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: 2021-0.490.127

Ihr Zeichen: BKA - PDion (PDion)7286/J-NR/2021

Wien, am 7. September2021

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 7. Juli 2021 unter der Nr. **7286/J-NR/2021** an mich eine schriftliche parlamentarische Anfrage betreffend Prävention und Bekämpfung von Cyberkriminalität - Umsetzung der Empfehlungen des Rechnungshofes gerichtet.

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

Zu den Fragen 1 und 8:

- *1. Der Rechnungshof empfahl dem BMI und dem BMJ, gemeinsam jene Delikte festzulegen, die unter den Begriff Cyberkriminalität zu subsumieren sind, um auf dieser Basis vergleichbare Zahlen erheben und darstellen sowie wirksame Steuerungsmaßnahmen ergreifen zu können. (TZ 4) Wird diese Empfehlung umgesetzt?*
  - *1.1. Wenn ja, wann und in welcher Form?*
  - *1.2. Wenn nein, warum nicht?*
- *8. Der Rechnungshof empfahl dem BMJ, eine mit dem Innenministerium abgestimmte Strategie für den Bereich Cyberkriminalität - auch im Hinblick auf das Regierungsprogramm 2020- 2024 - zu entwickeln und konsequent zu verfolgen. (TZ 10) Wird diese Empfehlung umgesetzt?*
  - *8.1. Wenn ja, wann und in welcher Form?*
  - *8.2. Wenn nein, warum nicht?*

Das aktuelle Regierungsprogramm weist im Zusammenhang mit der Bekämpfung von Cyberkriminalität dem Justizministerium 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“ zu („Aus Verantwortung für Österreich. Regierungsprogramm 2020 – 2024“, S 27).

Dieser Aufgabe wird vom Bundesministerium für Justiz laufend nachgekommen. Beispielsweise wurde mit dem Hass-im-Netz-Bekämpfungsgesetz, BGBl I Nr. 148/2020, der Tatbestand gegen Cybermobbing, § 107c StGB (nunmehr: „Fortdauernde Belästigung im Wege einer Telekommunikation oder eines Computersystems“), im Sinne dieser Vorgabe ausgeweitet und verschärft.

Überdies läuft aktuell das Begutachtungsverfahren zum Ministerialentwurf eines Bundesgesetzes, mit dem das Strafgesetzbuch und das Zahlungsdienstegesetz 2018 zur Umsetzung der Richtlinie zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln geändert werden, 137/ME 27. GP. Damit werden die zur vollständigen Umsetzung der Richtlinie (EU) 2019/713 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln erforderlichen Regelungen getroffen. Der Entwurf ist insofern als Maßnahme zur Umsetzung des eingangs genannten Punktes des Regierungsprogramms anzusehen, als eine der wesentlichen Neurungen dieser Richtlinie ist, dass nicht mehr nur körperliche unbare Zahlungsmittel, sondern auch nicht körperliche unbare Zahlungsmittel und damit insbesondere auch der Online-Zahlungsverkehr, erfasst werden. Der Entwurf sieht dementsprechend eine Änderung der Definition der unbaren Zahlungsmittel in § 71 Abs. 1 Z 10 StGB und unter anderem auch Verschärfungen im Bereich der §§ 148a, 241b und 241f StGB vor.

Demgegenüber weist das aktuelle Regierungsprogramm die der Empfehlung des Rechnungshofs TZ 10 entsprechende „Erstellung eines Strategiekonzepts zur verbesserten Bekämpfung von Cybercrime in Österreich“ dem Bundesministerium für Inneres zu („Aus Verantwortung für Österreich. Regierungsprogramm 2020 – 2024“, S 155).

Das Justizministerium wird sich selbstverständlich an den diesbezüglichen Arbeiten beteiligen.

Zur Empfehlung des Rechnungshofs TZ 4 betreffend die Festlegung jener Delikte, die unter den Begriff Cyberkriminalität zu subsumieren sind, ist zunächst festzuhalten, dass die vom Rechnungshof zitierte Polizeiliche Kriminalstatistik für 2019 als mengenmäßig größten Teil

der Internetkriminalität den Internetbetrug mit 16.831 Anzeigen ausweist. Dem ist jedoch gegenüberzustellen, dass es 2019 insgesamt 43.887 Betrugsanzeigen gab. Im Jahr 2019 entfielen sohin rund 38 % der Betrugsanzeigen auf Internetbetrug, während dies bei rund 62 % der Betrugsanzeigen nicht der Fall war. Das Delikt des Betruges insgesamt zur Cyberkriminalität zu zählen, wäre daher ebenso wenig sinnvoll, wie den Anteil an Cyberkriminalität an diesem Delikt einfach zu ignorieren. Es geht also vielmehr darum, ob bzw. inwieweit an bestimmte Formen der Cyberkriminalität spezifische Maßnahmen, wie etwa spezifische Behördenstrukturen, spezifische Präventionskonzepte bis hin etwa zur spezifischen statistischen Erfassung geknüpft werden (sollen). Diese Fragen können jedenfalls im Rahmen einer Strategieentwicklung erörtert werden, an der sich das Bundesministerium für Justiz wie ausgeführt nach Maßgabe der zur Verfügung stehenden Ressourcen gerne beteiligen wird.

Zu den Fragen 2 und 7:

- *2. Der Rechnungshof empfahl dem BMI und dem BMJ, die polizeilichen und justiziellen Kriminalstatistiken aufeinander abgestimmt weiterzuentwickeln und methodische Angleichungen vorzunehmen. (TZ 5) Wird diese Empfehlung umgesetzt?*
  - *2.1. Wenn ja, wann und in welcher Form?*
  - *2.2. Wenn nein, warum nicht?*
- *7. Der Rechnungshof empfahl dem BMJ, im Zuge der Weiterentwicklung der internen Informationstechnologie sicherzustellen, dass zuverlässige und aussagekräftige Statistiken zu Anfall und Erledigung von Strafverfahren durch Staatsanwaltschaften und Gerichte generiert werden können; insbesondere sollten auch deliktspezifische Statistiken für den Bereich Cyberkriminalität ermöglicht werden. (TZ 5) Wird diese Empfehlung umgesetzt?*
  - *7.1.Wenn ja, wann und in welcher Form?*
  - *7.2.Wenn nein, warum nicht?*

Im Rahmen der Digitalisierungsinitiative Justiz 3.0 wird eine vollelektronische Verfahrensführung und – damit einhergehend – eine Verbesserung der Datenlandschaft angestrebt. Eine wesentliche Hürde stellen jedoch auch in Zukunft ua die unterschiedlichen Arbeits- und Dokumentationsformen der Polizei und Staatsanwaltschaften dar, welche sich auch in den Registeranwendungen der Ressorts – das Protokollierungssystem PAD des BMI und die Verfahrensautomation Justiz (VJ) – niederschlagen. So würde beispielsweise die weitere Aktualisierung der Fakten im staatsanwaltschaftlichen Ermittlungsverfahren zu vergleichsweise höheren Dokumentations- und Personalaufwänden führen, als dies heute mit der fallorientierten Arbeitsweise der Fall ist. Infolgedessen stellte sich bislang auch die Übernahme der einzelnen Fakten aus dem PAD in die VJ als wenig zielführend heraus. Im

Rahmen der als Teil von Justiz 3.0 geplanten Erneuerung der Verfahrensautomation Justiz ist hingegen die registermäßige Erfassung von Delikten bei Entscheidungen geplant, womit auch eine deutliche Qualitätsverbesserung im Bereich der Statistik erzielt werden kann.

Zur Frage 3:

- *Der Rechnungshof empfahl dem BMI und dem BMJ, die Voraussetzungen für eine systematische Nachverfolgung der Erledigung polizeilicher Anzeigen gegen tatverdächtige Personen z.B. auf Basis bereichsspezifischer Personenkennzeichen zu schaffen. (TZ 5) Wird diese Empfehlung umgesetzt?*
  - *3.1. Wenn ja, wann und in welcher Form?*
  - *3.2. Wenn nein, warum nicht?*

Das bereichsspezifische Personenkennzeichen steht seit November 2020 in allen Registern (dh auch Strafregistern) zur Verfügung und wird - sofern technisch möglich - für die Verfahrensbeteiligten automatisch ermittelt und in der VJ-Datenbank gespeichert. Es wurden somit bereits erste technische Schritte iSd Empfehlungen des Rechnungshofs gesetzt.

Zu den Fragen 4 und 5:

- *4. Der Rechnungshof empfahl dem BMI und dem BMJ, die Kooperation bei der Datenanalyse in Großstrafverfahren auf Basis der im Pilotprojekt 2018 bis 2019 gemachten Erfahrungen institutionalisiert fortzuführen; dabei wären klare rechtliche, organisatorische und finanzielle Rahmenbedingungen festzulegen. (TZ 46) Wird diese Empfehlung umgesetzt?*
  - *4.1. Wenn ja, wann und in welcher Form?*
  - *4.2. Wenn nein, warum nicht?*
- *5. Der Rechnungshof empfahl dem BMI und dem BMJ, nach entsprechender Markterkundung geeignete, anforderungsspezifisch weiterentwickelbare Softwareprodukte für die Analyse großer Datenmengen in Strafverfahren zu beschaffen. (TZ 46) Wird diese Empfehlung umgesetzt?*
  - *5.1.Wenn ja, wann und in welcher Form?*
  - *5.2.Wenn nein, warum nicht?*

Neben den ohnedies laufenden Marktbeobachtungen wird bis zur Identifikation von Alternativen der Einsatz des bereits vorhandenen und in letzten Jahren auch erfolgreich in der Strafverfolgung eingesetzten Werkzeugs m2n forciert. In gemeinsamen projektbezogenen Arbeitsgruppen werden dafür auch die organisatorischen und technischen Rahmenbedingungen für Kooperationen und Schnittstellen erarbeitet.

Zu den Fragen 6 und 12:

- *6. Der Rechnungshof empfahl dem BMI und dem BMJ, ein System zum automationsunterstützten Datenaustausch zwischen Kriminalpolizei und Justiz mit adäquaten Zugriffsmöglichkeiten, einer vollständigen Dokumentation sämtlicher Bearbeitungsschritte und der Archivierung der im Zuge von Strafverfahren sichergestellten Daten und elektronischen Beweismittel einzurichten. (TZ 47) Wird diese Empfehlung umgesetzt?*
  - *6.1. Wenn ja, wann und in welcher Form?*
  - *6.2. Wenn nein, warum nicht?*
- *12. Der Rechnungshof empfahl dem BMJ, ausreichende Kapazitäten für die Archivierung der im Zuge von Strafverfahren sichergestellten Daten und elektronischen Beweismittel aufzubauen. (TZ 47) Wird diese Empfehlung umgesetzt?*
  - *12.1. Wenn ja, wann und in welcher Form?*
  - *12.2. Wenn nein, warum nicht?*

Im Rahmen des Projekts zum Ausbau des Einsatzes von IT-Expert*innen im Strafverfahren ist auch der Aufbau von entsprechenden IT-Infrastruktur-Kapazitäten geplant. Durch diese sollen sowohl die „Inhouse-Speicherung“ von Beweismitteln (an Stelle der Speicherung bei Sachverständigen) ermöglicht, als auch die Voraussetzung für einen automationsunterstützten Datenaustausch geschaffen werden. Für Großverfahren mit enormen Datenmengen (> 10 TB) bleiben jedoch weiterhin rein physikalische Grenzen, welche die faktische Übertragungsmöglichkeit über elektronische Schnittstellen maßgeblich beeinflussen.

Zur Frage 9:

- *Der Rechnungshof empfahl dem BMJ, basierend auf internationalen Beispielen und den Erfahrungen besonders betroffener Staatsanwaltschaften organisatorische Rahmenbedingungen für eine spezialisierte Bearbeitung von Ermittlungsverfahren im Bereich Cyberkriminalität festzulegen. (TZ 43) Wird diese Empfehlung umgesetzt?*
  - *9.1. Wenn ja, wann und in welcher Form?*
  - *9.2. Wenn nein, warum nicht?*

§ 4 Abs. 3 DV-StAG bietet bereits derzeit die Möglichkeit der Schaffung von Sonderreferaten auch für Cyberkriminalität; die Aufzählung des zweiten Satzes ist nicht taxativ („insbesondere“). Cybercrime ist jedoch ein umfassender Begriff, für den bislang eine allgemein gültige Definition fehlt. Cybercrime im engeren Sinn umfasst jene Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikations-technik begangen werden. (z.B. Datenbeschädigung, Hacking, DDoS -

Attacken). Unter Cybercrime im weiteren Sinn versteht man Straftaten, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung und Ausführung für herkömmliche Kriminaldelikte eingesetzt wird, wie z.B. Betrugsdelikte, Kinderpornografie, Cyber-Grooming oder Cyber-Mobbing. Diese Straftaten können praktisch jede Form von Kriminalität annehmen (vgl. https://bundeskriminalamt.at/306/start.aspx).

Die Zielsetzung einer ausdrücklichen staatsanwaltschaftlichen Spezialisierung im Bereich Cyber-Kriminalität verlangt im Vorfeld eine großflächige Analyse unter Einbeziehung der Standesvertretung, wie der Bereich digitaler Verbrechen abzugrenzen ist, um schwierige Zuordnungsprobleme in der praktischen Handhabung zu unterbinden. Ebenso zu beleuchten ist die Frage möglicher Auswirkungen auf die Auslastungsstatistik, hier ist valides Zahlenmaterial zu erheben.

Für die Bündelung staatsanwaltlicher Ermittlungskompetenzen zur Bekämpfung digitaler Verbrechen (Cybercrime) bestehen zwei grundsätzliche Möglichkeiten:

1. Die Schaffung einer „Spezial"-Staatsanwaltschaft mit dem ausschließlichen Fokus auf digitale Verbrechen.

2. Die Schaffung von Sonderreferaten für digitale Verbrechen bei den einzelnen Staatsanwaltschaften.

Vor Setzung dahingehender Schritte ist jedenfalls auch die im Regierungsprogramm vorgesehene „Erarbeitung zeitgemäßer und Erweiterung bzw. Präzisierung vorhandener Straftatbestände zur Bekämpfung aller Arten von Cyberkriminalität" abzuwarten, die unmittelbaren Einfluss auf die vom Begriff Cybercrime umfassten Delikte hat.

Zur Frage 10:

- *Der Rechnungshof empfahl dem BMJ, Vorkehrungen zu treffen, die eine möglichst zeitnahe bundesweite Zusammenführung der Bearbeitung von Cyberkriminalität-Massendelikten mit unbekannter, aber mutmaßlich gleicher Täterschaft bei einer Staatsanwaltschaft sicherstellen. (TZ 43) Wird diese Empfehlung umgesetzt?*
  - *10.1. Wenn ja, wann und in welcher Form?*
  - *10.2. Wenn nein, warum nicht?*

Aufgrund der damit verbundenen Unschärfen, der möglichen Produktion von „Wanderakten" (Anm.: bei Zuständigkeitswechsel bei Staatsanwaltschaften, die zu einem Abtreten von Akten an eine Behörde mit entsprechenden Zeit- und Effizienzverlusten

führen), der möglichen Fülle erforderlicher Zuständigkeitsentscheidungen, der Auslastungssituation, der Auswirkungen auf andere Deliktsbereiche und der unklaren Frage des Vorgehens bei Unzutreffen der Annahme gleicher Täterschaft sind legistische Maßnahmen zur Zusammenführung der Bearbeitung von Cyberkriminalität-Massendelikten mit unbekannter, aber mutmaßlich gleicher Täterschaft nicht zweckmäßig.

Zur Frage 11:

- *Der Rechnungshof empfahl dem BMJ, damit alle mit Cyberkriminalität befassten Bediensteten der Staatsanwaltschaften über das für eine effiziente Fallbearbeitung notwendige technische Grundwissen verfügen, ein Aus- und Fortbildungskonzept zu erarbeiten und umzusetzen, das Schulungsangebot auszuweiten und den selbstständigen Wissenserwerb und -transfer zu unterstützen. Diesbezüglich wäre verstärkt mit dem Bundesministerium für Inneres zusammenzuarbeiten. (TZ 44) Wird diese Empfehlung umgesetzt?*
  - *11.1. Wenn ja, wann und in welcher Form?*
  - *11.2. Wenn nein, warum nicht?*

Im Rahmen des EU-Projekts "Systematische Erfassung diskriminierender Motivlagen bei Strafanzeigen" konzipierte das Bundesministerium für Inneres neben technischen Neuerungen zur Erfassung von Vorurteilskriminalität eine umfassende Online-Schulung zum Thema „Hate Crime". Diese Online-Schulung wurde vom Bundesministerium für Justiz für eine Verwendung in der Justiz leicht adaptiert und um ein spezifisches Modul zum Thema „Hass im Netz" erweitert.

Das seit Juli 2021 aktive e-Learning-Programm ermöglicht einen selbständigen und individuellen Wissenserwerb im Bereich Vorurteilskriminalität und soll die Rechtsanwender*innen zugleich mit den umfangreichen, als Reaktion auf die Herausforderungen neuer Informationstechnologien eingeführten Neuerungen des „Hass-im-Netz-Bekämpfungsgesetzes" (in Kraft seit 1. Jänner 2021) vertraut machen.

Ergänzend dazu wurde mit dem Fortbildungsbeirat akkordiert, dass zusätzliche neue bedarfsgerechte Bildungsveranstaltungen eingeführt werden. Insbesondere wird die Vereinigung der Staatsanwält*innen 2022 ein Seminar zu „Aktuelle Fragen der Cyberkriminalität" anbieten.

Dr.in Alma Zadić, LL.M.

	Datum/Zeit	2021-09-07T18:56:11+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	2021-09-07T19:07:52+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.	