Workshop Sicherheits- und Strafrecht im Angesicht der Digitalisierung

von Ass. iur. Nicole Selzer

Amadeus Peters (HIIG), *Sebastian Golla* (Johannes Gutenberg-Universität Mainz) und *Christian Rückert* (Friedrich-Alexander Universität Erlangen-Nürnberg) luden am 27. Juni 2019 zum Workshop „Sicherheits- und Strafrecht im Angesicht der Digitalisierung" für NachwuchswissenschaftlerInnen ein, der in den Räumlichkeiten des Alexander von Humboldt Instituts für Internet und Gesellschaft (HIIG) in Berlin stattfand. Der Workshop wurde mit dem Ziel ins Leben gerufen, Fragen rund um das Thema Sicherheitsrecht im Zusammenhang mit der Digitalisierung zu identifizieren, zu untersuchen und zu diskutieren und damit jungen WissenschaftlerInnen eine Plattform für aktuelle Forschungsvorhaben und Forschungsthemen zu geben.[1]

Nach einer herzlichen Begrüßung durch die drei Veranstalter, wobei *Christian Rückert* zeitgemäß per Videochat zugeschaltet wurde, eröffnete *OStA Thomas Goger* von der Zentralstelle Cybercrime Bayern als Keynote-Speaker den Workshop. Am 1. Januar 2015 gründete er gemeinsam mit einem weiteren Kollegen die Zentralstelle Cybercrime bei der Staatsanwaltschaft in München, die mittlerweile 14 Staatsanwälte umfasse. In Gießen sei die erste Zentralstelle gründet worden, Berlin und Nordrhein-Westfalen verfügen ebenfalls über derartige Schwerpunktabteilungen. Bevor *OStA Goger* über tägliche Herausforderungen im Bereich Cybercrime berichtete, verwies er auf die Polizeiliche Kriminalstatistik (PKS), die einen Schaden für Cybercrime in Höhe von 51 Mio. EUR in 2016 (72 Mio. EUR in 2017) ausweise. Dies sei im Vergleich zu anderen Deliktsfeldern ein äußerst geringer Schaden. Die Aussagekraft der PKS sei aber vor allem im Bereich Cybercrime sehr gering. Grund hierfür sei, dass Auslandstaten nicht erfasst würden. Da es sich in diesem Phänomenbereich aber gerade um Delikte handle, die einen grenzüberschreitenden Bezug aufwiesen und Täter oftmals im Ausland ansässig seien, sei eine erhebliche Verzerrung gegeben. Eine Anpassung der Statistik sei daher dringend erforderlich. Erkenntnissen der Staatsanwaltschaft zufolge, seien IT-Kenntnisse bei den Tätern nicht erforderlich, da jegliche Dienstleistung i.S.v. „crime-as-a-service" einkaufbar sei, wodurch eine sehr viel größere Zahl potenzieller Täter bestehe, als man geheimhin für möglich halte. Fast anekdotisch fuhr *OStA Goger* fort, dass die Strafprozessordnung analog geblieben sei. Zwar sei bereits am 3. August 1984 die erste E-Mail in Deutschland versandt worden, direkt erfasst sei sie von der Strafprozessordnung aber immer noch nicht. Dafür aber das antiquierte Fax und Telegramm. Zwar könne man sich behelfen, dies sei aber auch problembehaftet.

Im Anschluss trug *Dr. Raphael Bossong* (Stiftung Wissenschaft und Politik) zur digitalen Beweissicherung vor und ging hierbei auf den US „Cloud Act" und die „E-Evidence"-Initiative der EU ein. Derzeit gelte für Strafverfolgungsbehörden in der EU ein rein freiwilliges Verfahren zur Abfrage von Bestandsdaten von US Serviceprovidern. Alternativ könne ein formelles Verfahren zur Mutual Legal Assistance (MLA) eingeleitet werden, das über das US Justizministerium laufe und im Durchschnitt zehn Monate dauere. Der Cloud Act schaffe die Verpflichtung für US Firmen Kommunikations- und Personenstammdaten zu US-Bürgern und Anwohnern zu übergeben, wenn diese durch Strafverfolgungsbehörden oder Gerichte von „complying countries" angefordert würden. Zudem erhielten „complying countries" direkten Zugang zu Daten, die privatwirtschaftlich in den USA gespeichert würden. Problematisch sei allerdings, dass keine Einzelfallprüfung wie im MLA Prozess erfolge, wodurch ein Einfallstor für Datenabfragen aus den USA durch Drittstaaten entstehen könne. Die E-Evidence-Verordnung sehe den direkten Zugriff auf elektronische Beweise (bspw. E-Mails) von Dienstleistern oder gesetzlichen Vertretern in einem anderen Mitgliedsstaat vor. Der Dienstleister bzw. gesetzliche Vertreter sei verpflichtet innerhalb von zehn Tagen oder in Notfällen innerhalb von sechs Stunden zu antworten. Kritisch sei hierbei neben anderen Punkten die Auslagerung der Entscheidung zur Datenherausgabe an privatwirtschaftliche Akteure mit kurzen Bearbeitungsfristen, die beschränkte Benachrichtigung Betroffener sowie die Aushebelung der Territorialität durch verpflichtende Schaffung eines rechtlichen Vertreters in der Union.

Dr. Oskar Josef Gstrein, M.A., LL.M (Rijksuniversiteit Groningen – Campus Fryslân) berichtete über das EU-Forschungsprojekt ‚Cutting Crime Impact' (CCI).[2] Das Projekt habe zum Ziel, die Auswirkung von Kriminalität zu verringern, indem innovative Instrumente zur Verhütung und Bekämpfung zusammen mit sechs europäischen Strafverfolgungsbehörden entwickelt werden. Ein besonderer Fokus liege darauf, die Chancen und Risiken der Digitalisierung in diesem Bereich auch aus (grund-)rechtlicher, ethischer und sozialer Perspektive interdisziplinär aufzuarbeiten. Das Projekt werde bis Oktober 2021 Maßnahmenpakete (‚toolkits') für vier Teilbereiche entwickeln: predictive policing, community policing, crime prevention through urban design and planning (CP-UDP) sowie measuring and mitigating citizens' feeling of insecurity.

Catharina Pia Conrad (Universität Bremen) sprach über die technischen (Un-)Möglichkeiten des Kernbereichsschutzes bei der strafprozessualen Online-Durchsuchung

[1] https://www.hiig.de/events/workshop-sicherheits-und-strafrecht-im-angesicht-der-digitalisierung/ (zuletzt abgerufen am 22.7.2019).

[2] https://www.cuttingcrimeimpact.eu (zuletzt abgerufen am 22.7.2019).

und stellte die These auf, das gesellschaftlich Wünschenswerte (Kernbereichsschutz) sei mit dem technisch Möglichen nicht vereinbar und neue Ansatzpunkte seien notwendig, um den Kernbereichsschutz zu gewährleisten. Problematisch sei die enorme Datenmenge und -vielfalt, die im Rahmen einer Online-Durchsuchung anfalle, wodurch die Erstellung von Persönlichkeitsprofilen möglich sei, welche mit dem Kernbereichsschutz nicht vereinbar seien. Einen neuen Ansatzpunkt sieht *Conrad* insbesondere in der Übertragung der Grundsätze des additiven Grundrechtseingriffs auf den Schutz des Kernbereichs der privaten Lebensgestaltung.

Jan Mysegades (Deutsches Forschungsinstitut für die öffentliche Verwaltung Speyer) referierte über die Rolle moderner Software als Beweismittel im Strafprozess. Nachdem er Beispiele für Algorithmen erläuterte und anschauliche Praxisbeispiele präsentierte, u.a. die Gesichtserkennungssoftware die beim G20 Gipfel in Hamburg und am Bahnhof Berlin Südkreuz verwendet wurde, verwies er auf die Gefahr falsch positiver Ergebnisse. So wurden bspw. in Amerika 28 amtierende Kongressabgeordnete von Amazon ‚Recognition' fälschlicherweise als Straftäter identifiziert. *Mysegades* zufolge sei die mangelnde Nachvollziehbarkeit derartiger Algorithmen das Problem. Die Datenübertragung und -auswertung sei von den Betroffenen nicht überprüfbar. Der Zugang der Öffentlichkeit und der Verteidigung seien erschwert. Eine positive Ausnahme bilde allerdings das Programm SKALA der Polizei und des Landeskriminalamtes Nordrhein-Westfalen. Unter prozessrechtlichen Gesichtspunkten ergebe sich die Frage, wie das Beweismittel in die Hauptverhandlung eingeführt werde – als Sachverständigengutachten, Urkunde oder Augenschein. Zudem müssen neue Methoden auch der Reproduzierbarkeit, Gleichförmigkeit und Validität unterliegen, woran mangels Nachvollziehbarkeit Zweifel bestünden. Die bisherige Rechtsprechung zu „standardisierten Verfahren" nehme faktisch eine Beweislastumkehr vor. Im Gegenzug sei es jedenfalls zwingend notwendig, verstärkte Einsichtsrechte der Verteidigung zu gewähren. *Mysegades* plädiert hinsichtlich moderner Software als Beweismittel für mehr Transparenz durch Black Box-Testing und Zertifizierung sowie für technische Garantien über Blindbeweise („zero-knowledge-proof").

Hieran schloss sich die Vorstellung des Forschungsprojektes MEDIAN durch *Dr. Jan Fährmann* (Hochschule für Wirtschaft und Recht Berlin) an. MEDIAN stehe für die mobile berührungslose Identitätsprüfung im Anwendungsfeld Migration.[3] Das Verbundprojekt laufe bis Juli 2021 und habe die Entwicklung eines mobilen Demonstrators zur polizeilichen Identitätsfeststellung zum Ziel, wobei der HWR unter Leitung von *Prof. Dr. Hartmut Aden* die Aufgabe zukomme, hohe Standards für Recht, Datenschutz und Ethik bei der mobilen Kontrolle sicherzustellen. Dabei solle neben der polizeilichen Perspektive die Sicht der Betroffenen einbezogen werden, damit die Kontrollen für beide Seiten möglichst wenig belastend werde. Auch solle geprüft werden, wie technische Anwendungen ausgestaltet werden können, damit sie rechtswidrigen Verhalten entgegenwirken oder dieses ausschließen, bspw. sog. „Racial Profiling".

Dimitris Zachos (Martin-Luther-Universität Halle-Wittenberg) erörterte den Begriff „virtuelle Handlung" aus strafrechts- bzw. handlungstheoretischer Sicht. *Zachos* stellte fest, dass in den letzten zwei Jahrzehnten immer wieder für das Strafrecht interessante Konstellationen vorgekommen seien, bspw. der virtuelle Mord („MapleStory"), der virtuelle Diebstahl („Runescape") oder die virtuelle Vergewaltigung („Lamda MOO"). In diesen Fällen habe der Begriff der „virtuellen Handlung" keiner wesentlichen Erweiterung oder Abänderung des Handlungsbegriffs auf handlungstheoretischer bzw. strafrechtsdogmatischer Ebene bedurft. Auch unter begriffsgeschichtlicher Betrachtung deute der Ausdruck „virtuell" nicht auf eine „falsche" bzw. „alternative" Realität hin. Demnach müsse auch keine kategorische Unterscheidung zwischen „Realem" und „Virtuellem" erfolgen. Der Aspekt der Virtualität erweitere und bereichere vielmehr den geistigen Horizont bzw. das Erkenntnispotenzial. Bei Handlungen, die lediglich systeminterne Konsequenzen zur Folge haben (bspw. virtueller Mord, virtuelle Vergewaltigung innerhalb eines Onlinespiels) sei das Verhalten nicht strafbar. Bei Handlungen, die dagegen auch extravirtuelle Folgen aufwiesen (bspw. virtueller Diebstahl von erworbenen Gegenständen innerhalb eines Onlinespiels), sollte das Strafrecht gleichwohl ultima ratio sein. An erster Stelle sollten *Zachos* zufolge systeminterne Sanktionen (bspw. dauerhafter Ausschluss vom Onlinespiel) stehen und ggf. zivilrechtliche Sanktionen (Schadensersatz) folgen.

Abschließend beschäftigte sich *Benedikt Kohn* (Universität Augsburg) mit Chancen und Risiken des Einsatzes Künstlicher Intelligenz im Rahmen der Strafzumessung. Hierbei wies er zunächst auf bestehende Probleme bei der Strafzumessung hin. So böten die weitgefassten Strafrahmen im Strafgesetzbuch den Richterinnen und Richtern zwar viel Spielraum für Einzelfallgerechtigkeit, führten allerdings auch zu lokalen Straftraditionen und in der Folge zu großen regionalen Unterschieden. Auch durch die Unvollkommenheit der menschlichen Natur würden Ungleichbehandlungen entstehen. Einen Ausweg könnte hier der Einsatz von Künstlicher Intelligenz bieten. In den USA seien dafür bereits *Risk Assessment Tools* im Einsatz. Diese Programme, die ursprünglich nur dafür entwickelt wurden, die Rückfallwahrscheinlichkeit von Straftätern für die Fragen der Untersuchungshaft zu bestimmen, würden zunehmend für Strafzumessungsentscheidungen eingesetzt werden. Dies würde bspw. für das Eingruppieren in die Stufen der in den USA üblichen *Sentencing Guidelines* verwendet werden. Der Einsatz der Künstlichen

[3] https://campus4u.hwr-berlin.de/qisserver/rds;jsessionid=ED197FB5BFE4731EA299E5C2B46F7979.qis2?state=verpublish&status=init&vmfile=no&publishid=1131&moduleCall=webInfo&publishConfFile=webInfoProjekt&publishSubDir=forschung (zuletzt abgerufen am 22.7.2019).

Intelligenz könne zwar dabei helfen, menschliche Voreingenommenheit auszuschließen, aber gleichwohl zu Ungleichbehandlungen führen. Problematisch sei, dass das Verfahren nicht transparent und eine Überprüfung unmöglich sei.

Zusammenfassend, *Amadeus Peters, Sebastian Golla* und *Christian Rückert* haben eine angenehme Atmosphäre für den Austausch und Diskurs geschaffen. Der Workshop beinhaltete eine Bandbreite spannender Vorträge zu zukunftsorientierten Themen. Strafprozessuale Herausforderungen der Gegenwart und Zukunft wurden ausgiebig diskutiert. Der Workshop zeigte, dass einiger Diskussions- und Handlungsbedarf besteht und der Digitalisierung in Bezug auf das Sicherheits- und Strafrecht im weiteren Sinne mehr Aufmerksamkeit geschenkt werden sollte. Zu hoffen bleibt, dass dieses gelungene Format eine Neuauflage erfährt und künftig fester Bestandteil der Tagungslandschaft in Deutschland wird.