Entwurf

Erläuterungen:

I. Allgemeiner Teil

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 Strafrahmen“ (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. 1 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), BGBl. 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 verpflichten).

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.

Kompetenzgrundlage:

Der vorliegende Entwurf stützt sich auf Art. 10 Abs. 1 Z 6 B-VG (Strafrechtswesen).

Besonderheiten des Normerzeugungsverfahrens:

Keine.

Verhältnis zu Rechtsvorschriften der Europäischen Union:

Mit § 118a, § 119, § 119a und § 126c StGB werden u.a. auch Vorgaben der RL 2013/40 und der RL 2019/713 umgesetzt. Durch die vorgeschlagenen Änderungen bleibt die vollständige Umsetzung dieser Richtlinien unbeeinträchtigt aufrecht.

Mit der Erhöhung der Strafdrohungen in den §§ 11, 12 UWG soll die Umsetzung von Art. 16 der Richtlinie 2016/943 verbessert werden.

II. Besonderer Teil

Zu Artikel 1 (StGB)

Zu Z 1 bis 5 (§ 118a, § 119, § 119a StGB):

Der Entwurf schlägt vor, die Strafdrohungen in § 118a StGB zu erhöhen: Die Strafdrohung des Grunddelikts soll von Freiheitsstrafe bis zu sechs Monaten oder Geldstrafe bis zu 360 Tagessätzen auf bis zu zwei Jahre Freiheitsstrafe erhöht werden. Darauf aufbauend soll die Tat nach § 118a Abs. 2 und Abs. 4 erster Fall StGB mit bis zu drei Jahren Freiheitsstrafe, jene nach Abs. 4 zweiter Fall mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bedroht werden. Unter einem sollen die Strafdrohungen in § 119 StGB und § 119a StGB auf bis zu zwei Jahre Freiheitsstrafe angehoben werden.

Mit der stetig größer werdenden Bedeutung der Informations- und Kommunikationstechnologie für weite Teile der Bevölkerung steigen auch die negativen Auswirkungen von Tathandlungen nach § 118a StGB,

§ 119 StGB und § 119a StGB. Nicht selten betreffen diese die Privatsphäre der:des Einzelnen, etwa im Bereich des *Internet of Things* (*Salimi*, Cybercrime und Cybersicherheit – Aktuelle Bedrohungen und die Antworten des Strafrechts in Müller (Hrsg.), Datenschutz-Informationsfreiheit-Geheimnisschutz [2019] 265, 272). Dies gilt z.B. auch für das Hacking einer Webcam eines Computers oder Laptops zum geheimen Ausspähen des Besitzers:der Besitzerin (§ 118a Abs. 1 Z 1 StGB), die Erstellung von BOT-Netzwerken, um Daten, die im Opfer-PC gespeichert sind, auszuspionieren (§ 118a Abs. 1 Z 2 StGB; vgl. zu BOT-Netzwerken auch *Reindl-Krauskopf*, Cyberstrafrecht im Wandel, ÖJZ 2015 112 [113f]), Hardware- bzw. Software-Keylogger oder Sniffer-Programme (vgl. *Bergauer* in Kert/Kodek, HB Wirtschaftsstrafrecht[2] [2022] Kap 11 Rz 11.194). Durch eine Erhöhung der Strafdrohungen soll der erhöhte soziale Störwert dieser Taten zum Ausdruck gebracht werden.

Zu Z 6 bis 14 (§ 121, § 122, § 123 und § 124 StGB):

Der wirksame Schutz von Geschäfts- und Betriebsgeheimnissen ist essentiell für die Wettbewerbsfähigkeit und den Markterfolg der Unternehmen und wirkt sich direkt auf ihre Motivation für Forschungs- und Entwicklungstätigkeiten aus. Dies hat wiederum Einfluss auf die Attraktivität des Wirtschaftsstandorts. Gleichzeitig erhöhen Faktoren wie die breitere Online-Präsenz von Unternehmen, die Zunahme der Globalisierung von Märkten und die Entwicklung neuer Technologien die Gefahr der Verletzung von Geschäfts- und Betriebsgeheimnissen. Unter diesem Gesichtspunkt wurde – in Umsetzung 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 15.6.2016 S. 1 – mit der UWG-Novelle 2018 ein ganzes „Paket“ zivilrechtlicher Bestimmungen zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung eingeführt.

Im Umsetzung des Regierungsprogramms 2020-2024 sollen nunmehr im Hinblick auf einen verstärkten Schutz von Geschäfts- und Betriebsgeheimnissen die diesbezüglichen strafrechtlichen Regelungen verschärft werden. Es wird daher eine Anhebung der Strafdrohungen in den §§ 122, 123 und 124 StGB vorgeschlagen. Auch sollen § 122 StGB und § 123 StGB künftig als Ermächtigungsdelikte ausgestaltet sein.

Da § 121 StGB eine *lex specialis* zu § 122 StGB darstellt (vgl. *Tipold* in Leukauf/Steininger, StGB[4] § 121 [Stand 1.10.2016, rdb.at] Rz 38) und die von § 121 insbesondere geschützten Gesundheitsdaten gleichwertigen Schutz genießen sollen wie Geschäfts- und Betriebsgeheimnisse nach § 122 StGB, ist auch eine entsprechende Erhöhung der Strafdrohungen des § 121 StGB und eine Umgestaltung zum Ermächtigungsdelikt systematisch geboten.

Zu Z 15 bis 17 (§ 126c StGB):

§ 126c Abs. 1 StGB ist derzeit mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen bedroht. 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, wurde die Strafdrohung (nur) für Taten, die in Bezug auf einen betrügerischen Datenverarbeitungsmissbrauch (§ 148a) begangen werden, auf bis zu zwei Jahre Freiheitsstrafe angehoben. Diese – der Umsetzung der RL 2019/713 geschuldete – punktuelle Anhebung der Strafdrohung nur in Bezug auf § 148a StGB wurde im Begutachtungsverfahren (137/ME, 27. GP) kritisiert. Angesichts von Phänomenen wie der Herstellung und Verbreitung von Computerprogrammen wie „WannaCry“, die Systemzusammenbrüche herbeiführen können, oder Phishing Software, mit deren einmaligem Einsatz bereits zahllose Personen geschädigt werden können, scheint eine Anhebung der Strafdrohung des § 126c Abs. 1 StGB auf bis zu zwei Jahre Freiheitsstrafe sachgerecht. Im Übrigen nennt der Cybercrime-Report 2021 als eine aktuelle Entwicklung die Zunahme angebotener Leistungen von „*Crime as a Service*“ Diensten (Caas) im Internet, darunter vorwiegend Hackingtools und Schadsoftware, wie beispielsweise Verschlüsselungstrojaner (Bundesministerium für Inneres, BKA, Cybercrime Report 2021, S. 10).

Andere Cybercrime-Delikte ieS kennen bereits Qualifikationstatbestände im Zusammenhang mit kritischer Infrastruktur (§ 74 Abs. 1 Z 11 StGB). So stellt insbesondere § 126a Abs. 4 Z 2 StGB darauf ab, dass durch die Tat wesentliche Bestandteile der kritischen Infrastruktur beeinträchtigt werden, § 126b Abs. 4 Z 2 StGB darauf, dass die Tat gegen ein Computersystem verübt wird, das ein wesentlicher Bestandteil der kritischen Infrastruktur ist. In diesem Zusammenhang scheint es auch sachgerecht, eine vergleichbare Qualifikation in § 126c Abs. 3 StGB einzuführen. Demnach soll mit Freiheitsstrafe bis zu drei Jahren bestraft werden, wer die Tat nach Abs. 1 in Bezug auf ein Computerprogramm oder eine damit vergleichbare Vorrichtung oder ein Computerpasswort, einen Zugangscode oder damit vergleichbare Daten begeht, die geeignet sind, eine Beeinträchtigung wesentlicher Bestandteile der kritischen Infrastruktur (§ 74 Abs. 1 Z 11) zu verursachen.

Zu Artikel 3 (UWG)

Zu Z 1 (§ 11 Abs. 1 und § 12 Abs. 1 UWG):

Die §§ 11 und 12 UWG enthalten Straftatbestände gegen die Verletzung von Geschäfts- und Betriebsgeheimnissen und den Missbrauch anvertrauter Vorlagen; die Strafdrohung beträgt aktuell drei Monate Freiheitstrafe oder Geldstrafe bis 180 Tagessätzen.

Vorgeschlagen wird, analog zu den §§ 121 – 124 StGB auch hier die Strafdrohungen deutlich anzuheben, nämlich auf ein Jahr Freiheitsstrafe bzw. auf 720 Tagessätze Geldstrafe zu vervierfachen. Dass alternativ zu einer Freiheitsstrafdrohung von einem Jahr eine Geldstrafe bis 720 Tagessätze angedroht ist, entspricht der Systematik im StGB.

Zu Z 2 (§ 11 Abs. 3 und § 12 Abs. 3 UWG):

Zunächst sollen – analog zu den Geheimnisschutzbestimmungen im StGB – die Straftatbestände nach den §§ 11, 12 UWG von Privatanklage- zu **Ermächtigungsdelikten** umgestaltet werden. Damit werden die Inhaber von Geschäftsgeheimnissen von der Last der Ermittlungen und insbesondere vom Kostenrisiko einer Privatanklage befreit; die Aufgabe, Verletzungen von Geschäftsgeheimnissen zu ermitteln und anzuklagen, soll also von der Allgemeinheit – in Gestalt der Staatsanwaltschaften und der Kriminalpolizei – übernommen werden.

Schließlich wird vorgeschlagen, dass für Hauptverfahren wegen §§ 11, 12 UWG die Zuständigkeit des **Einzelrichters des Landesgerichts** verankert wird.