

2159 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVII. GP

Bericht des Justizausschusses

über die Regierungsvorlage (2088 der Beilagen): Bundesgesetz, mit dem das Strafgesetzbuch und das Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG geändert werden

1. Das Regierungsprogramm 2020-2024 „Aus Verantwortung für Österreich“ sieht im Kapitel „Justiz und Konsumentenschutz“ u.a. die „Erarbeitung zeitgemäßer und Erweiterung bzw. Präzisierung vorhandener Straftatbestände zur Bekämpfung aller Arten von Cyberkriminalität sowie Prüfung der Erhöhung der derzeit in Geltung stehenden Strafraahmen“ (S. 27) sowie die „Prüfung von strafrechtlichen Bestimmungen, die Einfluss auf den Wirtschaftsstandort haben (verstärkter Schutz von Geschäfts- und Betriebsgeheimnissen sowie Novellierung der Bestimmungen über Industriespionage)“ (S. 27) vor.

2. Die Bedeutung des Internets, sozialer Medien und smarter Technologien nimmt im Wirtschafts- wie auch im Privatleben stetig zu. Die COVID-19-Pandemie hat diese Entwicklung nochmals deutlich verstärkt und aufgezeigt. Mit der zunehmenden Verlagerung des Lebens ins Internet und der Verwendung von Computertechnologien im Alltag geht auch ein signifikanter Anstieg der Kriminalität in diesen Bereichen einher. Die jährlichen Cybercrime-Berichte des Bundeskriminalamts zeichnen ein deutliches Bild: Wurden im Jahr 2016 bundesweit noch 13.103 Cybercrime-Delikte angezeigt, so waren es im Jahr 2019 28.439 und im Jahr 2020 schließlich 35.915, der Anstieg vom Jahr 2019 auf das Jahr 2020 liegt sohin bei 26,3% (Bundesministerium für Inneres, BKA, Cybercrime Report 2020, S. 36). Im Jahr 2021 wurden schließlich 46.179 Cybercrime-Straftaten angezeigt, was einem Anstieg im Vergleich zum Vorjahr um 28,59% entspricht (Bundesministerium für Inneres, BKA, Cybercrime Report 2021, S. 27).

Im Bereich der Cybercrime-Delikte bestehen auch internationale Vorgaben. Insbesondere zu nennen sind das von Österreich im Jahr 2012 ratifizierte Übereinkommen zur Computerkriminalität des Europarats, BGBl. III Nr. 140/2012, sowie die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl. Nr. L 218 vom 14.08.2013, S. 8ff (in der Folge „**RL 2013/40**“). Zur vollständigen Umsetzung der RL 2013/40 wurden mit dem Strafrechtsänderungsgesetz 2015, BGBl. I Nr. 112/2015 Änderungen in den Tatbeständen der §§ 118a, 126a und 126b StGB vorgenommen (vgl. EBRV 689 BlgNR 25. GP, S. 20, 22). Diese sind am 1.1.2016 in Kraft getreten.

In der aktuellen Legislaturperiode wurden bereits im Jahr 2021 mit dem Bundesgesetz, 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, BGBl. I Nr. 201/2021, einige Änderungen im Bereich der Cybercrime-Delikte vorgenommen. Dieses Bundesgesetz diente der vollständigen Umsetzung der Richtlinie (EU) 2019/713 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI des Rates, ABl. Nr. L 123 vom 10.05.2019 S. 18ff (in der Folge „**RL 2019/713**“). Unter anderem wurden die Strafdrohungen mehrerer Tatbestände erhöht bzw. Qualifikationstatbestände eingeführt, z.B. in § 148a Abs. 3 StGB und § 126c Abs. 1 StGB.

Die im Lichte der Vorgaben des Regierungsprogramms vorgenommene Prüfung hat ergeben, dass weitere inhaltliche Änderungen in den (Grund)-Tatbeständen der Cybercrime-Delikte ieS (also insbesondere der §§ 118a, 119, 119a, 126a, 126b und 126c StGB) derzeit nicht angezeigt scheinen. Zwar bestehen mitunter zu Einzelfragen unterschiedliche Auffassungen im Schrifttum, doch können keine einhellig konstatierten

oder durch (höchstgerichtliche) Rechtsprechung untermauerten Lücken im materiellen Strafrecht ausgemacht werden, deren Schließung erforderlich wäre. Dies gilt insbesondere auch im Lichte der Bindung an die erwähnten internationalen bzw. europarechtlichen Verpflichtungen sowie der *ultima ratio*-Funktion des Strafrechts.

Aufgrund der großen Bedeutung, die die automationsunterstützte Datenverarbeitung mittlerweile im Leben jedes Einzelnen einnimmt und der sich daraus ergebenden möglichen Bedrohungslagen sowohl auf individueller Ebene als auch aus gesamtgesellschaftlicher Sicht (etwa bei Beeinträchtigungen kritischer Infrastruktur) soll aber dem erhöhten sozialen Störwert verschiedener bestehender Cybercrime-Delikte ieS durch eine Erhöhung von Strafdrohungen Rechnung getragen werden.

3. Auch im Bereich der Straftatbestände zum Schutz von Geschäfts- und Betriebsgeheimnissen (§§ 122-124 StGB) wird eine Anhebung der Strafdrohungen vorgeschlagen. Überdies sollen § 122 StGB (Verletzung von Geschäfts- und Betriebsgeheimnissen) und § 123 StGB (Auskundschaftung eines Geschäfts- und Betriebsgeheimnisses) hinkünftig als Ermächtigungsdelikte, sohin als – wenn auch weiterhin (letztlich) in der Ingerenz des:der Verletzten gelegene – Offizialdelikte ausgestaltet sein. Die verletzte bzw. geschädigte Person soll damit vom Kostenrisiko befreit werden, wenn er:sie die Strafverfolgung wünscht; im Hinblick auf den sensiblen Gegenstand der bezughabenden Causen (Verletzung von Geschäfts- und Betriebsgeheimnissen) soll er:sie letztlich darüber entscheiden können, ob gegebenenfalls überhaupt eine Strafverfolgung Platz greifen soll. Darüber hinaus soll aus systematischen Gründen auch die Strafdrohung des § 121 StGB (Verletzung von Berufsgeheimnissen) als gegenüber § 122 StGB speziellere Norm entsprechend angehoben werden.

Die Erhöhung der Strafdrohungen in § 118a Abs. 1, § 119 Abs. 1, § 119a Abs. 1, § 121 Abs. 1 und Abs. 2, § 122 Abs. 1 und Abs. 2 sowie § 126c Abs. 1a StGB führt zu einer Verschiebung der Zuständigkeit für das Hauptverfahren vom Bezirksgericht zum Einzelrichter des Landesgerichts, was auch einen gewissen Bündelungseffekt mit sich bringen soll. Mit der Erhöhung der Strafdrohungen geht schließlich auch eine Erweiterung des Spektrums an Ermittlungsmaßnahmen einher.

4. Parallel dazu wird auch für die Straftatbestände zum Schutz von Geschäfts- und Betriebsgeheimnissen im Bundesgesetz gegen den unlauteren Wettbewerb 1984 (UWG), BGBI. Nr. 448/1984, namentlich die §§ 11 und 12 UWG, eine deutliche Anhebung der Strafdrohungen vorgeschlagen, nämlich von bisher drei Monaten Freiheitsstrafe auf ein Jahr. Damit soll auch die Umsetzung von Art. 16 der Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. Nr. L 157 vom 15.06.2016 S. 1 (in der Folge „**RL 2016/943**“), verbessert werden (auch wenn diese RL – anders als die beiden oben genannten RL 2013/40 und 2019/713 – nicht zu Sanktionen im gerichtlichen Strafrecht verpflichtet).

Auch hier sollen die Straftatbestände von Privatanklage- in Ermächtigungsdelikte umgewandelt werden. Schließlich soll eine Zuständigkeit des Einzelrichters des Landesgerichts für das Hauptverfahren verankert werden, um auch hier den erwähnten Bündelungseffekt zu erreichen.

Der Justizausschuss hat die gegenständliche Regierungsvorlage in seiner Sitzung am 28. Juni 2023 in Verhandlung genommen. An der Debatte beteiligten sich außer dem Berichterstatter Abgeordnetem Mag. Klaus **Fürlinger** die Abgeordneten Mag. Ulrike **Fischer**, Sabine **Schatz** und Dr. Johannes **Margreiter** sowie die Bundesministerin für Justiz Dr. Alma **Zadić**, LL.M.

Bei der Abstimmung wurde der in der Regierungsvorlage enthaltene Gesetzentwurf mit Stimmenmehrheit (dafür: V, S, F, G, dagegen: N) beschlossen.

Als Ergebnis seiner Beratungen stellt der Justizausschuss somit den **Antrag**, der Nationalrat wolle dem von der Bundesregierung vorgelegten Gesetzentwurf (2088 der Beilagen) die verfassungsmäßige Zustimmung erteilen.

Wien, 2023 06 28

Mag. Klaus Fürlinger

Berichterstattung

Mag. Michaela Steinacker

Obfrau

