Bundesministerium
Justiz

bmj.gv.at

Dr.in Alma Zadić, LL.M.
Bundesministerin für Justiz

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2020-0.089.478

Ihr Zeichen: BKA - PDion (PDion)743/J-NR/2020

Wien, am 06. April 2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Robert Laimer, Kolleginnen und Kollegen haben am 6. Februar 2020 unter der Nr. **743/J-NR/2020** an mich eine schriftliche parlamentarische Anfrage betreffend „Internetbetrug“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zu den Fragen 1 und 2:

1. *Wie definiert das Bundesministerium für Justiz den sogenannten Internetbetrug?*
2. *Auf Grund welcher Systematik werden die einzelnen Delikte dem Kapitel "Internetbetrug" zugeordnet?*

Nach § 147 Abs. 1 Z 1 des österreichischen Strafgesetzbuches (StGB) ist ein Betrug u.a. dann von Gesetzes wegen ein schwerer Betrug, wenn zur Täuschung der geschädigten Person ausgespähte Daten eines unbaren Zahlungsmittels oder falsche oder verfälschte Daten benützt werden. Daneben gibt es den Spezialtatbestand des betrügerischen Datenverarbeitungsmissbrauchs nach § 148a StGB, den begeht, wer mit dem Vorsatz, sich oder einen Dritten unrechtmäßig zu bereichern, einen anderen dadurch am Vermögen schädigt, dass er das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung

von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs beeinflusst.

Abgesehen davon, dass auch die beiden genannten Bestimmungen nicht notwendigerweise auf das Internet beschränkt sind, ist „Internetbetrug“ insgesamt kein Rechtsbegriff. Phänomenologisch wird „Internetbetrug“ zu „Cybercrime im weiteren Sinne“ gezählt: Darunter versteht man herkömmliche Kriminaldelikte, zum Beispiel eben Betrugsdelikte, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung und/oder Ausführung eingesetzt wird.

Zu den Fragen 3 bis 5:

3. *Auf Grund welcher Ereignisse kann die hohe Summe an Delikten im Jahre 2009 im Bereich des Internetbetrugs erklärt werden?*
4. *In welchen Bereichen des Internetbetrugs wurden im Jahre 2019 besondere Steigerungen verzeichnet?*
5. *Welche Bundesländer sind in welchem Ausmaß davon betroffen (detailliert nach Bundesland und Delikt)?*

Unabhängig davon, wie man Internetbetrug definiert und welche Delikte man darunter subsumieren möchte, ist eine gezielte statistische Auswertung mangels Erfassung der Art der Tatbegehung in den einschlägigen Registern nicht möglich.

Zu den Fragen 6 bis 9:

6. *Welche Maßnahmen wurden von Ihnen im Bereich der Cyberkriminalität insgesamt gesetzt? (detaillierte Darstellung)*
7. *Welche Maßnahmen wurden im Bereich Internetbetrug von ihrem Ministerium gesetzt und welche Maßnahmen planen Sie?*
8. *In welchem Ausmaß wird die Prävention und Information der Bürger und Bürgerinnen verbessert?*
9. *Planen Sie eine zusätzliche Hilfestellung für Bürger und Bürgerinnen, die bei einem Internetbetrug unschuldig zu Verdächtigen werden?*

Im aktuellen Regierungsprogramm wird zum einen die Bekämpfung von Hass im Netz hervorgehoben. Meine Bestrebungen gehen insbesondere dahin, Opfern rasch und kostengünstig Zugang zum Recht zu verhelfen. Grundsätzlich ist die weit überwiegende Anzahl von Postings mit diskriminierenden Inhalt ohnedies ein von Amts wegen zu verfolgendes Delikt (z.T. mit Ermächtigung des betroffenen Opfers). Ich glaube aber, dass es mehr Möglichkeiten für Oper von Hasspostings geben muss, auf die Ausforschung der

Beschuldigten hinzuwirken. In diesem Sinn wird in meinem Ressort ein Maßnahmenpaket erarbeitet. Am 4. März dieses Jahres hat es dazu auch bereits eine Sitzung einer von mir eingesetzten Expert*innenrunde gegeben; eine noch für März in Aussicht genommene weitere Sitzung dieser Gruppe ist allerdings den aktuellen Entwicklungen im Zusammenhang mit dem neuartigen Coronavirus zum Opfer gefallen.

Ein weiterer Punkt des aktuellen Regierungsprogramms betrifft die Erarbeitung zeitgemäßer und Erweiterung bzw. Präzisierung vorhandener Straftatbestände zur Bekämpfung aller Arten von Cyberkriminalität sowie Prüfung der Erhöhung der derzeit in Geltung stehenden Strafrahmen.

Vorauszuschicken ist dabei, dass im vorliegenden Kontext EU- und andere europarechtliche Vorgaben bestehen, namentlich die EU-Richtlinie 2013/40 über Angriffe auf Informationssysteme (die Cybercrime im engeren Sinn betrifft) sowie die Cybercrime-Konvention des Europarats aus dem Jahr 2001 (die sowohl Cybercrime im engeren Sinn als auch Aspekte von Cybercrime im weiteren Sinn, z.B. Kinderpornographie im Internet umfasst). In Bezug auf beide Rechtsinstrumente kann grundsätzlich von Vollumsetzung ausgegangen werden.

Aktuell zeichnen sich in diesem Zusammenhang folgende Vorhaben ab:

Das zweite in Arbeit befindliche Vorhaben betrifft die Umsetzung der Richtlinie (EU) 2019/713 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln. Eine der wesentlichen Neurungen dieser Richtlinie besteht nämlich darin, dass nicht mehr nur körperliche unbare Zahlungsmittel, sondern auch nicht körperliche unbare Zahlungsmittel erfasst werden. Die Richtlinie wurde im Wesentlichen unter der österreichischen Ratspräsidentschaft in der zweiten Jahreshälfte 2018 verhandelt und zum Abschluss gebracht. Sie ersetzt und aktualisiert einen Rahmenbeschluss aus 2001. Dieser Rahmenbeschluss wurde in Österreich umgesetzt, insbesondere durch Einfügung der §§ 241a ff in das StGB. Abgesehen von dem Anpassungsbedarf bei der Definition in § 74 StGB sind nach derzeitigem Stand der Überlegungen geringfügige Anpassungen im Bereich der §§ 241b und 241f sowie 148a StGB erforderlich. (Des Weiteren könnte sich ein Handlungsbedarf insb. in den – überwiegend außerhalb der Zuständigkeit des BMJ gelegenen – Bereichen Prävention, Opferschutz und Datenerfassung ergeben.) Die Umsetzungsfrist für die Umsetzung der Richtlinie läuft noch bis 31.5.2021, und ich werde rechtzeitig einen entsprechenden Entwurf vorlegen.

Zur Frage 10:

Wird der Bereich zur Bekämpfung von Cyberkriminalität personell und finanziell aufgestockt werden:

a. Wenn ja: In welchem Ausmaß (detaillierte Darstellung)

b. Wenn nein: Warum nicht?

Ganz generell bin ich bestrebt, den Staatsanwaltschaften die erforderlichen personellen Ressourcen zur Verfügung zu stellen, damit diese die gestiegenen Herausforderungen insbesondere auf dem Gebiet der Terrorismusbekämpfung sowie der Bekämpfung von Cybercrime und Hass im Netz rasch und qualitätsvoll bewältigen können. Im Rahmen der jüngsten Budget- und Personalverhandlungen ist es mir gelungen, sowohl für die Staatsanwält*innen als auch für den Supportbereich der Staatsanwaltschaften zusätzliche Planstellen zu erhalten, die nicht zuletzt zur wirksamen Bekämpfung neuer Formen strafbaren Handelns zur Verfügung stehen werden.

Um Richterinnen und Richtern sowie Staatsanwältinnen und Staatsanwälten das notwendige Rüstzeug zur effektiven Bekämpfung von „Cyberkriminalität“ an die Hand zu geben, werden auch im Bereich der justiziellen Aus- und Fortbildung zahlreiche hierauf abzielende Maßnahmen gesetzt.

Der Oberste Gerichtshof, die vier Oberlandesgerichte, die Vereinigung der Österreichischen Richterinnen und Richter, die Vereinigung Österreichischer Staatsanwältinnen und Staatsanwälte, die vier Oberstaatsanwaltschaften und das Bundesministerium für Justiz (BMJ) bieten jährlich eine Vielzahl von Fortbildungsveranstaltungen für Richter*innen sowie Staatsanwältinnen und Staatsanwälte auf dem Gebiet des Strafrechts an. Regelmäßig werden in diesen Veranstaltungen aktuelle Themen behandelt, unter anderem auch das immer relevanter werdende Phänomen der Kriminalität im Netz.

Da dem BMJ im Bereich der Aus- und Fortbildung – neben der Planung und Durchführung eigener Veranstaltungen – im Wesentlichen eine Koordinierungs- und Aufsichtsfunktion zukommt, liegen nicht zu allen im Justizressort abgehaltenen Veranstaltungen Detailprogramme vor. Aus diesem Grund verstehen sich die nachfolgenden Ausführungen als exemplarischer Auszug aus dem Aus- und Fortbildungsprogramm des Justizressorts im Zusammenhang mit dem Themenkomplex „Cyberkriminalität“.

Einschlägige Straftatbestände, die in den letzten Jahren vermehrt im Internet begangen wurden, wie etwa Verstöße gegen das Verbotsgesetz, Verhetzung, „Cyber-Mobbing“ aber auch Vermögensdelikte, werden im Rahmen der laufenden Ausbildungskurse für

Richteramtsanwärter*innen insbesondere auch anhand konkreter Beispiele aus dem Netz besprochen; sie sind ebenfalls Prüfungsstoff bei der Richteramtsprüfung.

Im Bereich der Fortbildung der Richter*innen sowie Staatsanwältinnen und Staatsanwälte werden laufend Seminare und Tagungen abgehalten, die den Themenkomplex „Cyberkriminalität“ (mit)behandeln. Besonders hervorzuheben sind in diesem Zusammenhang folgende justizeigenen Seminare:

- „46. Fortbildungsseminar für Strafrecht und Kriminologie“ (21.-23. Februar 2018)
- „Kriminalität und Extremismus im Netz“ (27. Juni 2018)
- „Cyberkriminalität - Ein Phänomen unserer Zeit und seine Bekämpfung durch die Strafverfolgungsbehörden“ (24. September 2018)
- „47. Fortbildungsseminar für Strafrecht und Kriminologie“ (20.-22. Februar 2019)
- Richter/innenwoche 2019 zum Thema „Digital Justice – Die Zukunft ist da“ (20.-23. Mai 2019)
- „Anonymität im Netz“ (11. November 2019)
- „Cybercrime - Ermittlungsansätze und rechtliche Rahmenbedingungen“ (20.-22. November 2019)

Darüber hinaus beschäftigen sich zahlreiche Fachgruppenseminare mit einschlägigen Themen. Hervorgehoben werden darf etwa das zweijährige „Curriculum für Jugendrichter*innen und Jugendstaatsanwältinnen und -staatsanwälte“ (zuletzt von 12 März 2018 bis 16. Dezember 2019). Auch eigens auf die Tätigkeit der Staatsanwältinnen und Staatsanwälte zugeschnittene Veranstaltungen beleuchten regelmäßig den Themenkomplex „Cyberkriminalität“. So beschäftigte sich das Forum der Staatsanwältinnen und Staatsanwälte – die größte Fachveranstaltung für Staatsanwältinnen und Staatsanwälte, die jährlich ein großes Publikum anzieht – schon im Jahr 2017 mit den Gefahren des Internets einschließlich hate crimes.

Ergänzend dazu besteht für Richter*innen, Staatsanwältinnen und Staatsanwälte sowie Richteramtsanwärter*innen zusätzlich zum justizinternen Fortbildungsangebot die Möglichkeit, an einschlägigen Fortbildungen ausländischer Veranstalter (zB. Europäische Rechtsakademie [ERA], European Judicial Training Network [EJTN] ua) teilzunehmen, um so das Thema auch aus einem internationalen Blickwinkel erörtern zu können. Die Teilnahme an (nationalen und internationalen) Seminaren und Fachtagungen gilt als Dienst.

Da es sich bei diesem Themenkomplex um ein zunehmend relevanter werdendes Phänomen handelt, das angesichts der immer weiter voranschreitenden Technologisierung

und Digitalisierung der Gesellschaft die Justiz voraussichtlich auch in den nächsten Jahren zunehmend beschäftigen wird, beabsichtigt das BMJ auch in Zukunft in diesem Bereich eine quantitativ und qualitativ adäquate Aus- und Fortbildung der Richter*innen sowie Staatsanwältinnen und Staatsanwälte sicherzustellen und für ein dementsprechendes Aus- und Fortbildungsangebot Sorge zu tragen.

Dr.in Alma Zadić, LL.M.

REPUBLIK ÖSTERREICH BMJ SIGNATUR	**Datum/Zeit**	2020-04-06T11:59:16+02:00
	Hinweis	Dieses Dokument wurde elektronisch signiert. Auch ein Ausdruck dieses Dokuments hat die Beweiskraft einer öffentlichen Urkunde.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: www.justiz.gv.at/amtssignatur

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-04-06T12:01:11+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	