TAGUNGSBERICHT

2. Workshop Sicherheits- und Strafrecht im Angesicht der Digitalisierung

von Till Reinholz

Am 17.7.2020 fand die zweite Auflage des Workshops „Sicherheits- und Strafrecht im Angesicht der Digitalisierung“ statt. Nach dem großen Erfolg der Erstauflage am 27.6.2019,[1] wurde der zweite Workshop federführend von *Nicole Selzer* (Martin-Luther-Universität Halle-Wittenberg) und *Jannik Piepenburg* (Martin-Luther-Universität Halle-Wittenberg) initiiert, organisiert und moderiert. Insgesamt nahmen knapp 30 Personen an dem Workshop teil, darunter auch Wissenschaftler*innen und Rechtsanwälte aus den Niederlanden, der Schweiz, Österreich und Japan sowie aus ganz Deutschland, unter anderem aus Berlin, Erlangen, Gießen, Halle, Magdeburg, Mainz und Saarbrücken. Die Zielsetzung des an der Martin-Luther-Universität gegründeten Netzwerks IT und Recht umfasst auch die frühzeitige Involvierung Studierender, welche ebenfalls die Möglichkeit zur Teilnahme erhielten.

In Anbetracht der herausfordernden Situation infolge der Corona-Pandemie galt es, eine alternative Form des Diskurses zu finden. Somit wurde der Workshop statt wie ursprünglich angedacht vis-à-vis in den Räumlichkeiten der Martin-Luther-Universität Halle-Wittenberg zeitgemäß als Videokonferenz durchgeführt. Es wurden mehrere Breakout-Sessions eingeplant, um einen intensiveren Austausch in kleinerer Gruppe zu ermöglichen, die vergangenen Vorträge vertieft zu debattieren und die Netzwerkbildung zu unterstützen.

Nach einer Begrüßung und kurzen Vorstellung der Teilnehmer durch die beiden Gastgeber, begann der Keynote-Speaker *Ammar Alkassar* als Bevollmächtigter für Innovation und Strategie & Chief Information Officer des Saarlandes mit seinem Impulsvortrag. Zunächst wies er auf die besonderen Herausforderungen der Digitalisierung hin, welche durch Corona noch verschärft wurden. So sei – im Gegensatz zur analogen Welt – eine einfache Abstinenz aus der digitalen Welt nicht mehr möglich, sodass Jedermann de facto rund um die Uhr dem Informationsfluss ausgesetzt ist. Gleichzeitig erlange der Einzelne jedoch auch mehr Macht und Möglichkeiten, seine Meinung darzulegen. Als Kritikpunkt stellte *Alkassar* die mangelnde Digitalisierung in der Verwaltung dar, so ist das grundlegende Modell seit etwa 200 Jahren nahezu unverändert und bedürfe einer grundlegenden Reformierung. Zur Diskussionsanregung stellte Herr *Alkassar* mehrere Thesen auf. So sei Cybersicherheit ein wesentlicher Parameter für die geopolitischen Konflikte der Zukunft, wobei die Bedeutung, insbesondere bezüglich der ökonomischen Tragweite, stetig zunehme. Weiterhin wurde hinterfragt, inwieweit die technologische Entscheidung der Cybersicherheit bereits gefallen sei, ergo inwiefern eine Angriffsrespektive Verteidigungsasymmetrie bestehe und wirksamer Schutz vor Attacken gegeben ist. Hinsichtlich der zukünftigen möglichen Entwicklungen stellte *Alkassar* anhand des EU-China-Konflikts mehrere Szenarien dar, welche von völliger Integration und Symbiose der technologischen Fähigkeiten bis zu eskalierender Konfrontation und Isolation reichten. In einer weiteren Fragestellung wurde die herausragende Bedeutung von Künstlicher Intelligenz (KI) für die Cybersicherheit thematisiert, um anschließend die Frage aufzuwerfen, ob die Digitalisierung dem Recht enteile. Hier stellte *Alkassar* die „Cyberwehr“ des Saarlandes als deutsches Pilotprojekt vor, um eine effektive Strafverfolgung und Verteidigung vor Cyberattacken zu gewährleisten. Zuletzt wurden Effektivität und eine eventuelle Automatisierung der Strafverfolgungsabläufe aus verschiedenen Perspektiven dargestellt, um weiterhin dem in der StPO gesetzlich manifestierten Legalitätsprinzip entsprechen zu können und eine Überlastung der Behörden entgegenzuwirken, ohne dem Bürger ein faires Verfahren vorzuenthalten. Der Impulsvortrag endete mit einer regen Diskussion aller Workshop-Teilnehmer*innen.

Im anschließenden Vortrag stellte *Sebastian Oelrich*, M.Sc., LL.M.oec. (Otto-von-Guericke-Universität Magdeburg) Ergebnisse einer gemeinsam mit *Nicole Selzer* vorgenommenen Untersuchung zum Einfluss der Dunklen Triade (Machiavellismus, Narzissmus und Psychopathie) und Moralentwicklung auf cyberkriminelle Absichten vor.[2] Hierfür fokussierten sie sich insbesondere auf Cyber-dependent Handlungen wie bspw. Hacken. Sie fanden einerseits, dass nur höhere machiavellistische und psychopathische Tendenzen mit höheren cyberkriminellen Absichten einhergehen, während Narzissmus keinen signifikanten Einfluss aufwies. Auf der anderen Seite hat die moralische Entwicklung auf einer regelkonformen Ebene erwartungsgemäß eine hemmende Wirkung, während eine höhere moralische Entwicklung (post-conventional Level) wiederum cyberkriminelle Absichten steigern könnte. In der anschließenden Diskussion wurde unter anderem debattiert, wie sich in Ansehung der Ergebnisse verschiedene Delikte und Begehungsweisen im Bereich Cybercrime verorten lassen und sich hinsichtlich des moralischen Aspekts Hackergruppen wie etwa Anonymous von stereotypen Cyberkriminellen unterscheiden könnten.

[1] Vgl. *Selzer*, KriPoZ 2019, 320 ff.

[2] *Selzer/Oelrich,* in: Leukfeldt/Weulen Kranenbarg (Hrsg.), Cybercrime in context: the human factor in victimization, offending, and policing (im Erscheinen).

Als nächstes stellte *Bettina Pospisil* (Donau-Uni Krems) die Problematik der Hell- und Dunkelfeldforschung im Bereich Cybercrime dar, wobei sie insbesondere auf die österreichische Situation Bezug nahm.[3] In den letzten Jahren sei ein zunehmender Anstieg von Cybercrime zu verzeichnen. Dabei zeige sich, dass eine große Differenz zwischen Hell- und Dunkelfeld, aber auch zwischen relativen und absoluten Dunkelfeld bestehe. *Pospisil* problematisierte hierbei die oftmals fehlende Wahrnehmung von Cybercrime und Opfer einer solchen Straftat geworden zu sein. Dies betreffe nicht nur Privatpersonen sondern auch Unternehmen. Neben anderen Faktoren sei es bspw. abhängig davon welche Art von Cybercrime verübt werde, so sei Spyware regelmäßig dem absoluten Dunkelfeld zuzuordnen. Um Cybercrime zu untersuchen, führte sie Untersuchungen sowohl im Hell- als auch Dunkelfeld durch, um ein möglichst genaues Bild der Verbreitung von Cybercrime zu erhalten. Hierbei ergaben sich vielfältige Herausforderungen, in der Hellfeldanalyse bspw. der mangelnde Zugang zu polizeilichen Akten, die unterschiedlichen Tathergänge die unter ein Strafnorm subsumiert werden oder unterschiedliche nationale und internationale Rechtsrahmen, welche die Vergleichbarkeit erschweren. Im Rahmen der Dunkelfeldstudien zeigte sich insbesondere die Wahrnehmung als Herausforderung, weshalb Informationen zum Tathergang und Umfang schwierig zu ermitteln waren.

Nach einer weiteren Breakout Session und der Mittagspause stellte *Florian Nicolai* (Friedrich-Alexander-Universität Erlangen-Nürnberg) das Internet of Things (IoT) und dessen Bezug zum Strafrecht vor und legte hierbei einen besonderen Fokus auf die Ermittlungsmaßnahmen der StPO und wie sich die Automatismen des IoT unter die gesetzlich formulierten Tatbestandsmerkmale subsumieren lassen. *Nicolai* hinterfragte beispielsweise eine mögliche Analogie im Bereich des Einbruchsdiebstahls nach §§ 243, 244 StGB durch das „digitale Eindringen" in die Privatsphäre, um anschließend die rechtspolitischen Konsequenzen zu erläutern. Andererseits wurde auch die Rolle des IoT als Aufklärungshilfe dargestellt, sodass etwa durch Smart Cars Straßenverkehrsdelikte leichter aufgeklärt oder die Installation eines Smart Homes häusliche Gewalt belegen könnten. Es ergeben sich somit diverse rechtliche und tatsächliche Probleme und Risiken rechtspolitischer, materiell- und prozessrechtlicher sowie kriminologischer Natur, allerdings auch diverse Chancen und neue Perspektiven.

Dr. Oskar Josef Gstrein, M.A., LL.M (Rijksuniversiteit Groningen – Campus Fryslân) stellte wie im vergangenen Jahr das Projekt Cutting Crime Impact (CCI) vor.[4] Der aktuellen Stand des Projektes, erste Resultate und Schwierigkeiten, die bei der Umsetzung auftraten, wurden erörtert. So wurden rechtliche Probleme im Rahmen von DGSVO und EU-Richtlinien thematisiert. Zentrale Bedeutung habe insofern die Fragestellung, wie transparent Polizeiarbeit sein darf, um einerseits den Ermittlungs- und Präventionserfolg nicht zu gefährden und andererseits den Datenschutz der Bürger als vertrauensschaffendes Element in die Ermittlungsbehörden zu schützen. Ethisch sei zu hinterfragen, inwieweit eine Stigmatisierung von Gruppen oder Wohngegenden stattfinde, die präventiven Maßnahmen ausgesetzt seien. Im Fokus steht hierbei vor allem Kleinkriminalität, sog. „petty crime". Prognostisch sei zu berücksichtigen, dass die Maßnahmen langfristigen Erfolg versprechen und der größte Nutzen für das interne Management, auch hinsichtlich städtebaulicher Entscheidungen, bestehe.

Im Anschluss an eine weitere Breakout Session, folgte der Vortrag von *Marcel Valentin* (Martin-Luther-Universität Halle-Wittenberg) zum Thema „Vernetzte Demokratie – Risiken des Einsatzes intelligenter Systeme im Wahlkampf". Der Aktualität und Relevanz des Themas entsprechend, nannte *Valentin* beispielhaft Anwendungsbereiche der letzten Jahre, etwa die Meinungsbeeinflussung des US-Wahlkampfes 2016 mit potentiell russischem Einfluss oder dem Twittern von Meinungsrobotern gegen den Migrationspakt der UNO im Jahr 2018. Die hervorgehobene Rolle spiele in Wahlkämpfen das Micro-Targeting, welches gezielt Wählergruppen durch Datenbankanalysen anspreche. Diese Variante sei erstmals von *Obama* in den Wahlkämpfen 2008 und 2012 angewandt worden, spielte jedoch auch bei Trumps Wahlkampf 2016 eine große Rolle. Genutzte Ressourcen seien bspw. Datenbanken wie Wählerverzeichnisse, Spenden oder sonstige freiwillige Angaben von Daten. Dies führe zu einer erhöhten Effizienz des Wahlkampfes und einer genaueren Wahlverhaltensvorhersage. Valentin problematisierte die daraus folgenden Konflikte mit den Wahlgrundsätzen im demokratischen System und der gesteuerten Beeinflussung der öffentlichen Meinungsbildung. Letztere würde speziell durch Social Bots in den Foren sozialer Netzwerke manipuliert. Grundlage der lebhaften Diskussion war die Frage, inwieweit der politische Willensbildungsprozess umgekehrt würde und wie eine unkontrollierbare und intransparente Nutzung intelligenter Systeme zum Schutze einer demokratischen Wahl verhindert werden könne.

Zum Abschluss stellte *Stefan Hessel* die von ihm sowie *Lena Leffer* und *Karin Potel* (reuschlaw Legal Consultants & Uni Saarland) untersuchte Thematik der Desinformationsangriffe auf Unternehmen vor. Im Fokus der Untersuchung standen Tätergruppen und deren Motivationen sowie die präventiven und reaktiven Schutzmöglichkeiten für Unternehmen. *Hessel* nannte hier das „Dreieck der Desinformation", welches aus Identität, Umfang und Steuerung des Desinformationsprozesses bestehe. Anschließend ordnete er die Angriffe rechtlich ein und zeigte auf, dass potentielle Rechtsschutzlücken, insbesondere hinsichtlich der Beweisführung, bestehen könnten. Er regte Lösungsmöglichkeiten wie die Einführung eines neuen StGB-Tatbestandes an oder die Verpflichtung von sozialen Netzwerken zum Löschen schädigender Posts und anderweitiger Beeinflussungen, wie von ihm beispielhaft genannt, eine Aktienkursbeeinflussung durch eine vermeintliche Übernahme des Unternehmens. In der anschließend geführten Diskussion wurde – wie im Rahmen

[3] *Huber/Pospisil*, in: Rüdiger/Bayerl (Hrsg.), Cyberkriminologie. Kriminologie für das digitale Zeitalter, 2020, S. 109-133.

[4] https://www.cuttingcrimeimpact.eu (zuletzt abgerufen am 2.8.2020).

der anderen Vorträge auch – auf die steigende Bedeutung von Social Media und Digitalisierung generell und hier speziell für Unternehmen eingegangen.

Im Anschluss fand ein gebührender Ausklang und eine letzte diskussionsfreudige Breakout-Session statt. Trotz der coronabedingten erschwerten Umstände für die Organisatoren ist es ihnen gelungen, jungen Forschern und Wissenschaftlern eine angemessene und interdisziplinäre Plattform für eine Vernetzung und wissenschaftliche Diskussion zu geben. Neben spannenden Vorträgen und Diskussionen wurden auch viele neue Kontakte geknüpft.

Durch internationale Referierende und Teilnehmer wurden auch länderübergreifende Perspektiven aufgezeigt und somit neue Denkansätze geschaffen. Das breitgefächerte Portfolio der Vorträge zeigt die Themenvielfalt und Risiken der Digitalisierung sowie die Relevanz der dringend notwendigen Bündelung des Forschungspotentials in Europa, um der immensen Herausforderungen Herr zu werden. Es ist wünschenswert, dass das Format eine weitere Fortsetzung findet und noch mehr Wissenschaftler*innen aus verschiedenen Disziplinen zum Eintritt in einen gemeinsamen Diskurs anregt.