BUNDESARBEITSKAMMER

PRINZ-EUGEN-STRASSE 20-22
1040 WIEN
www.arbeiterkammer.at
erreichbar mit der Linie D

Bundesministerium für Justiz
Museumstraße 7
1070 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel **501 65**	Fax **501 65**	Datum
2023-0.091.937	AR-GStBK/Jh	Dr David Koxeder	DW 16434	12471	14.04.2023

Bundesgesetz, mit dem das Strafgesetzbuch und das Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG geändert werden

Die Bundesarbeitskammer (BAK) bedankt sich für die Übermittlung des Entwurfs und nimmt dazu wie folgt Stellung.

Zum Inhalt des Entwurfs:
Die gegenständliche Novelle zielt darauf ab, Cyber-Kriminalität effektiv zu bekämpfen sowie einen wirksameren Schutz von Geschäfts- und Betriebsgeheimnissen zu gewährleisten. Insofern wird unter anderem in den Bereichen der Verletzungen der Privatsphäre und bestimmter Berufsgeheimnisse die Anhebung der Strafdrohungen und die Einführung von neuen Qualifikationen beabsichtigt. Parallel dazu werden auch die Strafdrohungen der Straftatbestände zum Schutz von Geschäfts- und Betriebsgeheimnissen im Bundesgesetz gegen den unlauteren Wettbewerb 1984 (UWG) deutlich angehoben. Damit einhergehend erfolgt eine Umgestaltung der Straftatbestände (§§ 121, 122 und 123 StGB sowie der §§ 11 und 12 UWG) von Privatanklage- in Ermächtigungsdelikte. Schließlich kommt es aufgrund der Erhöhung der Strafdrohungen zu einer Verschiebung der Zuständigkeit für das Hauptverfahren vom Bezirksgericht zum Einzelrichter des Landesgerichts, was auch einen gewissen Bündelungseffekt nach sich ziehen soll. Darüber hinaus werden mit der gegenständlichen Novellierung auch Vorgaben von Richtlinien umgesetzt (ua RL 2013/40, RL 2019/713, RL 2016/943).

Mit dem Anstieg der Bedeutung des Internets und der sozialen Medien sowohl im Privatleben als auch im Wirtschaftsleben ist es im Vergleichszeitraum 2016 bis 2021 auch zu einem enormen Anstieg von Cyber-Kriminalität in Form von Hacking, Datenbeschädigung, Betrugsdelikte, Drogenhandel im Darknet, Online-Kindesmissbrauch sowie Cybergrooming oder Cybermobbing gekommen (Web_Cybercrime_2016.pdf (bundeskriminalamt.at) (03.04.2023); Cybercrime Report (bmi.gv.at) (03.04.2023). Insbesondere die Covid19-Pandemie haben Kri-

minelle ausgenutzt und ihr Vorgehen weiter angepasst. Mittlerweile kann das Fachwissen, das es für die Begehung von „Online-Straftaten“ braucht, zugekauft werden, sodass es auch weniger technikaffinen Tätern ermöglicht wird, ihre illegalen Machenschaften umzusetzen. Parallel dazu erschweren verschiedene Verschleierungsmöglichkeiten im Internet die Ermittlungen der Strafverfolgungsbehörden.

Das Wichtigste in Kürze:

- Die BAK befürwortet grundsätzlich die vorgeschlagenen Änderungen bzw Anpassungen, die Strafdrohungen etwa bei der Beeinträchtigung kritischer Infrastruktur im Bereich der Cyber-Kriminalität zu erhöhen.

- Rechtliche Rahmenbedingungen sind die Grundvoraussetzungen für eine effektive, erfolgreiche und nachhaltige Bekämpfung von Cyber-Kriminalität. Die BAK ortet allerdings eine Tendenz des Gesetzgebers, auf drängende gesellschaftliche Probleme in erster Linie oder sogar ausschließlich mit einer Erhöhung von Strafrahmen zu reagieren. So sehr in gewissen Fällen eine solche Verschärfung der Strafdrohungen nachvollziehbar oder geboten erscheint, ist anzumerken, dass die Bekämpfung von kriminellen Handlungen, wie auch in diesem Fall, darüber hinaus eines wesentlich breiteren Ansatzes bedarf. So ist es zB dringend erforderlich, intensiv in Präventionsarbeit zu investieren. Es braucht eine verbesserte Bewusstseinsbildung für mehr Sicherheit im Internet. Gleichzeitig muss die Widerstandsfähigkeit gegen kriminelle Cyber-Angriffe in der Wirtschaft gestärkt und eine schnelle, wirksame Reaktion auf Cyber-Vorfälle ausgebaut werden. Unternehmen sollten iZm dem UWG nicht in falscher Sicherheit gewiegt werden, mangelhafte Sicherheitsstandards durch erhöhte Strafdrohungen gegen Mitarbeiter:innen kompensieren zu können Nicht zuletzt müssen daher die Strafverfolgungsbehörden sowie Anlauf- und Meldestellen mit den notwendigen personellen, technischen und logistischen Ressourcen für eine zielgerichtete Cyber-Kriminalitätsbekämpfung ausgestattet werden.

Zu den wesentlichen Bestimmungen des geplanten Entwurfs:

Zu Artikel 1 (StGB):

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

Der gegenständliche Entwurf schlägt eine Strafverschärfung der Strafdrohungen in §§ 118a, 119 und 119a StGB vor und begründet dies damit, dass mit der stetig größer werdenden Bedeutung der Informations- und Kommunikationstechnologie für weite Teile der Bevölkerung auch die negativen Auswirkungen von Tathandlungen nach den zuvor genannten Bestimmungen steigen und durch die Erhöhung der Strafdrohungen der erhöhte soziale Störwert dieser Taten zum Ausdruck gebracht werden soll.

Zweifellos müssen Strafen tat- und schuldangemessen sein und dürfen keine Bagatellisierung der Tat in der Gesellschaft zum Ausdruck bringen. Das Strafrecht soll Verbrechen verhindern,

und zur Erreichung der Strafzwecke der Spezial- und Generalprävention gehört auch, dass Straftatbestände mit entsprechenden Strafdrohungen ausgestattet sind. Eine (laufende) Verschärfung der Strafen werden aber potenzielle Straftäter von der Begehung der Taten nicht abschrecken, wenn zentrale begleitende Maßnahmen unterbleiben. Vielmehr müsste im Zuge der gegenständlichen Novellierung parallel in eine fundierte und treffsichere Präventionsarbeit insbesondere im Bereich der Computer- und Internetsicherheit investiert werden. Damit einhergehend bedarf es einer Sensibilisierung und Bewusstseinsbildung in der Bevölkerung durch entsprechend verstärkte Aufklärungs- und Öffentlichkeitsarbeit (zB in den Rundfunkmedien, auf Social-Media, in Form von Informationsveranstaltungen, Informationsbroschüren oder Workshops). Die Aufklärungs- und Öffentlichkeitsarbeit muss zielgruppengerecht erfolgen, wobei damit bereits in Schulen in Form von Vorträgen rund um den sicheren Umgang mit digitalen Medien, Internet und Smartphones begonnen werden sollte bzw bestehende Aktivitäten intensiviert werden sollten. Dies setzt wiederum die Bereitstellung dementsprechender finanzieller Ressourcen voraus. Gleichzeitig sollte im Zuge der Bekämpfung von Cyber-Kriminalität auch eine bessere Vernetzung bzw ein Austausch zwischen den zuständigen Behörden, privaten Organisationen und Institutionen sowie relevanten Unternehmen stattfinden. Zwar werden in der Zwischenzeit Präventionsmaßnahmen – beispielsweise vonseiten des Bundeskriminalamtes gemeinsam mit dem Bundesministerium für Arbeit und Wirtschaft über die Plattform www.fit4internet.at – angeboten. Die laut Statistik stetig steigenden Zahlen der Cybercrime-Delikte belegen jedoch, dass die bisher iZm der Präventionsarbeit, Sensibilisierung und Bewusstseinsbildung gesetzten Schritte noch ausbaufähig sind.

All die zuvor erwähnten Maßnahmen werden im gegenständlichen Entwurf nicht aufgegriffen, obwohl es sich hierbei um Überlegungen handelt, die einen wesentlichen, essenziellen Beitrag zur Eindämmung und Bekämpfung aller Arten der Cyber-Kriminalität leisten würden.

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

Die BAK kann die Überlegung, den Geschädigten durch eine Änderung der Ausgestaltung der bisherigen Privatanklagedelikte zu Ermächtigungsdelikten vom Prozesskostenrisiko zu befreien durchaus nachvollziehen. Gleichzeitig ist anzumerken, dass die geplante Vervierfachung der Strafdrohung völlig unverhältnismäßig erscheint und daher abgelehnt wird. Die Erläuterungen wiesen zutreffend darauf hin, dass sowohl mit dem Strafrechtsänderungsgesetz 2015, als auch mit der UWG-Novelle 2018 umfassende straf- und zivilrechtliche Anpassungen vorgenommen wurden, um unionsrechtlichen Anforderungen und der wachsenden Bedeutung der automationsgestützten Datenverarbeitung und der notwendigen Bekämpfung der Cyberkriminalität zu entsprechen. Auch vor dem Hintergrund, dass der Gesetzgeber iZm der Whistleblower-Richtlinie nahezu jede über das absolute Mindesterfordernis hinausgehende Maßnahme verworfen hat, erscheint besonders unverständlich, warum iZm dem strafrechtlichen (!) Schutz der Geschäfts- und Betriebsgeheimnisse eine so weit gehende Übererfüllung unionsrechtlicher Vorgaben angestrebt wird.

Eine bessere Unterstützung für Unternehmen, sich und ihre Daten zu schützen, erscheint demgegenüber durchaus nachvollziehbar. Diesbezüglich bedarf es aber weniger strafrechtli-

cher Sanktionsverschärfungen als einer intensiveren Vernetzung und einem Austausch der Unternehmen untereinander, zB durch Schaffung von Plattformen, einer Melde- und Beratungsstelle – die gegebenenfalls die betroffenen Unternehmen bei der strafrechtlichen Anzeige bis hin zu den operativen IT-Security-Dienstleistungen unterstützt – und einer engeren Kooperation mit den zuständigen Behörden, um präventiv und reaktiv gegen Cybercrime vorzugehen. Der gegenständliche Entwurf sieht auch hierzu keine Maßnahmen bzw Bestrebungen des Gesetzgebers vor, weshalb die BAK – ähnlich wie in der zuvor genannten Ziffer – einen Nachholbedarf sieht.

Zu Z 15 bis 17 (§126c StGB):

Nach Ansicht der BAK scheint eine Anhebung der Strafdrohung angesichts des Erfolgsunwerts – insbesondere der Möglichkeit mit speziellen Computerprogrammen Systemzusammenbrüche herbeizuführen bzw zahllose Personen zu schädigen – nachvollziehbar. Es wird allerdings angeregt nochmals zu überdenken, ob eine Verdoppelung der Strafdrohung gegenüber der geplanten Vervierfachung nicht sachgerechter wäre. Sofern eine Zuständigkeit des Einzelrichters am Landesgericht gewünscht ist, erschiene eine verfahrensrechtliche Sonderzuständigkeit für diese Deliktsgruppe die wesentlich sinnvollere Methode als die unverhältnismäßige Anhebung der Strafdrohung, um diese Zuständigkeit zu bewirken.

Auch hierbei ist zu erwähnen, dass – parallel zur Strafverschärfung – Präventionsmaßnahmen samt einer verstärkten Sensibilisierung und Bewusstseinsbildung zum Schutz der Bevölkerung und der Unternehmerlandschaft getroffen werden müssen, die der gegenständliche Entwurf schuldig bleibt.

Zu Artikel 3 (UWG):

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

Vonseiten der BAK wird die beabsichtigte Anhebung der Strafdrohungen auf ein Jahr Freiheitsstrafe bzw 720 Tagessätze Geldstrafe aus den oben zu Z 6 bis 14 angeführten Gründen abgelehnt. Besonders im Kontext gut ausgeprägter zivilrechtlicher Rechtsschutzmechanismen und bereits vorhandener strafrechtlicher Sanktionsnormen scheint eine derartig massive Erweiterung der Strafdrohungen nicht erforderlich und sogar kontraproduktiv, wenn die Strafgerichte noch stärker in grundsätzlich zivilrechtliche Auseinandersetzungen involviert werden. Im Übrigen wird betreffend die im Entwurf außer Acht gelassene Präventionsarbeit auf die obigen Ausführungen verwiesen.

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

Die BAK nimmt die Umgestaltung der Straftatbestände nach den §§ 11 und 12 UWG – analog den Geheimnisschutzbestimmungen des StGB – von Privatanklage- in Ermächtigungsdelikte zur Kenntnis. Dies stellt eine massive Entlastung betroffener Unternehmen (Inhaber:innen von Geschäftsgeheimnissen) von der Ermittlungslast und vor allem vom Kostenrisiko einer Privatanklage dar. Es ist dabei mitzuerwägen, dass Betroffene bzw Verletzte und Geschädigte aufgrund dieses Entfalls des Kostenrisikos eher einer Strafverfolgung zustimmen werden und daher mit einer verstärkten Inanspruchnahme der Strafjustiz gerechnet werden muss.

Die BAK ersucht um Berücksichtigung ihrer Anliegen und Anregungen.

Unterzeichner	Bundeskammer für Arbeiter und Angestellte
Datum/Zeit-UTC	15.04.2023 9:11
Prüfhinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.