Braucht eine digitale Gesellschaft eine digitale Polizei?

Von Petra Saskia Bayerl, PhD und Thomas-Gabriel Rüdiger, M.A.

Internet, soziale Medien und digitale Neuerungen bestimmen mittlerweile unser Leben. Von Online-Einkäufen und digitalen Marktplätzen zu Beziehungsanbahnungen über Tinder, neuen Formen des Arbeitens im Rahmen von Crowdsourcing bis zum Einsatz erweiterter und virtueller Realitäten für Therapien und berufliche Trainings oder der Freizeitgestaltung, beispielhaft zu erkennen an der Verlagerung von Musik, Film und Video zu Online-Streaming oder den 34 Millionen Nutzern digitaler Spiele allein in Deutschland. Gemäß neuester Zahlen einer Online-Erhebung von ARD und ZDF nutzen 83,8 Prozent der Deutschen das Internet in seinen unterschiedlichsten Facetten.

Dabei zeigt sich ein differentes Nutzungsverhalten zwischen Generationen: so nutzen Erwachsene eher klassische soziale Netzwerke wie Facebook und Twitter, Kinder und Jugendliche setzen – neben den genannten digitalen Spielen – hingegen verstärkt auf Bild- und Medienplattformen wie Instagram und Snapchat. Lediglich Youtube und WhatsApp werden von allen Altersstufen annähernd gleich genutzt. Diese Medien formen eine Art digitalen öffentlichen Raum, der es ermöglicht, dass Menschen jeglichen Alters und Herkunft miteinander in Interaktion treten, faktisch ohne physische Grenzen wahrzunehmen. Lediglich Sprachgrenzen scheinen sich im Internet zu halten.

Die Schnittfläche zwischen online und offline ist bereits heute verwischt und die Unterscheidung zwischen digitalem und realem Lebensraum damit größtenteils illusorisch. Pure Online-Beziehungen sind für viele heute ebenso selbstverständlicher Teil ihres Freundschaftsbegriffs wie Beziehungen zu Menschen, die sie von Angesicht zu Angesicht kennen. Automatische Algorithmen

versuchen Einfluss auszuüben auf die Information, die wir lesen, die Leute, die wir einstellen, unser Kaufverhalten und über Social Bots sogar unsere Wahlentscheidungen.

Manche Gemeinden in den Niederlanden setzen gezielt automatisierte Systeme ein, um potenzielle „Problemfamilien“, mögliche Steuerhinterzieher oder Betrüger bei Sozialleistungen zu identifizieren, möglichst bevor diese überhaupt dazu kommen, solche Taten zu begehen. In China soll hingegen bis 2020 ein „Social Scoring System“ eingerichtet werden, dass den Verhaltensweisen von Menschen einen Wert zuschreibt. Wer beispielsweise Normen bricht wie über eine rote Ampel zu gehen oder Steuern zu hinterziehen oder auch einfach zu viel Computer zu spielen, erhält negative Punkte. Dies soll sich dann auf die Job- und Wohnungsvergabe und Ähnliches auswirken. Hierzu sollen alle vorhandenen digitalen Datenbanken verbunden werden – der Gang zu vermeintlichen Vorhersage von Kriminalität ist dann nur eine Frage der Zeit. Minority Report lässt grüßen. Bereits heute werden chinesische Polizisten mit Google-Glasses ausgerüstet, um Tatverdächtige effektiver finden zu können. Die Brillen sind mit der zentralen Datenbank verbunden und ermöglichen so die automatische Gesichtserkennung (potenzieller) Straftäter.

Digitale Polizeipräsenz hat zugenommen, aber …

Wo aber in diesen digitalen Lebensräumen sind die deutschen Sicherheitsbehörden Teil der digitalen Realität? Die Präsenz deutscher Polizeien auf sozialen Medienplattformen hat zunächst in den letzten Jahren zugenommen, trotzdem scheinen viele andere Bereiche, die für Bürger inzwischen zum normalen Alltag gehören, immer noch eine Art No Go Area zu sein. Es scheint an einer grundsätzlichen gesellschaftlichen Debatte darüber zu fehlen, ob die Sicherheitsbehörden tatsächlich auch Teil einer digitalisierten Gesellschaft sein sollen, und wie deren Teilnahme aussehen sollte und könnte.

Eines scheint jedoch festzustehen: Diese Entwicklungen werden auch die Polizeiarbeit in Deutschland in einer Art und Weise verändern, wie sie jetzt noch gar nicht vollumfänglich erfasst werden kann. Gegenwärtig scheint sich die Auseinandersetzung mit einer digitalen Polizeipräsenz in Deutschland dennoch vor allem auf zwei Felder zu konzentrieren: die Aktivitäten von Polizeibehörden rund um soziale Medien und die Bekämpfung von Cybercrime-Delikten im engeren Sinne. Dies erfolgt aber ohne, dass die Sicherheitsbehörden in diesem digitalen Raum auch tatsächlich tiefergehend verankert wären.

Dabei ist es nachvollziehbar, dass eine unkritische Übernahme jeder technologischen Innovation, die gerade neu auf den Markt kommt und verspricht Polizeiarbeit einfacher und Entscheidungen (weil Algorithmen-basiert) objektiver zu machen, nicht der einzuschreitende Weg sein kann. Dazu gibt es zu viele Beweise von zumindest diskussionswürdigen Entscheidungen durch und Voreingenommenheiten in solche Anwendungen (siehe zum Beispiel die Debatte um die Fehlerhaftigkeit automatischer Gesichtserkennungssoftware, die manche Polizeien in Großbritannien einsetzen oder eingesetzt haben).
Es bedarf daher einer reflektierten Diskussion über die Möglichkeiten der Digitalisierung der deutschen Sicherheitsbehörden, vor allem der Polizei, und über deren Rolle in einer Gesellschaft, in der der (globale) digitale Raum ein ganz selbstverständlicher Teil des Alltags geworden ist. Diese Diskussion sollte weder getrieben sein von Technologiegläubigkeit, noch von irrealen Ängsten vor Robocops (zumindest noch). Die Fragen, die gestellt werden müssen, haben vielmehr zu tun mit einer klaren Positionierung von Polizei, mit der Schaffung eines gesellschaftlichen Konsensus über diese Position, sowie mit der Schaffung angemessener organisationaler wie rechtlicher Rahmenbindungen, als Voraussetzungen für die Umsetzung einer umfassenden digitalen Polizeiarbeit.

Die Krux mit der Rechtsfreiheit im Internet

Die Debatte über Polizei in einem digitalen Raum kann auch an der Frage fest gemacht werden, ob das Internet nun ein rechtsfreier Raum ist oder nicht. Bereits im Jahr 2010 hatte Bundeskanzlerin Angela Merkel in einem Podcast die Aussage getroffen, das Internet „sei kein rechtsfreier Raum“. Im Februar 2018 hat sie diese Aussage erneut in demselben Podcast wiederholt. Welchen Bedeutungs- und Aussagewert hat die stetige Wiederholung einer solchen Floskel?
Diese Aussage wird ja nicht nur durch die Bundeskanzlerin getroffen, sondern in fast allen Pressemitteilungen, Interviews oder Artikeln im Zusammenhang mit Internet- und Cybercrime-Phänomenen. Wenn ein Raum in der Tat kein rechtsfreier ist, dann muss dies vermutlich auch nicht über mehrere Jahre wiederholt werden, denn dann wäre es irgendwann eine Selbstverständlichkeit. Wenn das Internet aber doch einem rechtsfreien Raum ähnelt, muss untersucht werden woran dies liegt.

Bereits US-Präsident Abraham Lincoln wusste, dass es nicht darauf ankommt, ob Recht gilt, sondern darauf, dass dieses Recht mit einer gewissen Wahrscheinlichkeit auch durchgesetzt wird. In seinen Worten: „Law without enforcement is just good advice“ wird dies deutlich. Daher stellt sich die offensichtliche Frage, ob die Durchsetzung – das heißt, die strafrechtliche Verfolgung von Delikten im digitalen Raum – noch nicht stark genug erfolgt, und es somit als notwendig erscheint, betonen zu müssen, dass der digitale Raum „kein rechtsfreier Raum“ sei. Einige Zahlen können dabei helfen, sich der Thematik zu nähern.
Für das Jahr 2017 erfasste die Polizeiliche Kriminalstatistik (PKS) insgesamt 85.960 angezeigte Cybercrime-Delikte im engeren Sinne und 251.617 Delikte im weiteren Sinne. Diese recht geringen Fallzahlen haben unter anderem mit den Anzeigemodalitäten der PKS zu tun. So weist das Bundeskriminalamt selbst darauf hin, dass beispielhaft der Cyberangriff auf circa 1,2 Millionen DSL-Router mit einer siebenstelligen Anzahl an Opfern lediglich als ein (!) einziger Fall der Computersabotage in die PKS Eingang gefunden hat. Das Dunkelfeld – also die

Delikte, die nicht den Strafverfolgungsbehörden und gegebenenfalls auch den Betroffenen selbst nicht zur Kenntnis gelangen – sei demnach durch die PKS kaum einzuschätzen, liege aber vermutlich um ein Vielfaches höher. Eine aktive rechtstaatliche Aufhellung dieses Dunkelfeldes wird offenbar noch nicht hinreichend betrieben.

Hinweise deuten tatsächlich auf ein gigantisches Dunkelfeld. So berichtete die Bundeswehr nach Angaben des „Spiegel“ alleine im Jahr 2015 knapp 71 Millionen Cyber-Angriffe auf ihre kritischen Infrastrukturen. Dass solche Zahlen nicht unrealistisch sind, legen auch verschiedene andere Studien nahe. Nach einer repräsentativen Umfrage des Branchenvertreters Bitkom wurde im Jahr 2017 jeder zweite Deutsche ab 14 Jahren Opfer eines Cybercrime-Delikts. Was im Umkehrschluss Millionen begangener Delikte bedeutet – betroffene Kinder nicht eingerechnet. Nach einer Studie des Softwareunternehmens Symantec fielen 2017 23,4 Millionen Menschen in Deutschland Cyberkriminellen zum Opfer. Dabei erfasst diese Studie noch nicht einmal die digitalen Delikte, die aus zwischenmenschlichen Handlungsweisen entstehen – also Cybercrime im weiteren Sinne wie Hatespeech, Cybermobbing oder Cybergrooming. Vermutlich kann sich jeder selbst fragen, wie häufig zum Beispiel Phishing-E-Mails im eigenen E-Mail-Konto landen – ganz zu schweigen von solchen, die bereits von der Firewall abgeblockt werden.

Wird das Blickfeld auch auf Cybercrime-Delikte im weiteren Sinne ausgeweitet, vergrößert sich die tatsächliche Diskrepanz noch. So gibt das Bundesministerium für Justiz in seiner Begründung zum Netzwerkdurchsetzungsgesetz (NetzDG) im Mai 2017 an, dass jährlich „mindestens 500.000 Beschwerden […] wegen Hasskriminalität und anderen strafbaren Inhalten“ eingehen. Studien deuten auch bei diesem Delikt auf ein immenses Dunkelfeld hin. So kam der Wissenschaftler Graven Titley bereits im Jahr 2015 zu dem Ergebnis, dass 36,5 Prozent der befragten Internetnutzer bereits einmal direkt mit Hasskriminalität konfrontiert wurden, was sich mit den Resultaten einer US-amerikanischen Studie von Dugan

im Jahr 2014 deckt. Nach einer Studie der Landesanstalt für Medien Nordrhein-Westfalen (LfM) gaben in Deutschland 91 Prozent aller 14 bis 27-Jährigen an, mindestens einmal damit konfrontiert worden zu sein. Dies entspricht vermutlich Fallzahlen im sechs- bis siebenstelligen Bereich. Im Gegenzug dazu gab es im Jahr 2016 lediglich 3.331 Anzeigen wegen Volksverhetzung über das Tatmittel Internet – wobei in diesem Jahr erstmalig mehr Volksverhetzungen über das Internet als im physischen Raum angezeigt wurden – und im Jahr 2017 konnte in der PKS sogar ein Rückgang auf 2.384 Strafanzeigen festgestellt werden.

Eine Studie der Soziologin Lea Stahel kommt zudem zu dem Ergebnis, dass die Mehrzahl der Täter mit Klarnamen handeln – wohl um Anerkennung für ihre Äußerungen zu erhalten, was jedoch auch die strafrechtliche Ermittlungsarbeit erleichtert. Dies könnte ein Teilgrund für die relativ hohe Aufklärungsquote von etwa 70 Prozent sein.

Ähnliche Ergebnisse gibt es auch für die onlinebasierte Anbahnung des sexuellen Missbrauchs eines Kindes nach Paragraf176 Abs. 4 Nr. 3 und 4 Strafgesetzbuch (StGB) – das sogenannte Cybergrooming. Für das Jahr 2017 ergab die PKS 1.080 Anzeigen in diesem Bereich. Dunkelfeldstudien deuten jedoch darauf hin, dass in einer konservativen Auslegung jedes dritte – das Internet nutzende – Kind in Deutschland von solchen Erfahrungen berichten kann, was eine Deliktzahl im sechs- bis siebenstelligen Bereich bedeuten würde. Solche Vergleiche ließen sich für eine Vielzahl von Delikten fortführen – von Beleidigungen bis Urheberrechtsverletzungen. Es zeigt sich stets eine immense Diskrepanz zwischen Hell- und Dunkelfeld.

Dabei ist es an sich nichts Außergewöhnliches, das das Dunkelfeld größer ist als das Hellfeld. Die Kriminologen Karl-Ludwig Kunz und Tobias Singelnstein gehen beispielhaft von einer ungefähren Anzeigequote für den physischen Raum von 1 zu 10 aus. Auch wenn es nicht „das eine“ Cybercrime-Delikt gibt, so sind die Quoten für den digitalen Raum gemäß des bereits Dargestellten allerdings exorbitant höher

als für den physischen Raum. Vermutlich kann hier nach einer eigenen Einschätzung eine Dunkelzifferrelation von etwa 1 zu 300 angenommen werden.
Damit geht einher, dass die Wahrscheinlichkeit für ein onlinebasiertes Delikt angezeigt und damit auch verfolgt zu werden, offenbar im überschaubaren Bereich liegt.
Es muss zudem bedacht werden, dass eine Vielzahl an Delikten im Internet nicht verdeckt oder unsichtbar stattfinden, sondern sichtbar und häufig auch in Form von Kommentaren oder Ähnlichem gerade in Sozialen Medien öffentlich fixiert ist. Diese Sichtbarkeit – beispielhaft im Rahmen von Hatespeech, sexuellen Kommentaren oder Beleidigungen – auf die keine gleichgeartete, sichtbare Reaktion erfolgt, kann bei anderen Nutzern zum Absinken der Hemmschwelle einer Tatbegehung führen, da die Begehung eines Deliktes nur mit einem geringen Risiko verbunden scheint. Dieser Umstand kann in Anlehnung an die Broken Windows Theorie auch als „Broken Web“ bezeichnet werden, nach der die Masse an sichtbarer Tatbegehung im Internet zu einer Herabsenkung der Hemmschwelle der Nutzer insgesamt führen kann, was zu weiteren Tatbegehungen führt, die wiederum eine Art Kreislauf auslöst.

Es stellt sich nun die Frage, wie die Sicherheitsbehörden diesen Entwicklungsprozessen begegnen können. Die Zeitschrift „Der Spiegel“ hat im Mai dieses Jahres für einen Beitrag alle deutschen Polizeien um die Mitteilung gebeten, wie viele Polizisten für die Bekämpfung und Ermittlung im Cybercrime Bereich eingesetzt werden. Demnach waren im Dezember 2017 insgesamt 1.823 Polizisten bundesweit für Cybercrime zuständig. Nach Angaben des Statistischen Bundesamtes waren im Jahr 2015 rund 311.000 Beschäftigte im Polizeibereich tätig; mit der aktuellen Entwicklung kann sogar von einer Steigerung des Personalbestandes ausgegangen werden. Dies entspräche einem Personalansatz für digitale Delikte von lediglich 0,58 Prozent aller Beschäftigten für einen Raum, in

dem die Menschen statistisch gesehen mehr Zeit verbringen als im physischen Straßenverkehr.
Dabei würden eine Steigerung dieser Personalquote und eine höhere digitale Polizeipräsenz vermutlich nicht zu einem Rückgang der Kriminalitätsraten in den Statistiken führen. Im Gegenteil kann vermutet werden, dass das bekannte Lüchow-Dannenberg-Syndrom auch auf den digitalen Raum übertragen werden kann. Demnach führt ein Mehr an polizeilicher Arbeit und Präsenz zu einer Steigerung des Vertrauens in den Rechtstaat sowie zu häufigeren Eigenfeststellungen durch Beamte. Beides würde sich in gesteigerten Anzeigeraten widerspiegeln.

Das aber eine solche Steigerungen durchaus sinnvoll wäre, manifestiert sich unter anderem darin, dass die Anzeigeraten bei digitalen Delikten gegenwärtig relativ gering sind. So ergab die zitierte LfM Studie auch, dass lediglich 8,5 Prozent der Opfer von Hatespeech überhaupt eine Anzeige in Erwägung ziehen würden. Diese Quote stimmt wiederum mit der allgemein für Cybercrime angenommen Anzeigerate überein, die bei ca. 9 Prozent liegen soll.[29] Letztlich stellen vielen Formen von Cybercrime Kontrolldelikte dar, die nur zu einem geringen Prozentsatz ohne aktive Maßnahmen des Rechtstaates ins Hellfeld gelangen.
Insgesamt ergibt sich das Bild, dass nur ein geringer Prozentsatz des Personals der Sicherheitsbehörden im digitalen Raum aktiv ist, und im Gegenzug auch die Anzeigeraten und damit letztlich das Hellfeld niedrig ist. Das digitale Hellfeld ist dabei nicht vergleichbar mit dem im physischen Raum, da die Dunkelzifferrelation in Letzterem viel geringer ist als im digitalen Raum. Dies führt zu der beschriebenen Situation, dass Nutzer offenbar ein Gefühl der Rechtsfreiheit im Internet entwickelt haben.
Die Verabschiedung des Netzwerkdurchsetzungsgesetzes (NetzDG) am 1. September 2017 kann deshalb auch so interpretiert werden, dass die klassischen Rechtsdurchsetzungsmechanismen bei Straftaten für den digitalen Raum offenbar als nicht ausreichend erachtet wurden. Wären von den 500.000 in der

Gesetzesbegründung angenommenen Delikten auch nur 20 Prozent zur Anzeige gekommen, wären das bereits mehr als alle registrierten Cybercrime-Delikte im engeren Sinne in ganz Deutschland in einem Jahr. Popitz sprach in einem vergleichbaren Zusammenhang auch einmal von der „Präventivwirkung des Nichtwissens“.[30]

Wer also tatsächlich aus einem digitalen Raum einen Rechtsraum machen möchte, muss in irgendeiner Form die Akzeptanz und Sichtbarkeit des Rechtstaates in diesem erhöhen und damit das Dunkelfeld zurückdrängen. Proll hatte dies 2016 in einem Artikel im Behördenspiegel treffend formuliert: „Wenn das Internet kein rechtsfreier Raum ist, wie es die Politik immer wieder postuliert, dann muss sie auch für die notwendige Strafverfolgung in diesem Raum sorgen“.[31] Gleichzeitig hat er gefordert, dass tausende Polizisten im Internet hierfür eingesetzt werden müssen – nicht nur zur Strafverfolgung, sondern auch zur sichtbaren Präsenz.[32]

Dabei ist ein Vergleich zum Straßenverkehr naheliegend. Die Einhaltung von Regeln wird auch hier dadurch erreicht, dass es eine gewisse Wahrscheinlichkeit gibt, dass ein Verstoß geahndet wird und das der Rechtstaat sich sichtbar durch Polizei – beispielsweise durch Polizeiwachen und sichtbaren Polizeistreifen – und Regeln – beispielsweise durch Verkehrszeichen und Ampeln – manifestiert. Vermutlich kennt jeder das Phänomen des schlagartig absinkenden Handyarms, wenn ein Autofahrer eine Polizeistreife sieht, die Bereitschaft zur Einhaltung der Geschwindigkeit, wenn die Polizei oder ein stationäres Messgerät ins Sichtfeld gerät, oder auch nur die Frage, ob in Gegenwart eines Polizisten Fußgänger bei Rot über die Ampel gehen. Gleichzeitig ist eine klassische Reaktion auf das Aufkommen von Orten mit Kriminalitätsschwerpunkten, uniformierte Polizisten zu entsenden. Diese zeigen für alle sichtbar, dass der Staat sein Gewaltmonopol wahrnehmen und verteidigen will. Dabei ist naheliegend, dass diese Wirkungen von der tatsächlichen visuellen Erkennbarkeit abhängen, denn obwohl auch Polizisten in Zivil objektiv die Sicherheit erhöhen, entfalten sie doch offenbar nicht dieselbe psychologische Wirkung auf die Gesellschaft.[33]

Polizeiliche Präsenz im digitalen Raum: Zahlen und Beispiele

Eine solche visuelle und flächendeckende Präsenz im digitalen Raum – oder zumindest in einem deutschsprachigen Raum – herzustellen, scheint eine intensive Diskussion zu erfordern und kann letztlich über zwei primäre Formen stattfinden: einerseits durch die Etablierung offizieller polizeilicher Accounts, andererseits durch virtuelle Polizeistreifen. Ersteres passiert derzeit vor allem auf Sozialen Medien, das heißt, onlinebasierten Programme, die nutzergetriebene Inhalte sowie direkte Nutzerinteraktionen und -kommunikation ermöglichen.

Die Präsenz von Sicherheitsbehörden auf Sozialen Medien nimmt kontinuierlich zu. Gab es im Jahr 2012 in Deutschland gerade einmal 81 polizeiliche Accounts, waren es Anfang 2017 bereits 216.[34] Gegenwärtig kann von circa 300 Accounts ausgegangen werden, wobei circa 95 Prozent davon auf Facebook und Twitter und der Rest vornehmlich auf Instagram und Snapchat entfallen.

Obwohl diese Entwicklung als positiv zu bewerten ist, ergibt ein internationaler Blick doch ein etwas anderes Bild. Die niederländische Polizei, die circa 65.000 Polizeiangehörige besitzt, betreibt alleine auf Twitter 2.200 Accounts, die von 3.400 sog. „Wijkagenten“ (grob zu übersetzen mit „Bezirks-„ oder „Revierpolizisten“) bedient werden. Insgesamt besitzt die niederländische Polizei derzeit ca. 2500 Accounts in unterschiedlichen Sozialen Medien.[35] Die Beamten nutzen diese dienstlichen Accounts, um einerseits Präsenz zu zeigen und andererseits eine direkte Kommunikation mit den Bürgern ermöglichen.

Die oben genannten Zahlen bedeuten, dass alleine 5,23 Prozent der niederländischen Polizisten auf sozialen Medien persönlich aktiv sind – wobei die traditionellen Cybercops damit noch gar nicht erfasst sind. Übertragen auf die deutsche Polizei entspräche dies in etwa 16.265 Polizeiangehörigen. Dies mag auf den ersten Blick utopisch erscheinen, aber auch die Bundeswehr hat sich entschieden, bei einer ungefähren Personalzahl von 180.000 Angehörigen bereits jetzt 12.613 Personen im neugeschaffen Bereich „Cyber- und Informationsraum“

(CIR) einzusetzen.[36] Dies entspricht einer Quote von 7 Prozent des Personalbestandes. Auf die deutsche Polizei übertragen wären die sogar 21.770 Beamten.

Das Konzept eines „digitalen community policing“ ist in Deutschland erst in den Anfängen. Ende 2016 ist mit dem niedersächsischen Polizeidirektor Johannes Lind der erste Beamte gestartet, der dienstlich mit seinen eigenen Accounts bei Facebook[37] und Twitter[38] diese Form der bürgernahen Polizeiarbeit betreibt. Mittlerweile gibt es in Niedersachsen immerhin schon zehn Beamte, die solche individuellen Accounts – vornehmlich auf Facebook – betreiben. Die niederländischen Beamten werden auch aktiv und sichtbar auf virtuelle Polizeistreife geschickt, um Straftaten zu suchen und damit das Dunkelfeld aufzuhellen[39]; ein Konzept, dass die Polizei des Landes Sachsen-Anhalt nun auch in Form einer 12-köpfigen virtuellen Polizeistreife aufgenommen hat, die sichtbar gegen Hatespeech vorgehen soll.[40,41] Ähnliche Vorschläge für eine virtuelle Polizeistreife kamen auch bereits aus dem saarländischen[42] und brandenburgischen Landtag[43].

Die Nutzung innovativer digitaler Mittel, inklusive aber nicht ausschließlich Sozialer Medien, durch die Polizei ist international also schon längst Realität. Polizeiliche Angebote auf Plattformen wie Facebook, Twitter, YouTube, WhatsApp, Instagram, Snapchat oder flickr, um nur einige zu nennen, sind inzwischen ein normaler Bestandteil der Polizeiarbeit weltweit – von Informationskampagnen in Dubai über Mitarbeiterwerbung in den Philippinen zu tanzenden Polizisten in Neuseeland und Weihnachtsgrüßen aus Finnland.[44] Als Teil von Open Source Intelligence (OSINT) sind Informationen von Sozialen Medien inzwischen auch selbstverständlicher Bestandteil strafrechtlicher Untersuchungen[45] und können auch bei Rekrutierungsentscheidungen einbezogen werden.

Abseits sozialer Medien finden sich international weitere innovative Ansätze. Dies sind nicht nur die bereits erwähnten Google-Glasses der chinesischen Polizei. Die Polizei in Dubai experimentiert derzeit mit Künstlicher Intelligenz (KI) in

Polizeifahrzeugen und Robotern.[46] Das MI5 in Großbritannien wirbt Kandidaten mit Hilfe eines Online-Spiels unter dem Motto „Do you have the skills to become a Mobile Surveillance Officer?“. [47] Und auch Serious Games, zum Beispiel als virtuelle Szenarien für Waffentrainings, werden zu einem stetig wachsenden Markt, etwa in den USA.[48]

Dies öffnet die Frage, wieso eine Entwicklung in diese Richtung, die mit dem internationalen Blick durchaus folgerichtig wäre, in Deutschland offenbar nur zögerlich vollzogen wird?

Vor fünf Jahren wurden in einem Artikel in dieser Zeitung mit einem leicht abgewandelten Autorenpaar bereits einige Vorhersagen für die digitale Polizeipräsenz getroffen, die mittlerweile auch eingetreten sind – etwa dass alle Polizeibehörden flächendeckend Soziale Medien nutzen werden und das diese wichtige Eckpunkte der polizeilichen Arbeit werden.[49] Gleichzeitig wurde bereits damals auf die primären Gründe eingegangen, warum die Digitalisierung der Sicherheitsbehörden trotz erster Fortschritte insbesondere im internationalen Vergleich noch eher zurückhaltend ist. Hierbei wurden drei Aspekte herausgearbeitet: Politischer Wille, Ressourcenfragen (vor allem Personal und Budget) und Rechtsfragen. Diese sind (leider) nach wie vor gültig.

Hürden der Digitalisierung – Politik, Ausstattung und Recht

Eine tatsächliche tiefgehende Digitalisierung der Sicherheitsbehörden bedarf einer grundsätzlichen gesellschaftlichen und politischen Debatte über die Rolle und Funktion von Normen und der Normenkontrolle in einem globalen digitalen Raum. Eine solche übergreifende Debatte fehlt bisher jedoch weitgehend. Auch müssten die Gesellschaft und die Politik es aushalten, dass eine gesteigerte Präsenz der Sicherheitsbehörden im digitalen Raum zu massiv steigenden Fallzahlen (im Hellfeld), bei einer vermutlich sinkenden Aufklärungsquote innerhalb der PKS führen wird. Dazu müsste die Erkenntnis reifen, dass sowohl die Zurückdrängung des Gefühls der Rechtsfreiheit als auch die Etablierung einer der damit

einhergehenden Art digitale Generalprävention diese Präsenz der Sicherheitsbehörden und der damit einhergehenden Aufhellung des Dunkelfelds im digitalen Raum erfordert. Ohne eine solche politische Akzeptanz wird eine grundsätzliche Ausrichtung der Sicherheitsbehörden für diese digitalen Fragen schwierig. Dieser Umstand führt zu einem weiteren Punkt: der Ausstattungsfrage.

Wie aufgezeigt, muss bei einer fortschreitenden Auseinandersetzung der Sicherheitsbehörden mit dem digitalen Raum durch Aufhellung des Dunkelfelds zwangsläufig mit einer höheren Anzeigenzahl gerechnet werden. Nicht umsonst steigen jährlich die Anzeigen im Bereich der Kinder- und Jugendpornografie über das Tatmittel Internet, unter anderem da durch die Internationalisierung vieler Fälle durch Ermittlungen anderer Länder ausgelöst werden. Es kann also davon ausgegangen werden, dass Delikte aus dem digitalen Raum bei einer fortschreitenden polizeilichen Digitalisierung in der nahen Zukunft einen wesentlichen Anteil der Strafanzeigen ausmachen werden. Dies erfordert wiederum einen höheren Personalansatz – auch bei der Justiz – und gleichzeitig die Bereitstellung einer dafür notwendigen technischen Infrastruktur sowie den Ankauf oder die Entwicklung entsprechender unterstützender Software für die unterschiedlichsten Bereiche. Dabei muss auch bedacht werden, dass die breite Masse dieser Entwicklungen nicht die spezialisierten IT-Experten innerhalb der Polizei betreffen, sondern jeder Polizist immer mehr mit digitalen Themen und Straftaten konfrontiert wird. Dies erfordert letztlich die Sicherstellung einer Art flächendeckenden polizeilichen Medienkompetenz.

Hierbei sollte sich auch nicht darauf verlassen werden, dass junge Beamten dies einfach Kraft ihrer Jugend und einem ‚digitalen Heranwachsen' von selbst mitbringen. Diese Gruppe hat oft eben keine Medienkompetenz institutionalisiert vermittelt bekommen, wie die erst jetzt wirklich stattfindende Debatte um Medienbildung in der Schule im Umkehrschluss offenbart. Vielmehr beherrschen gerade junge Menschen offenbar häufig eher eine Wisch- als eine reflektierte Medienkompetenz.[50] Es erscheint daher naheliegend, dass die Vermittlung einer

verpflichtenden polizeilichen Medienkompetenz für Polizeianwärter notwendig sein wird, um der Digitalisierung Rechnung zu tragen.

Gleichzeitig zeigt sich, dass es international üblich wird, Polizeibeamte mit dienstlichen Smartphones oder mit den entsprechenden Applikationen – wie polizeiliche Messenger – für private Smartphone auszustatten. Beispielsweise hat Österreich kürzlich 30.000 Smartphones mit entsprechenden polizeilichen Applikationen für alle Polizeibeamten angeschafft.[51] In Deutschland existieren zwar einige Pilotprojekte wie in der Polizei des Landes Niedersachsen[52], dass aber alle Polizisten in Deutschland mit entsprechenden Smartphones oder Apps ausgestattet würden, ist gegenwärtig nicht ersichtlich. Der damalige österreichische Innenminister hat hierzu eine interessante Aussage getroffen: „Wir trauen Polizisten zu, mit einer Waffe umgehen zu können. Also werden sie auch mit Handys umgehen können“.[53]

Eine noch utopische Strategie, um der Masse an Delikten und der Tendenz zur Automatisierung und Entmenschlichung von Kriminalität im digitalen Raum zu begegnen, könnte in einer Automatisierung der digitalen Polizeiarbeit liegen. So könnten in ferner Zukunft im digitalen Raum Polizeibots und künstliche Intelligenz (KI) eingesetzt werden, die automatisch und eigenständig gegen Normenüberschreitungen vorgehen.[54] Eine ähnliche Entwicklung lässt sich bereits im Bereich der Auswertung von Massendaten nachvollziehen. Unabhängig davon, welchen Weg die Entwicklung einschlägt, wird die polizeiliche Digitalisierung massive finanzielle und personelle Ressourcen bedürfen, die wiederum durch die Politik bereitgestellt werden müssen.

Die rechtlichen Rahmenbedingungen stellen die dritte große Hürde der polizeilichen Digitalisierung dar. Neben der allgegenwärtigen Thematik des Datenschutzes[55] ist insbesondere das Legalitätsprinzip mit seinem Absolutheitsanspruch auch im digitalen Raum eine kaum zu überwindende Hürde für eine flexible Polizeiarbeit.[56] Das Legalitätsprinzip in Kombination mit dem Tatbestand der Strafvereitelung im Amt ist ein Konstrukt, dass für die Regeln des öffentlichen physischen Raumes

geschaffen wurde. Es basiert im Kern auf der Grundüberlegung, dass die Sicherheitsbehörden nur mit einem kleinen Teil der tatsächlich begangenen Delikte konfrontiert werden, diese aber dann ohne jede Gewichtung zu verfolgen haben. Eine signifikante Dunkelfeldaufhellung (über das Streifenfahren hinaus) war nie grundlegender Bestandteil der Polizeiarbeit – und Personal, Ressourcen und der Rechtsrahmen haben sich an diesem Prinzip ausgerichtet. Im digitalen Raum aber ist es für Jeden möglich, mit ein paar Mausklicks oder Fingertippen das Dunkelfeld selbst massiv aufzuhellen.

Hinzu kommt, dass nicht der Polizist die Verjährung eines Deliktes feststellt, sondern die Staatsanwaltschaft. Man stelle sich ein Forum mit strafrechtlich relevanten Kommentaren vor, das 10 Jahre in die Vergangenheit reicht. Es erscheint illusorisch anzunehmen, dass die Sicherheitsbehörden so viel Personal bekommen, dass sie mit klassischen Mechanismen dieser Masse an Informationen und Delikten bewerkstelligen könnten. Vielmehr scheint es notwendig, dass Sicherheitsbehörden im digitalen Raum Schwerpunkte setzen können, was sie zu verfolgen haben und was nicht. Es gebe hier mehrere Möglichkeiten: So könnte das Legalitätsprinzip im Rahmen einer gesellschaftlichen Debatte für das Internet zu einem Opportunitätsprinzip fortentwickelt werden, die Gültigkeit könnte nur auf Verbrechen beschränkt werden oder es wird thematisiert, welche Delikte tatsächlich im Internet als Straftaten qualifiziert werden sollen.[57]

Aber nicht nur das Legalitätsprinzip stellt einen Diskussionspunkt dar. Krischock hat sich kürzlich der Frage angenommen, inwiefern die Polizeigesetze der Länder im Sinne einer Verbrechensverhütung und letztlich Gefahrenabwehr auch im digitalen Raum zur Anwendung kommen können. Sie kommt dabei zu dem Ergebnis: „Äußerst unbefriedigend ist die Situation, dass die Polizei schon aufgrund mangelnder Zuständigkeit keine Maßnahmen treffen kann, um Straftaten im Internet zu verhüten bzw. die Fortführung zu unterbinden. Hier wird ein zentrales Handlungsfeld der Polizei völlig unbeachtet gelassen. Der Staat ist aber verpflichtet, die Bürger vor solchen Gefahren zu schützen“.[58] Die Grundproblematik ist, dass der

digitale Raum keine physischen Grenzen kennt, die Anwendung der jeweiligen Polizeigesetze aber typischerweise eine örtliche Zuständigkeit erfordern. Was bedeutet dies für die institutionelle Selbstreflexion der Landespolizeien, die sich ja besonders durch ihre jeweiligen Polizeigesetze zu einander abgrenzen, im Internet – oder sollte die Zuständigkeit für die polizeiliche Gefahrenabwehr auf die Bundesebene verlagert werden?[59]

Auch andere Fragen stehen im Mittelpunkt, etwa: Welche Rolle spielen die Sicherheitsbehörden beispielhaft bei der Durchsetzung des Kinder- und Jugendmedienschutzes in Deutschland im Sinne einer digitalen Generalprävention? Oder sollten die Sicherheitsbehörden, um Zugang zu Foren mit kinderpornografischen Inhalten zu bekommen, die Möglichkeit erhalten, kinderpornografische Darstellungen in Form von virtuellen Avataren selbst herzustellen? Können Behörden und auch die Polizei in den Sozialen Medien auf eine Art virtuelles Hausrecht zurückgreifen, um Menschen zu blockieren?[60]

Welche Form von ‚digitaler Polizei' ist nun wünschenswert?

Weltweit stehen die Polizeien in einem digitalen Umstrukturierungsprozess geprägt von einem starken Trend zur Automatisierung etwa durch Algorithmen (zum Beispiel, automatische Gesichtserkennung oder predictive policing Anwendungen), durch Einsatz Künstlicher Intelligenz (KI) oder der Hilfe durch (semi-) autonome Objekte (Fahrzeuge, Drohnen, Roboter). Daneben steht die stets weiter wachsende Verbreitung Sozialer Medien sowie virtueller oder erweiterter Realitäten.

Wie oben andiskutiert, sind viele dieser Entwicklungen in deutschen Sicherheitsbehörden höchstens angedacht, aber noch weit von den Möglichkeiten entfernt. Eine Normalisierung solcher Technologien als integraler Bestandteil von Polizeiarbeit wird vermutlich noch auf sich warten lassen, was sicherlich auch dem föderativen Charakter der deutschen Sicherheitsarchitektur geschuldet ist. Zur gleichen Zeit verdeutlichen gesellschaftliche und ökonomische Entwicklungen, dass die Digitalisierung für viele Bürger und andere Institutionen bereits zum alltäglichen

Lebens- und Berufsalltag gehört. Die Sicherheitsbehörden sind Teil der Gesellschaft und sollten demnach auch relevanter Teil der digitalen Gesellschaft sein.

Es ist durchaus zu begrüßen, dass die Sicherheitsbehörden sich eher zurückhaltend zeigen beim Einsatz von Technologien und Innovationen, die in die Privatsphäre und die Selbstbestimmungsmöglichkeiten von Bürgern eingreifen. Chinesische Zustände will hier vermutlich keiner. Und gerade Automatisierungsbemühungen werfen ja auch immer wieder die Frage auf, wer denn solche Entscheidungen noch nachvollziehen und gegebenenfalls korrigieren kann und ob diese Entscheidungen wirklich so ‚objektiv' sind, wie immer behauptet.

Auf der anderen Seite, scheint diese Vorsicht manchmal so weit zu reichen, dass auch Technologien, die schon längst gesellschaftlich selbstverständlich sind, im Sicherheitsbereich immer noch Unwohlsein auslösen. Ein Paradebeispiel ist die langsame Annäherung an Soziale Medien, die über Jahre hinweg vielfach als bloße ‚Jugend-Unterhaltung', als ‚unseriös', und deshalb nicht relevant für Polizeiarbeit angesehen wurden. Das hat sich inzwischen zum Glück geändert.

Was dieses Beispiel und allgemeiner die Diskussionen um eine umfassendere digitale Polizeiarbeit zeigt, ist, dass offenbar eine Gesamtstrategie notwendig erscheint für den Umgang mit der tiefgreifenden Digitalisierung (und damit auch Globalisierung) der Gesellschaft. Wie weit wollen deutsche Polizeien gehen, etwa in der Präsenz in Online-Spielen oder anderen bei jüngeren beliebten Sozialen Medien oder im Einsatz von autonomen Fahrzeugen oder Drohnen? Sollten Automatisierungsentscheidungen für ganz Deutschland homogen angepasst werden oder sind Unterschiede etwa im Einsatz bestimmter Kommunikationsplattformen, Software-Pakete oder KI-Anwendungen gar wünschenswert? Was, wenn Bürger Polizei-Roboter oder autonom fahrende Polizeiautos auf ihren Straßen wollen – oder gerade nicht? Und wie gehen deutsche Polizeien mit der grenzüberschreitenden Natur sozialer und wirtschaftlicher

Beziehungen und Entwicklungen um, wenn die bisherige Rechtslage dafür wenige Vorkehrungen trifft?

Digitale Präsenz ist ein Kontinuum – nicht nur von ‚abwesend' zu ‚übermächtig', sondern auch von ‚unangemessen' zu ‚dringend notwendig', sowie von ‚unakzeptabel' zu ‚gesellschaftlich erwünscht'. Was als ‚unangemessen' versus ‚dringend notwendig' oder als ‚unakzeptabel' versus ‚gesellschaftlich erwünscht' gilt, ist natürlich kein fixer Punkt auf solch einem Kontinuum. Das sind Abwägungen, die historisch fluide sind, und zumindest teilweise abhängig sind von Situationen, Personen sowie rechtlichen, organisationalen und gesellschaftlichen Rahmenbedingungen.

Dennoch braucht es – angesichts der angedeuteten technologischen und gesellschaftlichen Entwicklungen – unserer Meinung nach, ein klareres Verständnis, wie digitale Polizeiarbeit jetzt und in Zukunft gestaltet werden soll. Es geht dabei weniger um eine Positionierung im digitalen Raum, als eine Positionierung in einer Gesellschaft, in der die digitale Lebenswelt reale Lebenswelt ist. Der digitale Raum wird genauso wenig verschwinden, wie der Straßenverkehr verschwunden ist. Er ist vielmehr ein essentieller Bestandteil einer gesellschaftlichen Infrastruktur, die annähernd die gesamte Menschheit umfasst. Die Sicherheitsbehörden müssen ihre aktive Rolle und Verantwortung in diesem Raum erst noch finden.

Die Suche lohnt sich…

Fußnoten:

1 https://www.game.de/marktdaten/altersverteilung-der-nutzer-digitaler-spiele-in-deutschland/, Zugriff 16. Mai 2018

2 ARD ZDF Online-Erhebung 2016

3 ARD ZDF Online-Erhebung 2016

4 https://www.nrc.nl/nieuws/2018/04/08/algoritme-voorspelt-wie-fraude-pleegt-bij-bijstandsuitkering-a1598669; Zugriff 16. Mai 2018

5 http://www.deutschlandfunkkultur.de/vertrauensbildung-auf-chinesisch-das-social-scoring-system.1264.de.html?dram:article_id=415543, Zugriff 20. Mai 2018

6 https://techcrunch.com/2018/02/08/chinese-police-are-getting-smart-glasses/, Zugriff 16. Mai 2018

7 http://www.bbc.com/news/technology-44089161, Zugriff 16. Mai 2018

8 https://www.bundeskanzlerin.de/Content/DE/Podcast/2010/2010-02-27-Video-Podcast/2010-02-27-video-podcast-internet.html
https://www.bundeskanzlerin.de/Content/DE/Podcast/2010/2010-02-27-Video-Podcast/2010-02-27-video-podcast-internet.html ,Zugriff 16. Mai 2018

9 https://www.bundesregierung.de/Content/DE/Podcast/2018/2018-02-03-Video-Podcast/2018-02-03-Video-Podcast.html , Zugriff 16. Mai 2018

10 PKS 2017, Tatschlüssel 980100

11 PKS 2017, Grundtabelle 05

12 Bundeslagebild Cybercrime 2016, S. 3 (mittlerweile soll sich die Modalität der Registrierung geändert haben)

13 http://www.spiegel.de/netzwelt/netzpolitik/bundeswehr-71-millionen-cyberattacken-in-2015-a-1082536.html , Zugriff 16. Mai 2018

14 https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html , Zugriff 16. Mai 2018

15 Norton Cyber Security Insights Report 2017, S. 11

16 Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken v. 16.05.2017 - Drucksache 18/12358 , S.4Fehler! Hyperlink-Referenz ungültig.

17 Titley, Graven 2015, No Hate Survey Results

18 Dugan, Maeve 2014, Online Harrassement

19 PKS 2016/2017 Grundtabelle 05 Tatschlüssel 627000,

20 Stahel, Lea 2016, Ich, der Troll: Wieso Online-Hasser gerne ihren vollen Namen nennen

21 PKS 2017, Grundtabelle 05, Tatschlüssel 131400

22 Weller, Konrad 2013, Partner 4 Studie

23 Kunz & Singelnstein 2015, §17 RN 33

24 Rüdiger, Thomas-Gabriel 2018 - 23 Millionen Deutsche Opfer von Cybercrime https://www.linkedin.com/pulse/23-millionen-deutsche-opfer-von-cybercrime-thomas-gabriel-r%C3%BCdiger/ Zugriff 16. Mai 2018, Zugriff 16. Mai 2018

25 Vgl. Rüdiger, Thomas-Gabriel 2018 „Das Broken Web“, S.259 in Rüdiger, Thomas-Gabriel/ Bayerl, Petra Saskia (eds.) 2018, Digitale Polizeiarbeit

26 http://www.spiegel.de/netzwelt/netzpolitik/cyberkriminalitaet-polizei-fordert-mehr-werkzeuge-a-1182501.html, Zugriff 16. Mai 2018 . Es kann davon ausgegangen werden, dass von diesen Beamten ein signifikanter Anteil mit der Abarbeitung von angezeigten Delikten beschäftigt ist, vermutlich wird nur ein geringer Bruchteil wird im Rahmen einer anlassunabhängigen Internetrecherche zur Aufhellung des Dunkelfeldes eingesetzt.

27 Teilweise werden andere Zahlen angegeben, dieser Beitrag bezieht sich jedoch auf offiziellen Zahlen des statistischen Bundesamtes. https://www.destatis.de/DE/ZahlenFakten/ImFokus/OeffentlicheFinanzenSteuern/PersonalPolizei.html

28 Spigrath, Tobias 2013, „Zur Abschreckungswirkung des Strafrechts“, S. 125

29 LKA BW 2013 Jahresbericht Cybercrime/Digitale Spuren, S. 8

30 Popitz, Heinrich 1968 „Die Präventivwirkung des Nichtwissens“

31 Proll, Uwe 2016, „Polizei muss zur Sicherheit ins Netz“, Behörden Spiegel Heft 11/2016

32 Ebd.

33 Interessanterweise erlauben beispielhaft die Verträge zur Nutzung Öffentlicher Verkehrsmittel durch Polizisten nur uniformierten Beamten kostenfrei zu fahren, obwohl objektiv auch zivil gekleidete Polizisten die Sicherheit erhöhen.

34 Bayerl, Petra Saskia/ Rüdiger, Thomas-Gabriel 2017 „Soziale Medien – Anbruch eines neuen Zeitalters polizeilicher Arbeit?“

35 https://www.vrt.be/vrtnws/nl/2018/02/14/digitale-wijkagent/ ,Zugriff 16. Mai 2018

36 http://www.bundeswehr.de/portal/poc/bwde?uri=ci:bw.bwde.streitkraefte.grundlagen.staerke ,Zugriff 16. Mai 2018

37 https://www.facebook.com/PolizeidirektorLind/ , Zugriff am 16. Mai 2018

38 https://twitter.com/Polizei_LER_JL , Zugriff am 16. Mai 2018;

39 https://www.vrt.be/vrtnws/nl/2018/02/14/digitale-wijkagent/ , Zugriff 16. Mai 2018

40 https://www.mz-web.de/sachsen-anhalt/hasskommentare-im-netz-polizei-geht-virtuell-auf-streife-im-internet-25206740 , Zugriff 16. Mai 2018

41 https://www.heise.de/newsticker/meldung/Gegen-Hasskriminalitaet-Sachsen-Anhalt-schickt-Polizisten-auf-Streife-im-Netz-3921503.html , Zugriff 16. Mai 2018

42 Landtag des Saarlandes, 2016 Drucksache 15/1855 „Polizei ins Internet bringen – Online-Streife einführen“

43 Landtag Brandenburg, 2018 Drucksache 6/8784 „Maßnahmenpaket zur wirksamen Abwehr von Internet- und Cyberkriminalität“

44 Bayerl, Petra Saskia/ Karlovic, Ruza/ Babak, Akhgar/ Makarian, Garik (eds.) 2018 „Community Policing – A European Perspective“

45 Akhgar, Babak/Bayerl, Petra Saskia/Sampson, Fraser (eds.) 2016, “Open Source Intelligence Investigation”

46 https://www.youtube.com/watch?v=cMtMk21FZUM; Zugriff 16 Mai 2018

47 https://www.mi5.gov.uk/careers/opportunities/intelligence-collection; Zugriff 16 Mai 2018

48 https://www.androidheadlines.com/2018/04/scranton-pa-police-department-to-embrace-vr-training.html; Zugriff 16 Mai 2018

49 Denef, Sebastian/Rüdiger, Thomas-Gabriel 2013, Deutsche Polizei 11/2013 „Soziale Medien – Muss sich die Polizei neu ausrichten?“

50 Triest, Daniel 2018 „Die Polizei als Filter der Anzeigen digitaler Straftaten“ , S. 133 in Rüdiger, Thomas-Gabriel/ Bayerl, Petra Saskia (eds.) 2018, Digitale Polizeiarbeit

51 https://kurier.at/chronik/oesterreich/polizisten-gehen-online-30-000-smartphones-bestellt/283.255.722 Zugriff 16 Mai 2018

52 https://www.mi.niedersachsen.de/aktuelles/presse_informationen/pilotprojekt-nimes-fuer-mobile-kommunikation-bei-der-niedersaechsischen-polizei-gestartet-164141.html Zugriff 16 Mai 2018

53 https://kurier.at/chronik/oesterreich/polizisten-gehen-online-30-000-smartphones-bestellt/283.255.722 Zugriff 16 Mai 2018

54 https://utopiensammlerin.com/2018/05/13/sex-eigentum-die-digitalisierung-der-kriminalitaet-und-die-zukunft-der-polizeiarbeit/ ,Zugriff 16 Mai 2018

55 Man denke hier beispielsweise auch an die Öffentlichkeitsfahndung über Soziale Medien, bei denen Bilder von Tatverdächtigen nicht gezeigt werden, da diese erst auf behördeneigenen Servern angezeigt werden dürfen. Hintergrund sei, dass nur so die Kontrolle über das Bild gewahrt bleiben könne. Vgl. Rüdiger, Thomas-Gabriel 2018 „Das Broken Web“, S.289 in Rüdiger, Thomas-Gabriel/ Bayerl, Petra Saskia (eds.) 2018, Digitale Polizeiarbeit

56 Rüdiger, Thomas-Gabriel 2018 „Das Broken Web“, S. 287 in Rüdiger, Thomas-Gabriel/ Bayerl, Petra Saskia (eds.) 2018, Digitale Polizeiarbeit

57 Die Justizministerinnen und Justizminister (JUMIKO) haben auf ihrer 87. Konferenz am 17. November 2016 in Berlin unter Top II.1 „Digitale Agenda für das Straf- und Strafprozessrecht“ die Einrichtung einer Arbeitsgruppe zu dieser Thematik beschlossen. Die Ergebnisse stehen noch aus.

58 Krischock, Heike 2018 „Das Internet in der polizeilichen Gefahrenabwehr“, S. 255 in Rüdiger, Thomas-Gabriel/ Bayerl, Petra Saskia (eds.) 2018, Digitale Polizeiarbeit

59 Eine Diskussion über ein weltweites Normenverständnis und Normenkontrolle geht hier zu weit, ist aber vermutlich eine Entwicklungstendenz für die Zukunft.

60 Der Wissenschaftliche Dienst des Bundestages hat sich in einer Ausarbeitung vom 21. Februar 2018 dieser Frage angenommen und kommt zu dem Schluss, dass das Blockieren eines Nutzers in den Sozialen Medien durch einen Polizei-Account beispielhaft dann gerechtfertigt sein kann, wenn es zur Unterbindung weiterer Straftaten passiert. Az: —WD 3 -3000 -044/18, S. 4

Neuste Buchveröffentlichung „Digitale Polizeiarbeit", Springer 2018 https://www.springer.com/de/book/9783658197551

"[...] Thomas-Gabriel Rüdiger gilt als einer der führenden Cyber-Kriminologen in Deutschland [...]", S.13 Weißer Ring, Ausgabe 01/2018

"[...] Kriminologe Thomas-Gabriel Rüdiger [...] ist ein bundesweit renommierter Spezialist für Cybercrime, Polizeiarbeit im digitalen Raum und Interaktionsrisiken in den sozialen Medien [...]"
Simone Schmollack in "Und er wird es wieder tun", S. 86 ff, 05/2017

"[...] Deutschlands bekanntester Cyberpolizist, der Brandenburger Kriminologe Thomas-Gabriel Rüdiger, vermisst kompetente Aufklärung an Schulen [...]", FAZ Printausgabe vom 07.06.2016

"[...] Thomas-Gabriel Rüdiger ist einer der wenigen, die sich trauen, beim fehlenden Medienschutz Klartext zu reden.[...]".
Christian Füller in "Die Revolution missbraucht ihre Kinder", S.205ff, 03/2015

"[...] Der wohl best informierteste Cybercop Deutschlands[...]" Frankfurter Allgemeine Sonntagszeitung (FAZ / FAS),
Printausgabe vom 03.03.2014