete sich *Hamm* im zweiten Teil seines Vortrages dem Themenkreis elektronische Akte. Aus der Sicht der Strafverteidigung werde sie insbesondere für die Akteneinsicht Folgen haben. Dabei stellte *Hamm* klar, dass die elektronische Akte auch für den Strafverteidiger alle Vorteile gegenüber einer nur gescannten Papierakte haben, also insbesondere die Möglichkeit der elektronischen Auswertung bieten müsse. Die Akteneinsicht müsse dann an die neue Technik angepasst werden. Für Digitalverweigerer werde es deshalb nicht nur in der Justiz, sondern auch in der Anwaltschaft schwer.

Der letzte Vortrag „Ermittlungen in sozialen Netzwerken" von *Dr. Saleh Ihwas* (Trier), der sich mit dieser Thematik im Rahmen seiner Doktorarbeit auch monographisch beschäftigte (Strafverfolgung in Sozialen Netzwerken, 2014), galt einem Problemfeld, das gerade für die anwesenden Praktiker aus der Strafverfolgung – dies wurde auch durch deren interessierte Fragen dokumentiert – von großer Bedeutung ist. Nach einer kurzen Einführung in die soziale Bedeutung der „sozialen Netzwerke" – in Deutschland gehören 28 Mio. Personen zu den weltweit fast 1,5 Mrd. Facebook-Nutzern – analysierte *Ihwas* exemplarisch zwei Ermittlungsmethoden. Neben der Erhebung öffentlich zugänglicher Daten erläuterte *Ihwas* insbesondere das Problemfeld der virtuell personalen Ermittlungen am Beispiel von Facebook. In diesen Fällen werden durch Ermittler Profile in sozialen Netzwerken angelegt, um mit (mutmaßlichen) Straftätern in Verbindung zu treten, insbesondere um von diesen in die „Freundes"-Liste aufgenommen zu werden, damit die Möglichkeit besteht, auch von nicht öffentlichen Chronik-Einträgen Kenntnis zu nehmen. *Ihwas* sieht hier insbesondere die Schwierigkeit in der Abgrenzung eines „virtuellen nicht offen ermittelnden Polizeibeamten" und eines „virtuellen verdeckten Ermittlers". Während der Einsatz des virtuellen nicht offen ermittelnden Polizeibeamten auf die Ermittlungsgeneralklausel gestützt werden könne, stelle sich beim virtuellen verdeckten Ermittler das Problem der fehlenden Rechtsgrundlage. *Ihwas* arbeitete sodann einen Kriterienkatalog zur Abgrenzung heraus. Da die sozialen Netzwerke die Verwendung von Echtpersonalien förderten – Facebook gibt eine Anmeldequote mit echten Namen von 95 % an –, bestehe in sozialen Netzwerken durchaus ein Vertrauen in die Identität des virtuellen Gegenübers. Die Schutzwürdigkeit des Vertrauens hänge dabei von drei Kriterien ab: von der Aussagekräftigkeit der Freundschaftsanfrage, von der Kontrolle der Anfragen durch den Nutzer sowie vom Umfang der Nutzung der Merkmale zum Identitätsmanagement durch den Ermittler, also der Gestaltung des Ermittlerprofils (Fotos, Kommentarbeiträge etc.). Kann nach diesen Kriterien schutzwürdiges Vertrauen in die Identität des Gegenübers in Anspruch genommen werden, handele es sich nicht mehr nur um einen virtuellen nicht offen ermittelnden Polizeibeamten. *Ihwas* hat damit handfeste und gut nachvollziehbare Kriterien zur Abgrenzung der Ermittlungsmethoden herausgearbeitet, die allerdings von einigen Praktikern als zu restriktiv angesehen wurden.

In einer abschließenden Podiumsdiskussion – unter der Moderation von Prof. *Dr. Björn Gercke* (Köln) – diskutierten die Referenten *Bär*, *M. Gercke*, *Hamm* und *Roggan* sowie der Leiter des LKA Rheinland-Pfalz *Kunz* über „Die dunkle Bedrohung – Fluch oder Segen des Einsatzes von Informationstechnologien im Strafverfahren". Hier standen sich insbesondere das durch *Kunz* geäußerte Bedürfnis nach der offenen Gestaltung von Ermächtigungsnormen und der von Seiten der Wissenschaft und Strafverteidigung erhobene Ein-

wand gegenüber, man müsse gesetzgeberische Entscheidungen, die u.U. zu strafverfolgungsfreien Räumen führten, akzeptieren. Zudem wurde das Problem der durch die neuen Ermittlungsmethoden generierten Datenflut thematisiert, die teilweise nur mittels einer Auswertung durch Privatunternehmen zu bewerkstelligen sei. Während *Bär* keine Alternative zur Zusammenarbeit mit Privaten sah, haben die Vertreter aus Wissenschaft und Strafverteidigung dieses „Outsourcing" und die damit verbundenen Gefahren kritisiert.

Das 3. TRIFORIS gab damit Einblick in neueste Entwicklungen der Strafverfolgung im digitalen Zeitalter und war erneut Plattform für die angestrebte Förderung des Dialogs zwischen Wissenschaft und Praxis, wenngleich auch die Differenzen teilweise deutlich zu Tage traten. Man darf auf das 4. TRIFORIS in zwei Jahren und die damit verbundene Gelegenheit eines erneuten Austausches auf dem Feld des Rechts der inneren Sicherheit gespannt sein.