TAGUNGSBERICHT

Das 7. Forum zum Recht der Inneren Sicherheit (FORIS)

Big Data im Sicherheitsrecht

*von Ruben Doneleit und Isabella Klotz**

Am 15. September 2023 fand zum nunmehr siebten Mal (und erstmals unter neuem Namen[1]) das Forum zum Recht der Inneren Sicherheit (FORIS) in Mainz statt. Die Schirmherrschaft für die Tagung hatte auch in diesem Jahr die rheinland-pfälzische Ministerpräsidentin *Malu Dreyer* übernommen. Tagungsort war deshalb wiederum die am Rhein gelegene Mainzer Staatskanzlei. Dieses Jahr lautete das Thema der vom Institut für Digitalisierung und das Recht der Inneren Sicherheit (IDRIS) der LMU München gemeinsam mit dem Landeskriminalamt Rheinland-Pfalz ausgerichteten Veranstaltung „Big Data im Sicherheitsrecht".

I. Grußwort und Einführung in das Tagungsthema

Zu Beginn richtete *Harald Esseln* (Ministerium des Innern und für Sport Rheinland-Pfalz, Referat Kriminalitätsbekämpfung) ein Grußwort an die Teilnehmer der Tagung. Dabei betonte er, dass Daten die „neue Währung" unserer Zeit seien und Massendaten, sogenannte Big Data, zunehmend auch im Sicherheitsrecht relevant würden. Anschließend führten *Mario Germano* (Präsident des Landeskriminalamtes Rheinland-Pfalz) und *Prof. Dr. Mark A. Zöller* (LMU München) in das Tagungsthema ein. Bereits zu Beginn wurde so deutlich, dass Big Data Wissenschaft und Praxis seit geraumer Zeit gleichermaßen beschäftigen.

II. Erste Sitzung

1. KI – Potentiale und Risiken

Den Auftakt zur ersten Sitzung, moderiert von *Alexander Büchel* (Ministerium des Innern und für Sport Rheinland-Pfalz), machte der Vortrag von *Prof. Dr. Sebastian Vollmer* (Deutsches Forschungszentrum für Künstliche Intelligenz [DFKI], Kaiserslautern). In seiner instruktiven Präsentation erklärte der Spezialist für Data Science und Leiter des gleichnamigen interdisziplinären Forschungsbereichs die Funktionsweisen und tatsächlichen Grenzen von Künstlicher Intelligenz (KI). KI sei ein Werkzeugkasten, der zweifelsfrei Vorteile mit sich bringe, dem zugleich aber auch verschiedene Nachteile immanent seien. Diese Potentiale und Risiken wurden allgemein und speziell für den Bereich der Massendaten an verschiedenen Beispielen erläutert. So bietet das bereits in der Praxis verwendete „supervised learning" die Möglichkeit, zum Beispiel Vorhersagen über Krankenakten bzw. -verläufe zu machen.

Die Ausführungen von *Prof. Dr. Sebastian Vollmer* beschränkten sich aber nicht auf die deutsche Lebenswirklichkeit. Anschaulich wurden auch Anwendungsbeispiele aus den USA, wie das COMPAS-System (Correctional Offender Management Profiling for Alternative Sanctions), erläutert, das dort zur Risikobewertung von Wiederholungstätern eingesetzt wird. Auch wurde die „generative artificial intelligence" vorgestellt, die beispielsweise bei der Wahrscheinlichkeitsermittlung zur Textvervollständigung für Dienste wie „Bing Chat" oder „ChatGPT" Anwendung findet.

Der Vortrag ließ jedoch auch nicht die mit der Anwendung solcher technischen Lösungen einhergehenden Probleme außer Acht. Diese beschränken sich keinesfalls auf rein technische Unsicherheiten, wie etwa Probleme beim Programmierungsablauf oder die Unklarheit, welche Daten für die „Fütterung" der KI verwendet werden, um diese zu trainieren. Da KI-Systeme eigene, nicht vorgegebene Entscheidungen treffen und neue Lösungen antizipieren sollen, stellen sich auch schwierige ethische Fragen, die nicht aus dem Blickfeld geraten dürfen. Eindrückliches Beispiel hierfür ist das zuvor genannte COMPAS-System, bei dem letztlich von menschlicher Seite aus erwogen werden müsse, ob die in der Prognose angelegte Fehleranfälligkeit bestimmter Entscheidungen in Kauf genommen wird. Nicht ohne Grund ist die Anwendung dieses Systems hochumstritten. Im Kern gelte es, einen Ausgleich zwischen der „fairness", das heißt vor allem die weitgehende Vermeidung von Diskriminierung, und möglichen Einbußen an „accuracy", also der Treffsicherheit bzw. Genauigkeit einer KI-Entscheidung, zu finden. Die KI allein könne diesen nicht bieten – ein Konsens diesbezüglich müsse von der Gesellschaft ausgehandelt werden. Zuletzt betonte *Prof. Vollmer*, er glaube zwar fest an das Potenzial von Künstlicher Intelligenz, mithilfe der Auswertung von Massendaten Lösungen für die relevanten Probleme unserer Zeit, etwa den Klimawandel, zu finden. Ihn beunruhige aber das Risiko, dass der Mensch die KI für „schlechte Zwecke" einsetzen könnte.

* Die *Verfasser* sind Wissenschaftliche Mitarbeiter am Lehrstuhl für Deutsches, Europäisches und Internationales Strafrecht und Strafprozessrecht, Wirtschaftsstrafrecht und das Recht der Digitalisierung (*Prof. Dr. Mark A. Zöller*) an der Ludwig-Maximilians-Universität München.

[1] Zuvor firmierte die Veranstaltung als „Trierer Forum zum Recht der Inneren Sicherheit (TRIFORIS)".

2. Die Überwachungsgesamtrechnung

Anschließend referierte *Prof. Dr. Markus Löffelmann* (Hochschule des Bundes für öffentliche Verwaltung, Berlin) über die sogenannte Überwachungsgesamtrechnung. Zunächst zeichnete er dafür die begriffliche und juristische Entstehungsgeschichte dieses Konzepts nach, welches seinen vorläufigen Höhepunkt mit der Aufnahme in den aktuellen Koalitionsvertrag von SPD, Bündnis 90/Die Grünen und FDP auf Bundesebene erreichte. Aus rechtsdogmatischer Sicht greife die Überwachungsgesamtrechnung im Wege einer doppelten Verhältnismäßigkeitsprüfung ein, bei der eine Regelung zunächst für sich genommen verhältnismäßig sein muss, bevor sie im Gesamtkontext der Überwachungsgesamtrechnung in Bezug zu sämtlichen bereits bestehenden (Überwachungs-)Normen gesetzt wird.

Hierbei ergäben sich jedoch verschiedene Probleme. Diese beginnen dem Referenten zufolge bereits mit der Konturierung des Gegenstands einer Überwachungsgesamtrechnung. Fraglich sei, was „Überwachung" überhaupt bedeutet, ob sich diese auf alle Daten oder nur auf Massendaten beziehen kann und ob nur verdeckte oder auch offene Maßnahmen des Staates hiervon erfasst sein sollen. Zudem müsse eine Gewichtung der verschiedenen Überwachungsmaßnahmen erfolgen. Da es hierfür kaum Parameter oder statistische Daten gebe, bereite auch dieser zweite Schritt in der Praxis erhebliche Probleme. Entsprechendes gelte für den „Nutzen" der Überwachung. Gegebenenfalls ließen sich hierfür die Fallzahlen der Polizeilichen Kriminalstatistik oder die der Verurteilungsstatistik heranziehen. Entscheidend sei aber auch, dass zugleich ein individueller Blick auf die Lage des jeweiligen Betroffenen geworfen werde und nicht nur eine rein kumulativ übergeordnete Betrachtung bezogen auf den gesamtgesellschaftlichen Nutzen erfolge.

Besonders problematisch sei im Rahmen einer Überwachungsgesamtrechnung jedoch die Frage, wie die „Verrechnung" von Belastungen und Nutzen zu erfolgen hat. *Prof. Löffelmann* führte dazu aus, dass einerseits häufig eine verfassungsrechtliche Asymmetrie bestehe, da eine Überwachungsmaßnahme für den Betroffenen stets grundrechtsrelevant sei, die Überwachung und ihr Zweck aber nicht zwingend verfassungsrechtlich geschützt sein müsse, da der Gesetzgeber frei in der Schaffung neuer Rechtsgüter ist. Andererseits seien die verschiedenen Rechtsgüter inkommensurabel, da eine vergleichende Gewichtung stets eines Paradigmas bedürfe, welches hierfür bisher nicht existiere. Um der Problematik Herr zu werden, versuche eine Überwachungsgesamtrechnung daher mittels einer normativen Evaluierung eine sachgerechte Lösung zu erzielen. Hierbei werde, anders als beim Überwachungsbarometer des Max-Planck-Instituts[2], eine subjektive Beeinflussung durch die Festlegung der Skalenwerte mit ihrer suggestiven Wirkung und die Gewichtung einzelner Faktoren vermieden.

In der Diskussion im Anschluss an den Vortrag ging es darum, wie eine solche Überwachungsgesamtrechnung vollzogen werden kann. Hierfür wurde eine unabhängige Freiheitskommission vorgeschlagen. Diese sollte aber weniger ein Kontrollgremium im engeren Sinne sein, sondern nur eine beratende Rolle übernehmen. Zudem wurde festgehalten, dass subjektive Einflüsse bei der Gewichtung einzelner Maßnahmen oder Rechtsgüter nie gänzlich ausgeschlossen werden können. Ferner sollte der – bereits weitgehend etablierte – Begriff „Überwachungsgesamtrechnung" in Zukunft überdacht werden, da eine mathematische Addition einzelner Rechte und Beeinträchtigungen nicht möglich sei. Denkbar erscheine die Bezeichnung als „Betrachtung" oder „Evaluation".

3. Die Vorratsdatenspeicherung – eine (un)endliche Geschichte?

Der darauffolgende Vortrag von *Prof. Dr. Jens Puschke, LL.M.* (King´s College) von der Philipps-Universität Marburg befasste sich mit den rechtlichen Entwicklungen rund um das Thema der Vorratsdatenspeicherung. Der Referent eröffnete mit der These, dass die Vorratsdatenspeicherung „noch nicht am Ende sei".

Vorratsdatenspeicherung meint, dass Telekommunikationsdienstleister dazu verpflichtet werden, massenhaft Verkehrs- und Standortdaten anlasslos zu speichern. Dabei wird nicht danach unterschieden, ob die Speicherung für repressives oder präventives Anschlusshandeln erfolgt. Im Mittelpunkt stehe die Information, „wann wer wo mit wem wie lange Kontakt hatte". Eine verfassungs- und unionsrechtskonforme rechtliche Regelung der Vorratsdatenspeicherung sei dem deutschen Gesetzgeber trotz zweier Anläufe bisher allerdings nicht gelungen, was eine „Blamage" darstelle. Nach Ansicht von *Prof. Puschke* sei bei der Konzeption einer gesetzlichen Grundlage zu beachten, dass die Speicherung sensibler Daten schon für sich genommen ein schwerer Grundrechtseingriff ist, der durch den fehlenden Anlass noch verstärkt werde. Den sogenannten „chilling effect", also ein abschreckendes Unsicherheits- und Überwachungsgefühl der Bürger, das dazu führen kann, dass Grundrechte nicht (mehr) ausgeübt werden, gelte es unbedingt zu vermeiden.

Bei den vorangegangenen Regelungsversuchen sei das verfassungsrechtliche Defizit vor allem bei den Regelungen zur Datensicherheit und zu den Abrufmöglichkeiten zu finden gewesen. Es werde auch vertreten, dass die anlasslose Speicherung von Daten stets rechtswidrig sei. Dennoch hatte der Europäische Gerichtshof in seiner jüngsten Entscheidung[3] der Vorratsdatenspeicherung keine vollständige Absage erteilt. Eine solche könne vielmehr in Abhängigkeit von dem betroffenen Rechtsgut und dessen Bedeutung oder bei der Bekämpfung schwerer Kriminalität möglich sein. Hierbei sei aber eine objektive Bestimmung anhand maßstabsbildender Kriterien schwierig. Zudem müsse die Speicherung auf den absolut not-

[2] Abschlussbericht des Max-Planck-Instituts zum Überwachungsbarometer, online abrufbar unter: https://shop.freiheit.org/#!/Publikation/1168 (zuletzt abgerufen am 6.10.2023).

[3] *EuGH*, NJW 2022, 3135 m. Anm. *Graulich* = GRUR-RS 2022, 24116.

wendigen Zeitraum begrenzt werden und eine „intensive Verhältnismäßigkeitsprüfung“ erfolgen.

Auf Basis dieser Erwägungen des *EuGH* wird von Befürwortern des Vorratsdatenspeicherung deren (Wieder-) Einführung vor allem im Bereich der Kinder- und Jugendpornographie gefordert. Eine hierfür vorgesehene Rechtsgrundlage müsste aber den strengen Verhältnismäßigkeitsanforderungen genügen. *Prof. Puschke* betonte in diesem Zusammenhang, dass die gesellschaftliche Forderung höchstens die Erforderlichkeit, jedoch weder die Gebotenheit noch die Angemessenheit zu begründen vermag. Insofern gebe es eine „Schieflage in der öffentlichen Diskussion“.

Der Referent ging auch auf das sogenannte Quick-Freeze-Verfahren als (vermeintlich) mildere Alternative zur Vorratsdatenspeicherung im bisherigen Sinne ein, bei dem die Daten nur kurzfristig gespeichert werden. Eine längere Sicherung mit anschließender Abrufmöglichkeit erfolgt hier nur bei einem bestimmten Anlass, wie einem strafprozessualen Tatverdacht. Eine solche Regelung sei zwar grundrechtsschonender, stehe jedoch in Konflikt mit der Dogmatik der StPO, da hierdurch die Gefahr begründet werde, die Anforderungen an den Tatverdacht zu lockern. Zudem gingen durch das Quick-Freeze-Verfahren unter Umständen relevante Daten dauerhaft verloren.

Sollte der Gesetzgeber tatsächlich einen dritten Anlauf für die Vorratsdatenspeicherung wagen, müsse diesem zwingend eine rationale Abwägung auf Basis der Empirie zugrunde liegen. Gleichzeitig gelte es dabei auch die Maßstäbe der Überwachungsgesamtrechnung zu berücksichtigen. Wichtig war *Prof. Puschke* zum Ende des Vortrags klarzustellen, „unüberwachte Bereiche – auch im Internet – gehören zu einer demokratischen Gesellschaft dazu“.

III. Zweite Sitzung

1. Umgang mit Massendaten im Strafverfahren

Die von *Prof. Dr. Jan-Hendrik Dietrich* (Hochschule des Bundes für öffentliche Verwaltung, Berlin) moderierte zweite Sitzung des Tages begann mit dem Vortrag von *Carsten Gußmann* (Generalstaatsanwaltschaft Köln, Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen) zum Umgang mit Massendaten im Strafverfahren. Dabei wurde anhand verschiedener Fallstudien erläutert, inwiefern Big Data die nationalen Sicherheitsbehörden vor teils erhebliche ermittlungsspezifische Probleme stellt, die über die zuvor von anderen Vortragenden erörterten rechtlichen Probleme hinausgehen. So können etwa die Datenmengen in strafrechtlichen Verfahren bei Urheberrechtsverstößen mittlerweile mehrere Petabyte umfassen, was mehreren Millionen Gigabyte entspricht. Von menschlicher Hand kann eine solche „Flut“ an Daten daher nur noch theoretisch bei einer unbegrenzten Anzahl von Ermittlern ausgewertet werden. Die in der Praxis begrenzten personellen Ressourcen können bei Verfahren mit Big Data-Bezug daher dazu führen, dass andere Verfahren zurückgestellt werden müssen. Ohne unterstützende externe Sachverständige ließen sich diese Art von Verfahren in der Praxis heutzutage jedenfalls kaum noch bewältigen.
Für die mit der Auswertung von Massendaten in der Strafverfolgung einhergehenden Probleme gebe es jedoch verschiedene Ansätze zu deren Bewältigung. So gelte es zunächst, einzelne Daten beziehungsweise Asservate zu kategorisieren und zu priorisieren. Hierbei kann etwa eine zentrale Datenaufbereitungsstelle helfen, wie sie in Nordrhein-Westfalen mittlerweile vom Landeskriminalamt betrieben wird. Die gesichteten Asservate können im Anschluss für Vernehmungsvorhalte oder die Validierung eines Anfangsverdachts verwendet werden. Zudem sei künftig zu erwägen, beispielsweise bei Massen von kinder- oder jugendpornographischen Daten eine automatische Sichtung mittels KI vornehmen zu lassen, die schneller und „schonender“ für die Ermittler ist. Werden etwa Erkenntnisse im Bereich der Organisierten Kriminalität oder des Betäubungsmittelhandels gewonnen, die unter Umständen zu hunderten oder gar tausenden Ermittlungsverfahren führen können, bietet sich als Unterstützung ein Softwareroboter (robotic process automation, RPA) an, der vollautomatisch einzelne Arbeitsschritte, wie das Einfügen von Personenstandsdaten in Haftbefehle, übernimmt.

Im Anschluss wurde unter anderem eine StPO-Reform diskutiert, insbesondere wurde vorgeschlagen, die einschlägigen Regelungen zur Anklageschrift und zum Urteil dahingehend abzuändern, dass dort auf einen Datenträger verwiesen werden kann.

2. Der Einsatz künstlicher Intelligenz im Sicherheitsrecht

Privatdozentin *Dr. Victoria Ibold* (LMU München) befasste sich im Anschluss mit dem Einsatz von KI im Sicherheitsrecht. Zunächst legte sie den Fokus auf den Begriff der „Künstlichen Intelligenz“. Diese wurde definiert als Computersystem, das menschlich intelligentes Verhalten mittels maschinellen Lernens imitiert. Anwendungsfelder seien etwa das predictive policing oder personenbezogene Rückfallprognosen.

Der Einsatz der KI-Systeme berge jedoch Risiken, da hinsichtlich des Entscheidungsfindungsprozesses stets eine sogenannte „Black Box“ bestehe. Wie genau das Ergebnis durch die KI erzielt wird, sei auch für Experten nicht in Gänze nachvollziehbar. Das technische Können geht somit weiter als das technische Verstehen. Im Strafverfahren muss der Einsatz von Technik jedoch vertrauenswürdig sein, was nicht stets der Fall ist, wie am Beispiel der Verwendung von Lügendetektoren deutlich wird. Zudem müssen technische Vorgänge transparent und nachvollziehbar sein. Daher müssten sie einer richterlichen Kontrolle zugänglich sein, denn das Recht dominiere nach wie vor die Technik und nicht anders herum. Dies sei bisher aber nicht ausreichend gewährleistet, da oftmals unklar bliebe, woher die Datengrundlage der KI stamme (sogenannter „Datenbias“).

Um diesen Problemen entgegenzutreten, befindet sich eine EU-Verordnung zum Thema KI im Trilogverfahren. Diese verfolgt einen horizontalen Ansatz, indem sie

grundsätzlich alle KI-Aktivitäten erfasst. Einzelne Ausnahmen bestehen etwa im Bereich der Nachrichtendienste. Die Verordnung soll sowohl für die Produktsicherheit von KI-Systemen als auch für das Sicherheitsrecht erstmalig einen einheitlichen Rechtsrahmen schaffen. Diesen Anspruch bezeichnete die Referentin als problematischen „Rasenmäher-Ansatz", da es sich um sehr verschiedene Rechtsgebiete handele.

Davon unberührt bleibt jedoch die zum Schluss des Vortrags erhobene Forderung der Referentin, dass das nationale Sicherheitsrecht weiterhin objektiv und rechtsstaatlich sein müsse. Da dies durch Art. 19 Abs. 4 GG auch verfassungsrechtlich determiniert sei, bedürfe es künftig einer richterlichen und somit transparenten Kontrolle des Einsatzes Künstlicher Intelligenz im Sicherheitsrecht.

3. Der Algorithmus als Ermittler – Zum Rechtsrahmen für Datenanalysen

Der letzte Vortrag des Tages von *Prof. Dr. Dieter Kugelmann* (Landesbeauftragter für den Datenschutz und die Informationsfreiheit, Rheinland-Pfalz) befasste sich mit der Frage, welche Rolle Algorithmen in der Ermittlungspraxis spielen. Anwendungsfelder für Algorithmen in der Strafverfolgung sind etwa automatische Datenanalysen oder Gesichtserkennungen. Bei diesen gebe es verschiedene Schritte, die durchlaufen werden. Zunächst erfolge die (Massen-)Datenerhebung, bevor die Daten strukturiert, ausgewertet und genutzt werden können. Dabei greife bereits die Datenerhebung zumindest in das Grundrecht auf informationelle Selbstbestimmung des Betroffenen ein. Weitere verletzte Grundrechte können das Recht auf die Integrität informationstechnischer Systeme sowie die Art. 10, 13 GG sein. Kein Grundrechtseingriff bestehe dagegen bei öffentlich zugänglichen Daten, weil diesen kein schutzwürdiges Vertrauen zukomme.

Vor diesem Hintergrund führte der Referent aus, dass zur verfassungsmäßigen Ausgestaltung einer Norm zur Rechtfertigung derartiger Grundrechtseingriffe die datenschutzrechtlichen Grundsätze zu beachten sind. So seien das Gebot der Datenminimierung und die Vorgaben der Zweckbestimmung und -änderung ebenso wie Gewährleistung der Betroffenenrechte zu achten. Werden Daten durch Algorithmen ausgewertet, bedürfe es daher spezifischer Schutzmechanismen durch technische und organisatorische Maßnahmen. Zudem seien Streubreitendaten Unbeteiligter zu reduzieren, was bedeute, dass alte Daten zu löschen oder bestehende Daten zu aktualisieren sind. Ferner müsse eine gesetzliche Regelung bestimmt genug sein. Dies werde dadurch sichergestellt, dass zwischen unterschiedlichen Adressaten differenziert wird und verschiedene Datentypen (beispielsweise anhand des darauf bezogenen Grundrechtseingriffes) kategorisiert werden. Schließlich müsse die Eingriffsschwelle der Rechtsgrundlage auch zum Gewicht des durch sie geschützten Rechtsguts passen. All das lasse sich bewerkstelligen, wenn der Gesetzgeber beim Einsatz von Algorithmen für die Datenanalyse ausdifferenzierte und abgestufte Regelungen implementiere.

In der anschließenden Diskussion kam die Frage auf, inwiefern eine staatliche Offenlegungspflicht für den Einsatz von Algorithmen besteht. Es ließe sich etwa erwägen, dass ein Angeklagter im Strafverfahren einen Anspruch auf Prüfung der Nachvollziehbarkeit, entsprechend dem Eichzeugnis eines Blitzers zur Überwachung des Straßenverkehrs, habe, um seinem Recht auf ein faires Verfahren nach Art. 6 Abs. 1 EMRK zu genügen. Hierbei bestehe dann aber das Problem, dass eine solche Pflicht – die im Ergebnis in der Diskussion daher abgelehnt wurde – im Widerspruch zu privaten Geschäftsgeheimnissen stünde und daher künftige Innovationen Dritter, auch zugunsten des Staates als potenziellem Käufer, auf diesem Feld vereiteln würde. Der (ausschließliche) Einsatz von open source-Technologien wurde in diesem Zusammenhang verworfen, da hierbei nicht sichergestellt sei, wie lange das System tatsächlich für die Strafverfolgungsbehörden verfügbar und aktualisierbar ist, da es jederzeit umprogrammiert werden könne.

IV. Podiumsdiskussion

Der finale Programmpunkt der Tagung war die Podiumsdiskussion zum Thema „Ransomware-Angriffe". An dieser nahmen *Carsten Meywirth* (Leiter Abteilung Cybercrime, Bundeskriminalamt), *Beatrix Jacobs* (Generalstaatsanwaltschaft Koblenz, Landeszentralstelle Cybercrime), *Dr. Dirk Häger* (Abteilungsleiter Operative Cyber-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik) und Rechtsanwalt *Dr. David Albrecht* (FS-PP Berlin) teil. Moderiert wurde die Diskussion von Rechtsanwalt *Prof. Dr. Björn Gercke*.

In der Diskussion zeichneten sich zwei Schwerpunkte ab. Zunächst ging es um eine aktuelle Bestandsaufnahme hinsichtlich der Häufigkeit und des Schädigungspotenzials von Ransomware-Angriffen. Dabei waren sich die Teilnehmer der Diskussion einig, dass sich in den vergangenen Jahren sowohl die Anzahl der registrierten Ransomware-Angriffe als auch der hieraus entstandene Schaden konstant gesteigert hat, was sich jedoch nicht nur mit der gestiegenen Aufmerksamkeit speziell im Bereich der Cyberkriminalität im engeren Sinne erklären lässt. Vielmehr habe die zunehmende Professionalisierung der Täter mit ihrem wachsenden technischen Fachwissen, aber auch der Möglichkeit, über das Darknet die Dienste von Hackern käuflich zu erwerben (sogenanntes Crime-as-a-Service), zu den Steigerungen beigetragen. Katalysator hierfür seien außerdem die Corona-Pandemie und der russische Angriffskrieg in der Ukraine gewesen, die das gesamte Leben weiter in die digitale Welt verlagert hätten. Die Diskussionsteilnehmer werteten Ransomware-Angriffe daher (auch künftig) als größte Bedrohung im Bereich Cybercrime.

Den zweiten Schwerpunkt bildete die Frage, welche Reaktion als Betroffener eines derartigen Angriffs sinnvoll ist. Zunächst stimmten die Diskutanten dahingehend überein, Lösegeldforderungen nicht nachzukommen. Es könne nie sicher sein, dass die Hacker auch tatsächlich in der Lage oder aber überhaupt gewillt sind, nach erfolgter Zahlung sämtliche infiltrierten Systeme wieder freizugeben.

Zudem setze man sich durch Verweigerung der Zahlung nicht der Gefahr eines eigenen Strafverfahrens, etwa wegen Terrorismusfinanzierung oder (finanzieller) Unterstützung einer kriminellen Vereinigung, aus. Inwieweit solche Strafbarkeitsrisiken der eigentlichen „Opfer" tatsächlich bestehen, ist derzeit noch nicht höchstrichterlich geklärt. Vertreten wird aber unter anderem von der Generalstaatsanwaltschaft Koblenz, dass im Falle einer Zahlung und dem oftmals nur schwer nachweisbaren Bestand einer kriminellen Vereinigung, eine Rechtfertigung über § 34 StGB in Betracht kommt. Empfehlenswert, wenngleich mühsam für die Betroffenen sei es aber, mithilfe professioneller Unterstützung und bestehender Backups die Daten und technischen Systeme neu aufzubauen. Zudem könne die Erstattung einer Strafanzeige zumindest unter dem Aspekt sinnvoll sein, dass für Strafverfolgungsbehörden und Politik sichtbar wird, wie viele solcher Angriffe überhaupt stattfinden. Aufgrund der regelmäßig grenzüberschreitenden Dimension von Ransomware-Angriffen und der häufigen Verweigerung von Rechtshilfe einzelner Länder, bestehe jedoch selten eine realistische Chance, die Täter strafrechtlich zur Verantwortung zu ziehen. Empfehlenswert sei daher für die Betroffenen vor allem eine hinreichende Prävention. Abschließend wurde noch ein Appell an die Politik gerichtet, künftig den Ressourcenmangel zur Bekämpfung von Cyberkriminalität zu beseitigen und durch eine bessere Gesetzgebung die Möglichkeiten zur Herstellung von unsicherer Software zu minimieren.

Zuletzt sprach Frau *Dr. Anslieb Esseln* (Landeskriminalamt Rheinland-Pfalz) das Schlusswort, in dem sie noch einmal zusammenfassend auf die verschiedenen Vorträge des Tages zurück und auf mögliche Entwicklungen in der Zukunft blickte. Nach den Danksagungen wurden die Teilnehmer verabschiedet.

V. Fazit

Das 7. Forum zum Recht der Inneren Sicherheit widmete sich einem der bedeutendsten Probleme, welches die rasant fortschreitende Digitalisierung aller Lebensbereiche mit sich bringt. Dass der Gesetzgeber und damit auch das Sicherheitsrecht sich den wandelnden gesellschaftlichen Entwicklungen nicht verschließen kann und darf, hat die Tagung deutlich gemacht. Big Data birgt jedoch nicht nur Gefahren für den einzelnen Betroffenen oder den Staat. Entscheidend wird sein, dass der Gesetzgeber die bestehenden Chancen nutzt und durch verfassungsgemäße Gesetze den Einsatz von fortschrittlichen Technologien und der Künstlichen Intelligenz, nicht nur in Bezug auf Massendaten, zugunsten der Bürger und dem Schutz ihrer Rechte regelt. So kann bei sinnvollem Einsatz von KI und Algorithmen allgemein der zunehmenden Tendenz entgegengewirkt werden, dass Strafverfahren mithilfe von Datenmengen überflutet werden und damit – anders als in der Vergangenheit – Beweise nicht zurückgehalten, sondern unter „Datenbergen" versteckt werden. Dass dabei ein Schulterschluss zwischen juristischer Theorie sowie polizeilicher und technologischer Praxis zwingend notwendig ist, haben die Vorträge in ihrer Gesamtheit eindrücklich gezeigt.