Neues aus der Gesellschaft –
Rückblick auf die Veranstaltung der Österreichischen Gesellschaft für Strafrecht und Kriminologie vom 16. März 2023

Am 16. März 2023 lud die „Österreichische Gesellschaft für Strafrecht und Kriminologie" (ÖGSK) zum Vortrag von Mag. *Theresa Holzmann*, Mag. *Tamara Hufnagl-Ranzdorf*, Mag. *Philipp Coufal* und Mag. *Andreas Isep* zum Thema „Vorstellung der Cybercrime-Kompetenzstelle bei der Staatsanwaltschaft Wien und aktuelle Phänomene der Cyberkriminalität in der Praxis" ins Dachgeschoß des Juridicums (Wien) ein.

Nach einleitenden Worten des Präsidenten Assoz. Prof. Dr. *Farsam Salimi*, eröffnete Staatsanwältin Mag. *Theresa Holzmann* die Vortragsreihe mit einer Einführung in die Tätigkeit der Cybercrime-Kompetenzstelle, die seit 1. April 2022 bei der Staatsanwaltschaft Wien eingerichtet ist. Ziel der Kompetenzstelle ist der Aufbau und die Intensivierung von Expertise im Bereich Cyberkriminalität sowie die Schaffung von kompetenten Ansprechpartnern sowohl für interne als auch externe Anfragen zum Thema Cybercrime. Hierdurch soll eine raschere und effizientere Durchführung von Ermittlungen in diesem Bereich gewährleistet werden. Überdies ist die Kompetenzstelle für die Organisation und Abhaltung von internen Schulungen, das Bereitstellen von relevanten Unterlagen (zB Leitfäden, Musteranordnungen) über eine Informationsplattform sowie die Beobachtung und Analyse von neuen Cybercrime-Phänomenen zuständig. Die Kompetenzstelle steht zudem in einem regelmäßigen bzw anlassbezogenen Austausch mit weiteren Kontaktstellen innerhalb der Justiz (zB Justiz-IT-ExpertInnen) und Kriminalpolizei (zB BMI, BKA, LKA) sowie externen Stellen (zB Universitäten). Derzeit kommt den ReferentInnen der Cybercrime-Kompetenzstelle allerdings keine Eigenzuständigkeit zu, dh die Verfahren werden entsprechend der allgemeinen Geschäftsverteilung verteilt.

Anschließend skizzierte Staatsanwältin Mag. *Tamara Hufnagl-Ranzdorf* aktuelle Phänomene im Bereich Cybercrime. Neben bekannten cyberkriminellen Erscheinungsformen – wie etwa dem Einsatz von Ransomware oder Phishing-Mails –, sind die Strafverfolgungsbehörden immer wieder mit neuen modi operandi der Täter konfrontiert. Beim sog „Love Scam" handelt es sich etwa um eine moderne Form des Heiratsschwindels, bei der die Täter zunächst eine Vertrauensbasis zu ihren Opfern aufbauen, um diese anschließend unter Vortäuschung einer Notsituation – zB dem Vorwand, ein Familienmitglied benötige eine lebensnotwendige Operation – finanziell auszubeuten. Die Kontaktaufnahme erfolgt dabei zumeist über Social-Media- bzw Dating-Plattformen (zB Instagram, Facebook, Tinder) unter Verwendung gefälschter Identitäten (sog „Fake-Profile"), wobei sich die Täter vorwiegend als im Ausland tätige Soldaten, Ärzte, Piloten etc ausgeben. Ganz aktuell beschäftigten die Staatsanwaltschaften betrügerische SMS-Nachrichten, die im Namen des österreichischen Finanzamtes versendet werden. Darin werden die Empfänger dazu aufgefordert, eine offene Forderung zu begleichen, um ein drohendes Pfändungsverfahren abzuwenden. Klickt man auf den in der SMS-Nachricht enthaltenen Hyperlink, kommt man auf eine gefälschte Website des Finanzamtes, die zur Überweisung

eines bestimmten Geldbetrages auffordert. Im Gegensatz zu anderen cyberkriminellen Erscheinungsformen besteht die Besonderheit laut Mag. *Hufnagl-Ranzdorf* darin, dass von den Tätern zunächst gerade keine ausländischen, sondern österreichische Rufnummern und Bankkonten verwendet wurden.

Im Anschluss daran erläuterte Staatsanwalt Mag. *Philipp Coufal* ausgewählte Ermittlungsansätze zur Aufdeckung von Cyberkriminalität und ging dabei auf die damit verbundenen Problemstellungen in der Praxis ein. Typisch für cyberkriminelle Erscheinungsformen ist nämlich, dass diese einen internationalen Bezug aufweisen. Gerade die internationalen Verflechtungen machen die Ausforschung der Täter besonders zeit- und ressourcenaufwendig. Denn sobald die Täter aus einem anderen Staat operieren, sind die nationalen Strafverfolgungsbehörden auf die Kooperationsbereitschaft von Unternehmen (zB Anbieter von Kommunikationsdiensten) sowie die Rechtshilfe anderer Staaten angewiesen, die erfahrungsgemäß – auch innerhalb der Europäischen Union – sehr stark divergiere. Zudem wenden die Täter ausgefeilte Methoden an, um ihre Identität sowie den Geldfluss zu verschleiern. So werden ua Konten bei in- und ausländischen Banken, Rufnummern oder Email-Adressen mit falschen oder entfremdeten Daten eröffnet. Außerdem greifen die Täter immer häufiger auf sog „money mules" – also Personen, die ihre Daten bzw Konten für „schnelles Geld" zur Verfügung stellen – zurück, wodurch das Ausfindigmachen der Täter(gruppen) nochmals erheblich erschwert wird.

Abschließend weist Mag. *Andreas Isep* in seinem Vortrag darauf hin, dass aktuell keine adäquaten Ermittlungsmöglichkeiten bei Cyberdelikten zur Verfügung stehen. Derzeit greifen die Strafverfolgungsbehörden auf Ermittlungsmaßnahmen zurück, die einen massiven Eingriff in die Grundrechte der Betroffenen (zB Hausdurchsuchung, Telefonüberwachung) darstellen, obwohl gerade im „Cyberspace" allenfalls weniger eingriffsintensive Maßnahmen in Betracht kämen, die technisch möglich, von den derzeitigen Ermittlungsbefugnissen jedoch nicht gedeckt sind. Insbesondere fehle es an einer gesetzlichen Grundlage für das Löschen bzw Sperren von Webseiten mit illegalem Inhalt, das legale „Hacken" von Geräten des Täters oder den Einsatz von Künstlicher Intelligenz zu Ermittlungszwecken. De lege ferenda bedarf es daher einer grundlegenden Anpassung der – zumindest im Hinblick auf Cyberkriminalität – veralteten Ermittlungsbefugnisse der StPO, um eine effektive Kriminalitätsbekämpfung zu ermöglichen. Im Zusammenhang mit Cyberkriminalität sei außerdem problematisch, dass sich der Erfolgsort oftmals im Ausland befindet. Beispielsweise wird bei Kryptowährungen häufig auf den – idR im Ausland gelegenen – Sitz des Exchanger abgestellt. In diesen Fällen ist den Opfern der österreichische Rechtsschutz verwehrt, weil es keine Anknüpfungspunkte für eine inländische Gerichtsbarkeit gibt. Abschließend stellte Mag. *Isep* das „European Judicial Cybercrime Network" vor. Hierbei handelt es sich um ein Netzwerk von Justizbehörden vorwiegend europäischer Staaten, das unter anderem der Vernetzung und dem Austausch von Fachwissen sowie der Verbesserung der Zusammenarbeit zur Bekämpfung von Cyberkriminalität auf EU-Ebene dient.

In der anschließenden Diskussion richtete Assoz. Prof. Dr. *Farsam Salimi* einen Appell an den Gesetzgeber, anstelle einer sukzessiven Anpassung der Bestimmungen der StPO einen umfassenden Reformprozess unter Einbeziehung von Arbeitsgruppen zu starten, um die strafrechtlichen Ermittlungsbefugnisse an die neuen cyberkriminellen Herausforderungen anzupassen und eine effektive Strafverfolgung sicherzustellen. Ergänzend hierzu hielt Hon.-Prof. Dr. *Fritz Zeder* fest, dass derzeit einige internationale Vorhaben im Bereich Cybercrime unterzeichnet wurden bzw sich in der Beschlussphase befinden (zB Zweites Zusatzprotokoll zur Cybercrime-Konvention des Europarates; E-Evidence-Paket der EU). Zwar bestehe auf nationaler Ebene Änderungsbedarf, jedoch müsse primär auf internationaler Ebene mehr getan werden, um einheitliche Eingriffsbefugnisse zur effektiven Bekämpfung von Cyberkriminalität zu schaffen.

Nähere Informationen zu kommenden Veranstaltungen der ÖGSK finden Sie unter *www.oegsk.at*.

Univ.-Ass. Dr. Jan Feldmann