Tatort: Internet

Die Polizei von heute auf die Kriminalität von morgen vorbereiten

Die Gesellschaft hat in den vergangenen Jahren einschneidende Veränderungen erlebt – viele haben direkt oder indirekt mit dem technologischen Fortschritt zu tun: Nach dem Siegeszug der Heimcomputer in den 1980er-Jahren, dem Start des World Wide Webs in den 1990er-Jahren, dem Aufkommen leistungsfähigerer portabler digitaler Endgeräte wie Smartphones in den 2000er-Jahren bis hin zur weitreichenden Etablierung der sozialen Netzwerke als virtuelle Informations- und Kommunikationsplattformen in den 2010er-Jahren. Nicht zuletzt wirkte auch die Corona-Pandemie als Digitalisierungs-Booster, mit allen Vor- und Nachteilen.

Jede technologische Errungenschaft bietet den Menschen neue Möglichkeiten, birgt aber auch Gefahren durch Einfallstore und Betätigungsfelder für Kriminelle. Hierbei stellt besonders das Internet – mit seiner überstaatlichen Beschaffenheit, der von außen undurchsichtigen technischen Struktur und den schier unzähligen Diensten und Angeboten – eine Herausforderung für die polizeiliche Arbeit dar. Straftaten werden aus dem Schutz einer Anonymität verschleiert. Es ergeben sich auch ganz neue Kriminalitätsfelder wie Phishing, Datenspionage oder durch Ransomware. Schließlich nutzen Kriminelle das Internet auch als virtuelles Hinterzimmer, um Straftaten anzubahnen oder zu planen, sowie als digitalen Marktplatz zur Hehlerei oder zum Tausch von inkriminierten Dateien wie Missbrauchsabbildungen von Kindern.

In Puncto Digitalisierung der Polizei wurde schon viel erreicht: Polizistinnen und Polizisten wurden mit Smartphones ausgerüstet, viele Dienststellen setzen auf ausgewiesene IT-Fachleute zur Unterstützung der polizeilichen Arbeit, es wurden neue Softwaresysteme entwickelt und angeschafft und die Aus- und Fortbildung in vielen Bereichen reformiert. In der Folge der aber schon heute existierenden, realen Gefahren der digitalen Medienwelt ist mehr erforderlich: ein gänzlich neues Bewusstsein für den Umgang der Sicherheitsbehörden mit dem Tatort Internet. Es braucht umfangreiche rechtliche Anpassungen, eine IT-Knowhow-Offensive sowie neue Ermittlungsansätze und -konzepte. Täter, Motive, Tatbegehungen und Beuten sind online zum Teil schlicht anders als in der Offline-Welt – darauf müssen die Sicherheitsbehörden reagieren.

Die Unionsgeführten Ressorts sind in dieser Hinsicht bereits auf einem guten Weg. Es bedarf aber einer gemeinsamen Anstrengung aller Länder und des Bundes, um den Bedrohungen im virtuellen Raum zu begegnen. Auch im Internet muss eine wirksame Gefahrenabwehr und effektive Ermittlungsarbeit möglich sein. Daher sind sich die Innenministerinnen und Innenminister von CDU und CSU sicher: Der Tatort Internet macht stetige Anpassungen der Arbeit und insbesondere der technischen Ausrichtungen und Befugnisse der Sicherheitsbehörden in Deutschland notwendig. Daraus erwachsen in den folgenden Handlungsfeldern diverse Umsetzungsaufträge, die auf der nächsten Innenministerkonferenz zur Diskussion gestellt werden:

Es gilt das Recht des Staates, nicht das (Un-)Recht des Internets.

Nach der Anfangszeit des Internets, die weitestgehend ohne Regulierungen auskam und von einer gewissen „Wild West"-Manier geprägt war, hat sich mittlerweile das Bewusstsein durchgesetzt, dass das Internet kein rechtsfreier Raum ist. Aber noch an zu vielen Stellen scheint es, als würde das Internet einen eigenständigen Rechtsraum darstellen, für den andere Gesetze gelten als für die Offline-Sphäre. Das zeigt sich beispielsweise daran, dass in vielen öffentlich gut zugänglichen Bereichen des Internets – beispielsweise in Messengern oder in den sozialen Netzwerken – noch immer faktisch anonym agiert werden kann – eine Anonymität, aus der heraus Straftaten verübt werden können. Deshalb fordern wir:

- **Ende der digitalen Maskerade!** Es braucht eine Änderung des Netzwerkdurchsetzungsgesetzes, um eine Vermummung durch Pseudonyme oder Phantasieaccounts im Falle des Straftatverdachts, aber auch bei extremistischen und verfassungsfeindlichen Äußerungen unterhalb dieser Schwelle, zu unterbinden. Daher muss das Recht dahingehend geändert werden, dass Nutzer von Telemedien und sozialen Netzwerken sich identifizieren und diese Daten auf begründete Nachfrage der Sicherheitsbehörden auch zur Verfügung gestellt werden müssen. Das gilt sowohl für kleinere Anbieter, wie beispielsweise Spieleplattformen und Messengerdienste unter zwei Millionen Nutzern, als auch für die großen Kryptowährungsbörsen und Handelsplätze.

Die Sicherheitsbehörden brauchen einen digitalen Instrumentenkoffer.

Für die Ermittlungsarbeit in der analogen Welt sind die Sicherheitsbehörden gut ausgestattet – von den Einsatzmitteln am Gürtel eines Polizisten bis hin zu speziell geschulten Spurensicherungsteams, Sachverständigen und Analyselabors. Viele Spuren, die bei einer Tatbegehung im Internet anfallen können, werden bislang nicht ausreichend erfassbar gemacht und verarbeitet. Die Sicherheitsbehörden brauchen demnach einen ständig angepassten Instrumentenkoffer für den Tatort Internet, der unter anderem das Folgende leisten muss:

- **Digitale Reifenspuren sichtbar machen!** Gemeint ist eine Neuregelung der Verkehrsdatenspeicherung, um beispielsweise auch die Inhaber von dynamischen IP-Adressen im Nachhinein identifizieren zu können. Gerade Extremistinnen und Extremisten sowie Anbieter von Missbrauchsabbildungen nutzen häufig Anonymisierungsdienste, um ihre „digitalen Reifenspuren“ zu verwischen. Gelingt dies, ist das insbesondere für die Fälle von noch aktivem Kindesmissbrauch mit unvorstellbarem Leid auf Seiten der jungen Opfer verbunden – ein Leid, das mit entsprechenden Speicherfristen zu verhindern wäre. Die Innenministerinnen und Innenminister fordern daher die Bundesregierung dazu auf, eine rechtssichere Neuregelung der Verkehrsdatenspeicherung zu verabschieden. Darüber hinaus fordern sie die Europäische Kommission dazu auf, im Einklang mit der Rechtsprechung des EuGH weitergehende Befugnisse zu identifizieren und deren einheitliche Anwendung in der EU sicher zu stellen.

- **Digitales Mithören in unverschlüsselter Form muss möglich sein!** Heutzutage existiert juristisch eine praktisch längst überwundene Trennung zwischen der Nutzung des Telefons und der Nutzung von Messenger-Diensten. Obwohl über Messenger-Dienste auch telefoniert werden kann und über Internettelefondienste auch Kurznachrichten verschickt werden können, sind die Befugnisse der Sicherheitsbehörden für die wichtige Aufgabe der Gefahrenabwehr nicht einheitlich geregelt. Diese Regelungen sind realitätsfern, sodass die rechtliche Trennung zwischen Telekommunikation und Telemedien aufgelöst und die Befugnisse technikneutral formuliert werden müssen. Es ist schlicht unerheblich, ob eine Straftat über das Mobilfunknetz oder per Internetmessenger vorbereitet wird. Darüber hinaus muss unser Augenmerk

insbesondere auch auf der Fortentwicklung der technischen Möglichkeiten zur gesetzeskonformen Durchführung liegen. Der restriktive Ansatz der Ampelkoalition hinsichtlich technischer Befugnisse der Sicherheitsbehörden ist nicht geeignet, die Sicherheitsbehörden mit zeitgemäßen Ermittlungsmethoden auszustatten.

- **Kein Sicherheitsrückschritt durch Technikfortschritt!** Der neue Mobilfunkstandard 5G, mit dem nur noch verschlüsselt kommuniziert wird, macht eine klassische Telekommunikationsüberwachung (TKÜ) unmöglich. Damit wird durch technologisch wünschenswerten Fortschritt ein Rückschritt bei den Ermittlungsmöglichkeiten der Sicherheitsbehörden bewirkt – diese Lücke gilt es zu schließen. Hierbei bauen die Innenministerinnen und die Innenminister auf die Arbeit der der zu diesem Zwecke im Herbst 2020 eingerichteten Europäischen Gruppe der Leiter der für die rechtmäßige Überwachung zuständigen Stellen.

- **Künstliche Intelligenz gegen Internetdelinquenz!** Das Internet ist ein schier unendlich großer Raum mit einer unüberblickbaren Anzahl an Informationen. Schätzungen zufolge besteht das Internet aus etwa 550 Millionen Terabytes. Wären all diese Daten Musikdateien würde das einmalige Anhören dieser Menge etwa 1,7 Milliarden Jahre dauern. Es liegt auf der Hand, dass das händische Suchen und Ermitteln in diesem Datenraum nur einen sehr begrenzten Einblick vermitteln kann. Das bestätigt sich allein mit dem Blick auf die schier unfassbare Anzahl an Missbrauchsabbildungen, die im Internet kursieren und deren Bearbeitung viel Personal bindet. Es wird daher unerlässlich sein, Systeme der künstlichen Ermittlungsintelligenz einzusetzen, um Spuren zu bewerten und abzugleichen. Kritisch zu würdigen ist daher der Vorschlag der Europäischen Kommission für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KOM[2020]206) vom 21.04.2021, soweit dieser grundsätzliche Beschränkungen des Einsatzes von KI durch die Sicherheitsbehörden vorsieht und hierbei nicht die besondere Aufgabenstellung der Sicherheitsbehörden angemessen berücksichtigt.

Digitale Streife, digitale Wache: Die Präsenz der Sicherheitsbehörden im Internet erhöhen.

Die Schutzfrau und der Schutzmann auf der Straße, die Polizeiwache an der Ecke oder der Streifenwagen in der Nachbarschaft sind seit langem in unserem Land Zeichen des Schutzversprechens des Staates gegenüber seinen Bürgerinnen und Bürgern. Sie schaffen Vertrauen, erhöhen das Sicherheitsempfinden und sorgen mit der wahrnehmbaren Präsenz auch objektiv für weniger Kriminalität auf den Straßen und Plätzen des analogen Teils der Welt. Umso wichtiger ist, dass die Präsenz der Sicherheitsbehörden im Internet sich diesem Niveau annähert! Dazu sind Internetseiten der Sicherheitsbehörden und Accounts in sozialen Netzwerken, die vor allem im Sinne der Öffentlichkeitsarbeit genutzt werden, nicht ausreichend:

- **Die digitale Wache ist nur einen Klick entfernt!** Nicht nur auf den Internetseiten der Polizei, sondern auch in den sozialen Netzwerken müssen Polizeirepräsentanzen etabliert werden, die weitestgehend das Funktionsspektrum der klassischen Polizeiwache abdecken. Hierbei sind unter anderem virtuelle Polizeibeamte einzusetzen, die – analog zu modernen Konversationsagenten aus dem privatwirtschaftlichen Kundenservice – automatisiert durch die Angebote führen. Insbesondere eine Soforthilfe-Funktionalität soll helfen, Anbahnungen an Kinder und Jugendliche – wie Cybergrooming in sozialen Netzwerken oder sonstigen Portalen – zu begegnen, indem Opfer per Knopfdruck Hilfe bekommen und Täter abgeschreckt werden können.

- **Digitale Streife auf Online Plattformen!** Neben der digitalen Wache gilt es ebenfalls, das Internet digital zu bestreifen. Speziell im Bereich der sozialen Netzwerke besteht deutliches Handlungspotenzial. Werden beispielsweise illegale Güter bzw. Dienstleistungen gehandelt oder werden in einem Konversationsverlauf Beleidigungen oder Bedrohungen ausgesprochen, kann eine digitale Streife direkt eingreifen, Anzeige erstatten, Hilfe anbieten oder schlichten. Auch diese Maßnahme würde – analog zur klassischen Streife – manche Straftat verhindern und in jedem Fall die Wahrnehmung der Polizei im digitalen Raum erhöhen.

- **Der Cyber-Cop: Ein neuer Typus Polizist.** Die oben geschilderten Herausforderungen, die dem Umgang mit dem Internet grundsätzlich innewohnen, aber auch die völlig

neuen Möglichkeiten zur Tatbegehung sowie teils völlig veränderte Tatabsichten machen deutlich, dass die Polizei in Deutschland einen neuen Typus Polizist aus- und fortbilden muss: Den Cyber-Cop. Wir müssen Polizeibeamtinnen und Polizeibeamten qualifizieren, damit sie sich in den Tiefen des Internets bewegen, mit den Systemen und Subsystemen umgehen und delinquentes Verhalten auf den gut ausgeleuchteten Plätzen des Internets, aber auch in den schattigen Nischen des Deep- und Darknets erkennen können.