Fünfter Digitaler Salon

Das „Darknet“. Bedrohung unserer Zivilisation oder Tor zur Freiheit?

Zu ihrem mittlerweile bereits fünften „Digitalen Salon“ hatte die Katholische Akademie Bayern am Montag, den 5. November 2018, eingeladen. Der Digitale Salon findet seit 2016 statt und zielt darauf ab, über das Internet als Phänomen nachzudenken, über Folgen der Digitalisierung zu reflektieren und unterschiedliche Positionen ins Gespräch zu bringen. Dieses Mal ging es um das Darknet, von dem viele schon gehört haben, von dem die meisten aber nichts Genaueres wissen als dass man sich dort auf Marktplätzen illegale Waren beschaffen kann. Relativ unbekannt ist dagegen, dass das Darknet auch einen Ort der politischen Freiheit und der bürgerlichen Selbstverteidigung bietet. In Überwachungsstaaten gibt es für Dissidenten sogar die Möglichkeit, sich mittels des Darknets der Observation durch Regierungen zu entziehen.

Moderiert wurde das Gespräch zwischen zwei freien Journalisten und einem Rechtswissenschaftler wie immer von Dr. Alexander Pschera, Publizist und Geschäftsführer bei „maisberger“, auf dessen Idee auch das Gesamtkonzept des Digitalen Salons zurückgeht.

Zunächst führte der Berliner Journalist Stefan Mey ein wenig in die Grundlagen des Darknets ein. Seine grundlegende Bedeutung liegt in der Abschottung vom normalen Internet und der Anonymität für alle Beteiligten, also nicht nur für die Nutzer, sondern auch für die Anbieter. Das bekannteste Projekt, das Zugang zum Darknet herstelle, sei „TOR“, abgekürzt für „The Onion Router“, da sich der Erfinder das Projekt wie eine Zwiebel vorstellte, deren Kern durch mehrere Schichten geschützt wird. Daher lautet die Endung der Adressen im Darknet auch – statt „.com“ oder „.de“ – einfach „.onion“.

TOR habe seinen Sitz in Amerika und ließe sich wie eine Mischung aus Amnesty International und Wikipedia beschreiben, so Mey; dabei sei es erstaunlicherweise aber auch aus Töpfen der US-Regierung mitgefördert. TOR hat ein Netzwerk von tausenden Knoten rund um die Welt und verbindet über einen speziellen Browser eine IP-Adresse mit der anderen über mindestens drei Knoten, wobei jeweils ein Knoten nur seinen vorherigen und seinen nachfolgenden identifizieren kann, eine komplette Rückverfolgung in beide Richtungen aber unmöglich ist. Das mache es leichter, Zensur zu umgehen, da auch ein Anbieter nicht blockiert werden kann.

Am bekanntesten sei die Funktion des Darknets als Marktplatz, so Mey, auf dem man sich relativ leicht verschreibungspflichtige Medikamente, Drogen, Waffen, Falschgeld, gefälschte Pässe oder kinderpornographische Inhalte beschaffen könne. Daneben werde das Darknet aber auch zu exklusiven, teils selbstreferentiellen Informationen über das Darknet genutzt, ferner als Programmbaustein für Messengerdienste wie BRIAR, mit denen eine nicht rückverfolgbare Kommunikation zwischen zwei Adressen möglich sei. Zudem würden Zeitungen wie die „New York Times“, der „Guardian“ oder die „taz“ auf ihren Internetauftritten „alternative Zugangstüren“ über das Darknet für sogenannte „Whistleblower“, wie es beispielsweise Edward Snowden ist, bereitstellen und so zu exklusiven Informationen gelangen.

Doch trotz aller Aktivität sei das Darknet bisher vergleichsweise klein: es gebe etwa 100.000 Onion-Adressen und 50.000 bis 100.000 Nutzer am Tag, was im Vergleich zum Internet extrem gering sei. Bei der heutigen Überwachungsmaschinerie bzw. der Datensammlung der halben Menschheit bei einigen wenigen Firmen wie Google, Amazon oder Facebook sei es aber sinnvoll, über eine größere Nutzung des Darknets als geschütztem Raum nachzudenken.

Dr. Christian Rückert, Dozent am Lehrstuhl für Strafrecht, Strafprozessrecht, Internationales Strafrecht und Völkerrecht der Universität Erlangen-Nürnberg, ordnete das Darknet juristisch ein und sprach zu den rechtlichen und ethischen Herausforderungen bei der Strafverfolgung im Darknet. Dazu ging er zunächst nochmals auf die bereits von Stefan Mey erwähnten Marktplätze und Handelsplattformen ein, die inzwischen derart professionalisiert worden seien, dass er selbst dafür den Ausdruck „Amazon Crime“ benutze. Sei vor der Etablierung des Darknets die Herstellung und der Vertrieb von falschen Geldscheinen praktisch gegen Null gegangen, habe die Falschgeldkriminalität seit dem Darknet massiv zugenommen.

Kriminelle und zu verfolgende Tatbestände seien vor allem der Handel mit illegalen Waren wie Betäubungsmitteln, Waffen und Drogen sowie Kinderpornographie. Ein neuer Straftatbestand solle künftig eventuell allein schon das Betreiben einer Seite sein, die Anderen als Handelsplattform zur Verfügung gestellt würde, denn bisher kommen die Seitenbetreiber wegen Beihilfe mit recht geringen Strafen davon. Allerdings, so Rückert, müsse man dann eigentlich auch eine allgemein genutzte Plattform wie „ebay“ kriminalisieren, denn sie stelle den größten Absatzmarkt für Hehlerware dar.

Seitens der Ermittlungsbehörden werde inzwischen immer mehr aufgerüstet, es gebe spezialisierte Einheiten beim Bundeskriminalamt und beim Zoll sowie Schwerpunktstaatsanwaltschaften. Auch sogenannte IT-Forensiker würden vermehrt eingesetzt. Ein Zentrum für Bayern entstehe hier gerade in Bamberg.

Da die Anonymität der Inhalte und das Bezahlen mit Bitcoins die Ermittlungen erschweren würden, werde auf gute alte Polizeiarbeit zurückgegriffen, indem beispielsweise Postsendungen kontrolliert würden. Nach wie vor müssten Waren wie Drogen per Post vom Absender zum Empfänger gelangen, deshalb seien Dienste wie DHL, Hermes u. ä. derzeit Deutschlands größte Drogenkuriere, wenn auch unwissentlich. Da aber vor kurzem das Zollverwaltungsgesetz verschärft wurde, dürften nun Pakete in den entsprechenden Paketzentren geöffnet und nach illegalen Inhalten untersucht werden. Ebenfalls zum Einsatz käme die sogenannte „Retrograde Abfrage von Sendungsdaten“. Aus umsatzsteuerlichen

Die Diskutanten: Gastgeber Dr. Alexander Pschera, Stefan Mey, Dr. Christian Rückert und Daniel Moßbrucker (v.l.n.r.).

Foto: CHROMORANGE/Christian Ohde/alamy stock

Das „Darknet“ hat auch sehr viele helle Stellen – die Fachleute beim Digitalen Salon sahen daher diesen Teil des Netzes überwiegend positiv.

Gründen müssten Dienste wie DHL oder Hermes Bestelldaten von Kunden bis zu zehn Jahre speichern, weswegen dieser Bestand inzwischen wertvoll für die Strafverfolgungsbehörden sei.

Daneben gebe es Cyberermittlungsmaßnahmen wie Online-Streifen und virtuelle verdeckte Ermittlungen, bei denen beispielsweise testweise Drogen bestellt und auf dem Postpaket dann möglicherweise Fingerabdrücke eines unvorsichtigen Absenders gefunden würden. Eine Ansatzmöglichkeit, selbst den TOR-Browser zu umgehen, sieht Rückert im sogenannten Zeitkorrelationsangriff und im Browserfingerprinting. Beim Zeitkorrelationsangriff wird geschaut, ob zu einem bestimmten Zeitpunkt zwei Leitungen gleichzeitig aktiv sind. Kommt dies mehrere tausend Male vor, könne man, grob gesagt, irgendwann davon ausgehen, dass diese beiden Leitungen miteinander kommunizieren und dann Rückschlüsse auf deren Aktivitäten ziehen. Beim Browserfingerprinting werden die Daten ausgelesen, die ein Endgerät mitschickt, wie der Markenname des Geräts oder die Bildschirmeinstellungen, und dann werden aus diesen Daten Rückschlüsse gezogen.

Letztendlich plädierte Rückert gegen ein pauschales Verbot des Darknets, da dies zum einen schon technisch unmöglich sei, und zum anderen in Deutschland ein Grundrecht auf Anonymität bestehe. Eine höhere Kriminalisierung führe außerdem schnell zu Kollateralschäden bei Plattformen, die sich rein politisch engagierten. Endkunden im Darknet sollten dennoch keinen Freibrief bekommen, sondern sich bewusst sein, dass die Strafverfolgungsbehörden aufmerksam sind; und er selbst, so Rückert, arbeite als Jurist daran mit, dass die Methoden der Strafverfolgung datensensibler und grundrechtschonender würden.

Zum Schluss ging der Berliner Journalist Daniel Moßbrucker auf „die helle Seite im dunklen Netz“ ein – „und was noch fehlt, damit das Darknet für die Masse attraktiv wird“. Neben den Themen Digitalisierung, Überwachung und Datenschutz ist er seit längerer Zeit bei „Reporter ohne Grenzen“ aktiv und betreibt neben der üblichen Basisarbeit auch politischen Aktivismus und ist in Gesetzgebungsverfahren involviert. Anhand zweier Beispiele aus Marokko und China verdeutlichte Moßbrucker in seinem Statement die Situation politischer Dissidenten und Exil-Journalisten, die über das Darknet Informationen austauschen oder Zugriff auf westliche Suchmaschinen bekommen. Auch nutzten diese das Netzwerk von TOR für das Ablegen von Daten, falls die örtliche Polizei in der eigenen Wohnung eine Durchsuchung vornimmt.

Doch selbst in Zeiten von TOR gelinge es verschiedenen Ländern inzwischen, den Zugang zu diesem anonymisierten Netzwerk für Nutzer zu blockieren, doch sei es ebenso technisch möglich, durch „TOR Bridges“ diese Blockaden zu umgehen. Davon würden die Nutzer hauptsächlich im Iran, in Ägypten und vermehrt auch in der Türkei Gebrauch machen.

In den Augen westlicher Medien stehe das Darknet für eine Art „Parallelwelt für alles Gute in der Welt“, insbesondere für die Whistleblower, doch momentan stehe es, gerade im Bereich des Journalismus, mehr für eine Brückentechnologie: es gebe wenige Medien, die selbst aus Ländern wie Iran, Ägypten oder Türkei berichteten, dafür vielmehr die Informationen von Exiljournalisten nutzten, deren heimliche Hauptstadt im Moment Berlin sei.

Das Darknet insgesamt, so Moßbrucker, sei für den großen Einsatz (noch) ungeeignet, da es keine nennenswerte Reichweite habe, weil es zu wenige Nutzer habe, und technisch teilweise zu langsam sei. Relevante Inhalte müssten langfristig ins normale Internet eingespeist werden, um viele Menschen zu erreichen. Dennoch sieht er eine Möglichkeit, das Darknet mehr zum Mainstream zu machen, was er am Beispiel von Messengerdiensten wie WhatsApp, Signal oder dem Facebook Messenger verdeutlichte: bisher würden dort nur die ausgetauschten Inhalte verschlüsselt, d.h. man wisse nicht, was zwei Menschen kommunizieren, aber man sähe nach wie vor anhand der IP-Adressen und anderer Metadaten genau, wer mit wem kommuniziere. Deshalb flögen auch Journalisten nach wie vor auf, die diese Messengerdienste nutzten. Verschlüsselten diese Dienste auch die Metadaten, käme es zu einer neuen Form von Anonymisierung, so dass ein viel höherer Datenschutz für alle gegeben sei. Es gebe sogar bereits ein EU-gefördertes Forschungsprojekt, das daran arbeite, die Darknet-Technologie in bereits bestehende Systeme zu implementieren statt ständig Neues zu entwickeln – so könnte diese Technologie irgendwann ganz regulärer Bestandteil moderner Kommunikation sein. □

Akademiestudienleiterin Dr. Astrid Schilling, die die Reihe Digitaler Salon verantwortet, begrüßte die rund 80 Teilnehmerinnen und Teilnehmer.