VEREINIGUNG ÖSTERREICHISCHER
STAATSANWÄLTINNEN
UND STAATSANWÄLTE

p.A.Staatsanwaltschaft Graz
Conrad-von-Hötzendorf Straße 41,
8010 Graz
www.staatsanwaelte.at
stavereinigung@justiz.gv.at

Empfehlungen zur effizienten Verfolgung von „Cybercrime"-Delikten

Die bei den Staatsanwaltschaften eingerichteten Kompetenzstellen „Cybercrime" haben sich in der Praxis sehr bewährt. Die hohe Anzahl der Rückmeldungen sowohl aus dem Bereich der Staatsanwält:innen aber auch der Bezirksanwält:innen zeigen die breite Akzeptanz der Kompetenzstellen, aber auch eine hohe Motivation aller Kolleg:innen, die Arbeit der Kompetenzstellen zu unterstützen.

Dennoch stoßen Staatsanwält:innen in der Fallbearbeitung sehr oft auf rechtliche oder strukturelle Hindernisse, die eine rasche Ausforschung der Täter:innen verzögern bzw. im schlechtesten Fall überhaupt verhindern. Legistische Lösungen sind daher dringen geboten, um diesen stark steigenden Kriminalitätsbereich effektiv und effizient bekämpfen zu können.

Insbesondere haben sich aus den staatsanwaltschaftlichen Erfahrungen folgende Problemstellungen herauskristallisiert:

I. Sicherstellung von Daten

Da eine Sicherstellung immer gegenstandsbezogen ist, wird ihre derzeitige gesetzliche Ausgestaltung den Anforderungen der digitalen Welt nicht mehr ausreichend gerecht.

Dabei greift die derzeitige Diskussion über die Neugestaltung der Sicherstellung von Datenträgern zu kurz. Daten werden immer öfter und im großen Umfang nicht auf Geräten, sondern in Clouds oder sonstigen ausgelagerten externen Speichermöglichkeiten verwahrt, sodass der Zugriff auch nicht mehr über ein bestimmtes Endgerät erforderlich ist bzw. die

Sicherstellung eines bestimmten Gerätes nicht garantiert, dass keine Abänderung oder Löschung von relevanten Daten erfolgt.

a. Sicherstellung und Einziehung von Websites und Accounts

So fehlt es in diesem Zusammenhang an klaren Regeln für die Sicherstellung von Websites, insbesondere für die Anbringung entsprechender Warnhinweise beim Aufruf sichergestellter Domains nach einem behördlichen „Takedown". Ebenso wäre die Möglichkeit einer Sperre von Zugangsberechtigungen (zB zu social media accounts oder einer Mailbox) sinnvoll, um Veränderungen oder fortgesetzte strafbare Handlungen zu unterbinden.

Auch für die Löschung von Daten oder Internetseiten mit illegalen Inhalten braucht es eine umfassende Rechtsgrundlage. Eine allfällige Einziehung kommt nicht in Betracht, weil das Gesetz ausdrücklich auf Gegenstände abzielt und im StGB ein generelles Analogieverbot besteht. § 33 Abs 2 MedienG wiederum ist nur für Medieninhaltsdelikte anwendbar, worunter die meisten Cybercrime-Delikte wohl nicht fallen. Darüber hinaus ist das hierfür vorgesehene Verfahren (Urteil nach Antragstellung bei Gericht, anschließend Löschung durch Medieninhaber bzw. Hostingdiensteanbieter gem. §§ 36a, b MedienG) wegen der meist bestehenden Dringlichkeit einer Löschung und der Abhängigkeit von der Mitwirkung der Medieninhaber, die oft selbst Beschuldigte sind, bzw. der Provider nicht praxistauglich. Selbst kinderpornografisches Material kann lediglich dann (mit)vernichtet werden, wenn das Speichermedium sichergestellt wurde bzw. der Eigentümer desselben zustimmt oder die Löschung selbst bzw. unter Beiziehung eines Sachverständigen vornimmt. Es kann jedoch nicht gewährleistet werden, dass die Daten bzw. Kopien derselben nicht noch auf einem Server oder in der Cloud vorhanden sind. Eine Fernlöschung wäre mitunter zwar technisch, aber nicht rechtlich möglich, wenn kein unmittelbarer körperlicher Zugriff auf den Datenträger besteht. Es braucht somit eine rechtliche Grundlage für eine Löschung durch die Kriminalpolizei (ggf. nach Anordnung der Staatsanwaltschaft).

b. Sicherstellung von Kryptowährungen

Nach aktuellen Entscheidungen des OGH (14 Os 137/22m, 14 Os 138/22h) kommt iZm Bankguthaben ausschließlich eine Sicherung nach § 109 Z 1 lit b StPO (Drittverbot) in Betracht,

nicht hingegen eine Überweisung des Geldbetrages auf ein gerichtliches Konto, weil das Gesetz nicht vorsieht, dass sich andere Vermögenswerte als körperliche Gegenstände in behördlicher Verwahrung befinden (RIS-Justiz RS0133580). Das OLG Innsbruck hat zu 11 Bs 62/23i diese Rechtsansicht auch auf Kryptowährungen übertragen, womit fraglich ist, ob ein Transfer von Kryptowährungen auf ein Behördenwallet iSd Leitfadens „Vermögensrechtliche Anordnungen“ (S 108) und der sich hierauf stützenden Ermittlungspraxis rechtlich überhaupt zulässig ist. Danach soll die Sicherstellung von Kryptowährungen durch den Transfer auf ein „Behördenwallet“ erfolgen, nachdem das körperliche Speichermedium des Wallets, in dem die Schlüssel für Transaktionen verwaltet werden (zB der Computer, das Smartphone, der USB-Stick oder das Blatt Papier, auf dem der Key abgedruckt ist), sichergestellt wurde. Dies soll verhindern, dass jemand, der im Besitz einer Kopie des „Schlüssels“ ist, trotz Sicherstellung auf die Vermögenswerte zugreifen kann und ist daher auch erforderlich, um die sichergestellten Kryptowährungen vollständig vor einem Zugriff durch Dritte zu schützen. Ebenso soll derart vorgegangen werden, wenn der Adressat eines Drittverbotes nicht „valide“ ist.

Darüber hinaus herrscht Unklarheit, wenn verschiedene potentiell sicherzustellende, jedoch das von der Sicherstellung gedeckte Volumen übersteigende Kryptowährungen vorhanden sind. Hier stellt sich für die Ermittler:innen regelmäßig die Frage, welche Kryptowährung in welchem Umfang sichergestellt werden soll.

Auch bei der Verwertung stellt die hohe Volatilität von Kryptowährungen regelmäßig eine Herausforderung dar und bedarf klarer Regeln. Der Erlass des BMJ vom 1.4.2020, GZ 2020-0.163.092, sieht vor, sichergestellte Kryptowährungen gem. § 115e StPO vorzeitig zu verwerten. Zwar existiert hierzu – soweit ersichtlich – noch keine gegenteilige Rechtsprechung, jedoch ist fraglich, ob die pauschale Annahme, dass Kryptowährungen per se einer „erheblichen Wertminderung“ unterliegen, weil regelmäßig Kursverluste zu befürchten seien, tatsächlich gerechtfertigt ist. Vielmehr sind aufgrund der volatilen Kursentwicklungen in diesem Bereich nicht nur Verluste, sondern auch bedeutende Gewinne möglich.

II. Rückzahlungen von betrügerisch herausgelockten Zahlungen an die Opfer

Die Ausfolgung von Gegenständen an Opfer ist auf völlig unstrittige Sachverhaltskonstellationen beschränkt und setzt voraus, dass sich die Gegenstände auch tatsächlich in behördlicher Verfügungsmacht („Verwahrung"; §§ 109 Z 1 lit a, 114 StPO) befinden. Dies ist bei Bankguthaben nie der Fall, weshalb es für die Strafverfolgungsbehörden beispielsweise nicht möglich ist, Rückzahlungen von betrügerisch herausgelockten Zahlungen an die Opfer auch dann anzuordnen, wenn die Täter nicht ausgeforscht werden können.

Die Strafprozessordnung enthält keine Bestimmungen, die eine Übertragung von Vermögenswerten (zB sichergestellte Bankguthaben oder Kryptowährungen) an die Geschädigten (ausnahmsweise) im Ermittlungsverfahren bzw. vor einer die Anklage erledigenden Gerichtsentscheidung ermöglichen. In der Praxis sind daher derzeit Fälle, in denen Vermögenswerte sichergestellt wurden, der Kontoinhaber jedoch nicht ausgeforscht werden kann (weil das Konto etwa mit falschen Daten eröffnet wurde), nicht auflösbar.

Bisher wurden - der Entscheidung des Oberlandesgericht Wien zu 17 Bs 149/17m folgend, wonach eine analoge Anwendung des § 367 StPO möglich sei - Auszahlungen an das Opfer angeordnet. Dem steht nunmehr die aktuelle Entscheidung des Obersten Gerichtshofes (14 Os 137/22m, 14 Os 138/22h) klar entgegen.

III. NAT-Adressen

Die Verwendung von NAT-Adressen zur Tatbegehung ist immer stärker wahrnehmbar, um die Ausforschung der Täter:innen zu erschweren. Obwohl den Diensteanbietern zumindest zu Verrechnungszwecken eine Zuordnung von einzelnen Teilnehmer:innen möglich sein müsste, besteht keine Speicherpflicht und nach § 76a Abs 2 Z 1 StPO auch keine Auskunftspflicht, wenn die Zuordnung eine größere Zahl von Teilnehmer:innen, also ab ca. 10, erfassen würde. Es bedarf daher einer dringenden Lösung, zB durch Beseitigung oder Anhebung dieser Beschränkung sowie unter Einschluss der kommunikationsrechtlichen Bestimmungen.

IV. Überwachung von verschlüsselter Kommunikation (Quellen-TKÜ), Online-Durchsuchung und weitere Ermittlungsmöglichkeiten im Internet

Eine weitere Notwendigkeit zur effizienten Kriminalitätsbekämpfung wäre die Anpassung der bestehenden Überwachungsmöglichkeiten an den digitalen Raum. Da professionelle Täter:innengruppen in aller Regel verschlüsselte Kommunikationsprogramme wie WhatsApp, Signal, Telegram oder andere Messengerdienste verwenden, geht die herkömmliche Überwachung von Nachrichten zumeist ins Leere. Die Schaffung einer grundrechtskonformen, an der Rechtsprechung des VfGH orientieren Rechtsgrundlage für die Überwachung verschlüsselter Nachrichten wäre daher dringend erforderlich, um gerade Verbrechen im Bereich der organisierten Kriminalität und der Terrorismusbekämpfung weiterhin erfolgreich aufklären zu können. So wie im analogen Leben Wohnungen durchsucht und Beschuldigte observiert werden dürfen, sollte im digitalen Raum – zumindest bei schweren Straftaten und unter strengen Auflagen – ein behördlicher Fernzugriff auf den Computer eines Tatverdächtigen zur gezielten Durchsuchung nach inkriminierten Daten möglich sein („Legal Hacking"; „Tracing"). Dies wäre technisch leicht umsetzbar und ist auch schon in anderen EU-Mitgliedstaaten (bspw. in Deutschland, Frankreich, Belgien und den Niederlanden) geltendes Recht. Betrachtet man die bestehenden – großteils ebenfalls verdeckten – Ermittlungsmöglichkeiten im analogen Bereich (Telefonüberwachung, verdeckte Ermittlung, Lauschangriff, Observation, Hausdurchsuchung, Sicherstellung und Auswertung von Mobiltelefonen und Datenträgern), wäre ein derartiger Grundrechtseingriff in der Gesamtschau keineswegs überdurchschnittlich grundrechtsinvasiv.

V. Anpassung der bestehenden Zuständigkeitsregeln an neue Tatphänomene

Die strafprozessualen Regeln über die Zuständigkeit und den Zusammenhang von Verfahren (§§ 26, 27 StPO) führen gerade im Bereich der Massendelikte wie bspw. dem aktuellen Tochter/Sohn-, FinLink- oder Vinted-Betrug regelmäßig zu einem wiederholten Wechsel der staatsanwaltschaftlichen Zuständigkeit, zumal auch das Zuvorkommen in einem Verfahren gegen unbekannte Täter zuständigkeitsbegründend ist und Konnexitäten teils erst relativ spät festgestellt werden. Dabei gehen nicht nur Ressourcen verloren, sondern es besteht die große

Gefahr, dass durch den Zeit- und Wissensverlust auch der Ermittlungserfolg beeinträchtigt wird. Außerdem kann die Pflicht zur gemeinsamen Führung des Ermittlungsverfahrens insofern ausufern, als sich in Zeiten von „crime as a service“ zB über den (zufällig) selben Geldwäsche-Dienstleister Konnexitäten zwischen völlig unterschiedlichen Tätergruppen bzw. modi operandi ergeben und damit zu kaum zu bewältigenden Großverfahren führen, die kleinere Dienststellen völlig lahmlegen können. Abgesehen von den beschränkten personellen Kapazitäten für derartige Verfahren stößt auch die EDV (VJ, DJAP) an ihre Grenzen, wenn teilweise hunderte Verfahren einzubeziehen sind.

Es wäre daher eine gewisse Einschränkung der strengen Konnexitätsregeln und eine etwas größere Flexibilität bei der Trennung von Verfahren anzudenken, wobei in diesem Zusammenhang natürlich auch die Regeln für die gerichtliche Zuständigkeit (insb. § 37 StPO) mitzudenken sind.

In personeller Hinsicht sollte geprüft werden, ob Verfahrensmanager, wie sie bereits bei Gericht bereits erprobt werden, auch die Staatsanwaltschaften bei der Führung von umfangreichen „Sammelverfahren“ unterstützen könnten.

VI. Monitoring von neuen Massenphänomenen

Das frühzeitige Erkennen von Konnexitäten und Phänomenen stellt gerade bei der Bearbeitung von Strafsachen mit Cybercrime-Bezug eine wichtige Komponente dar, um Täter:innengruppen ausforschen zu können. Insbesondere die Errichtung bzw. Verstärkung eines bundes- bzw. europaweiten frühzeitigen Monitoring wäre daher wichtig, um eine konzentrierte Anzeigenerstattung durch die Kriminalpolizei und so eine rasche und effiziente Verfahrensführung zu ermöglichen.

Ein erster wichtiger Schritt wäre es, das PAD (Protokollierungssystem der Polizei) zu adaptieren. Derzeit haben die einzelnen Sicherheitsbehörden außerhalb ihrer Zuständigkeit keinen Zugriff auf diese Datenbank, wodurch für die Ermittlungen wichtige Zusammenhänge uU nicht erkannt werden. Dbzgl. wäre auf eine in der Zuständigkeit des BMI liegende Anpassung hinzuwirken.

VII. Virtuelle IBANs und europäisches Kontenregister

Von zahlreichen Banken werden mittlerweile sog. „virtuelle IBANs“ (kurz: vIBAN) angeboten, die zwar mit einem normalen Konto (mit einer regulären IBAN), auf dem die tatsächlichen Transaktionen abgewickelt werden, verbunden sind, jedoch lediglich – sozusagen eine Ebene darunter – das Guthaben auf diesem Konto unterteilen. Im Zahlungsverkehrs mit anderen SEPA Banken sind vIBANs herkömmlichen IBANs technisch gleichgestellt, d.h. über sie können Zahlungen gesendet und empfangen werden. Aufgrund der schnellen und vollautomatisierten Verarbeitung von vIBAN-Systemen sowie der Möglichkeit, diese weiterzugeben, werden vIBANs immer häufiger auch zur Begehung von Straftaten bzw. Verschleierung der Geldflüsse verwendet. Die Nachverfolgung von Geldtransaktionen stellt häufig den einzigen Ermittlungsansatz dar. Da Banken offenkundig durch Kooperationen mit Bankinstituten in anderen Ländern auch ausländische vIBANs vergeben können, bedeutet die Kennung (zB „AT“) allerdings nicht (mehr) zwangsläufig, dass es sich um ein im jeweiligen nationalen Kontenregister eingetragenes Konto handelt. Gleichzeitig kann oft nicht mehr nachvollzogen werden, wo das hinter einer vIBAN stehende Konto tatsächlich registriert ist und welches Kontenregister zur Erteilung der Auskunft über den:die Kontoinhaber:in angefragt werden muss. Eine Kontenregisterabfrage hat bei vIBANs somit idR ein negatives Ergebnis zur Folge. Deutschland hat diesem Phänomen dadurch entgegengewirkt, dass sämtliche (v)IBANs mit der Länderkennung „DE“ im Kontenregister erfasst sein müssen. Eine generelle Lösung dieses Problems dürfte nur über eine strengere europaweite Regulierung zu erreichen sein. Für eine effektive Strafverfolgung wäre die Schaffung eines umfassenden europäischen Kontenregisters, das die (auch virtuellen) Konten sämtlicher in einem Mitgliedstaat ansässigen Banken enthält, dringend geboten.

VIII. Weitere aus Sicht der Praxis reformbedürftige Bereiche

In der Strafprozessordnung braucht es gesetzliche Klarstellungen

- zu Ermittlungen im offenen Bereich des Internets (OSINT-Recherchen),
- für eine „Inhaltsdatenüberwachung“ für die Vergangenheit,

- zur Feststellung von Standortdaten von Verdächtigen auch außerhalb von Kommunikationsvorgängen durch Erweiterung der Anlage zur TKG-DSVO
- für den Einsatz von Drohnen
- bei der verdeckten Ermittlung in Bezug auf die Weiterverwendung eines social media-Accounts eines:einer Beschuldigten nach dessen:deren Festnahme, um seine:ihre Mittäter:innen auszuforschen
- sowie für den Einsatz von Deep-Fake-Technologien

Im materiellen Strafrecht wären darüber hinaus Überlegungen zu folgenden Punkten anzustellen:

- Das Objekt des Raubes sollte (zumindest unter bestimmten Voraussetzungen) um Daten erweitert werden. Derzeit besteht bspw. ein Ungleichgewicht, wenn der:die Täter:in einem betäubten Opfer die Geldbörse wegnimmt oder sich unter Verwendung seines Smartphones mittels Telebanking Geld überweist.
- Da § 126a StGB einen messbaren wirtschaftlichen Wert der Daten verlangt, ist fraglich, ob zB Fotos, die das Opfer als Beweismittel in einem Gerichtsverfahren vorlegen wollte, darunterfallen. Ganz generell kann gerade bei Daten der ideelle Wert deutlich größer sein als der materielle, weshalb sich die Frage stellt, ob diese Fälle nicht demselben strafrechtlichen Schutz unterliegen sollten.
- Inländische Gerichtsbarkeit bei betrügerischem Herauslocken von Krypto-Assets:
  Die Generalprokuratur (Gw 163/22m) vertritt die Ansicht, dass im Fall der Übertragung einer virtuellen Währung der effektive Verlust an der Vermögenssubstanz (und damit der tatbestandsmäßige Erfolg des Betrugs nach § 146 StGB) bereits mit der Abbuchung der Krypto-Assets vom – einem Bankkonto vergleichbaren – Krypto-Assets-Konto des Geschädigten entsteht und als Ort des Erfolgseintritts jener Ort anzusehen ist, an dem das Opfer die Übertragung der Krypto-Assets von seinem Krypto-Assets-Konto vorgenommen hat, somit jener, an dem der Dienstleister der virtuellen Währung seinen Sitz hat. Dies ist (von wenigen österreichischen Dienstleistern abgesehen) im Regelfall – wie auch der Handlungsort der Täter – ein Ort im Ausland. Dieser Ansicht hat sich auch das OLG Wien (23 Bs 2/23x) angeschlossen und ein Abstellen darauf, dass

der Erfolg weltweit begangener Straftaten in der Blockchain als dezentrales und somit auch im Bundesgebiet gespeichertes Netzwerk stets auch in Österreich eintreten und inländische Gerichtsbarkeit begründen würde, ausdrücklich ablehnt. Im Ergebnis bedeutet dies, dass zumindest dann, wenn die Krypto-Assets von einem Dienstleister gehalten werden und dem:der Kunden:Kundin der bezughabende kryptografische Schlüssel nicht bekannt ist, Straftaten zum Nachteil österreichischer Staatsbürger:innen, die sich zur Tatzeit in Österreich aufgehalten haben, im Inland teilweise nicht verfolgt werden können. Zu prüfen wäre in diesem Zusammenhang daher, ob der Erfolgsort neu definiert werden könnte (ev. Abstellen auf die Vermögenssphäre bzw. den Standort der wirtschaftlichen Tätigkeit des:der – wenn auch nur mittelbar, jedoch letzten Endes – Geschädigten).

Die Vereinigung Österreichischer Staatsanwältinnen und Staatsanwälte empfiehlt daher dringend, unter Einbindung der Wissenschaft und der Praxis einen Diskussionsprozess über legistische Reformen zur Verbesserung der angeführten Problemlagen in die Wege zu leiten.

Mag. Cornelia Koller
Präsidentin