Geschäftszahl: 2023-0.603.326

Erlass vom 23. August 2023 über die Regelungen des Bundesgesetzes, mit dem das Strafgesetzbuch und das Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG geändert werden

Am 7. Juli 2023 beschloss der Nationalrat das **Bundesgesetz, mit dem das Strafgesetzbuch und das Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG geändert werden**. Der Bundesrat beschloss in seiner Sitzung am 13. Juli 2023, gegen den Gesetzesbeschluss des Nationalrats keinen Einspruch zu erheben.

Das Bundesgesetz, mit dem das Strafgesetzbuch und das Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG geändert werden, wurde am 29. Juli 2023 als BGBl I Nr. 99/2023 (**Beilage ./A**), kundgemacht und tritt **am 1. September 2023 in Kraft**. Dem gegenständlichen Erlass sind überdies die Erläuterungen zur Regierungsvorlage (ErlRV 2088 BlgNR 27. GP; **Beilage ./B**), die Textgegenüberstellung (**Beilage ./C**) und die Wirkungsorientierte Folgenabschätzung (**Beilage ./D**) angeschlossen. Auf diese Materialien, insbesondere die Erläuterungen zur Regierungsvorlage, wird ausdrücklich hingewiesen.

Die ergänzenden Ausführungen geben die Rechtsansicht des Bundesministeriums für Justiz wieder und verstehen sich unvorgreiflich der unabhängigen Rechtsprechung.

Inhaltsverzeichnis

I. Überblick über die wesentlichen Änderungen des StGB und des UWG

1. Änderungen der Strafdrohungen und Zuständigkeitsverschiebung

Sowohl im Bereich der Cybercrime-Delikte ieS (§§ 118a, 119, 119a und 126c StGB) als auch bei den Straftatbeständen zum Geheimnisschutz (§§ 121 bis 124 StGB sowie §§ 11 und 12 UWG) werden die **Strafdrohungen angehoben**. Lediglich bei Begehung des § 126c StGB in Bezug auf § 148a Abs. 1 StGB wird die Strafdrohung herabgesetzt (s. hierzu unter I.3). Die Änderungen der Strafdrohungen gestalten sich wie folgt:

StGB		Strafdrohung bisher	Strafdrohung neu
§ 118a	**Abs. 1**	FS bis zu sechs Monaten oder GS bis zu 360 TS	**FS bis zu zwei Jahren**
	Abs. 2	FS bis zu zwei Jahren	**FS bis zu drei Jahren**
	Abs. 4 erster Fall		
	Abs. 4 zweiter Fall	FS bis zu drei Jahren	**FS von sechs Monaten bis zu fünf Jahren**
§ 119	**Abs. 1**	FS bis zu sechs Monaten oder GS bis zu 360 TS	**FS bis zu zwei Jahren**
§ 119a	**Abs. 1**		
§ 121	**Abs. 1**		
	Abs. 2	FS bis zu einem Jahr oder GS bis zu 720 TS	**FS bis zu drei Jahren**
§ 122	**Abs. 1**	FS bis zu sechs Monaten oder GS bis zu 360 TS	**FS bis zu zwei Jahren**
	Abs. 2	FS bis zu einem Jahr oder GS bis zu 720 TS	**FS bis zu drei Jahren**
§ 123		FS bis zu zwei Jahren	**FS bis zu drei Jahren**
§ 124		FS bis zu drei Jahren	**FS von sechs Monaten bis zu fünf Jahren**
§ 126c	**bei Begehung in Bezug auf die §§ 118a, 119, 119a, 126a Abs. 2 bis 4, 126b Abs. 2 bis 4 StGB**	FS bis zu sechs Monaten oder GS bis zu 360 TS	**FS bis zu zwei Jahren**
	bei Begehung in Bezug auf § 148a Abs. 1 StGB	FS bis zu zwei Jahren	**FS bis zu sechs Monaten oder GS bis zu 360 TS**
UWG		**Strafdrohung bisher**	**Strafdrohung neu**
§ 11	**Abs. 1**	FS bis zu drei Monaten oder GS bis zu 180 TS	**FS bis zu einem Jahr oder GS bis zu 720 TS**
§ 12	**Abs. 1**		

Diese Anhebung der Strafdrohungen bedeutet in Bezug auf die Vergehen gemäß §§ 118a Abs. 1, 119 Abs. 1, 119a Abs. 1 und 126c Abs. 1a StGB jeweils eine **Zuständigkeitsverschiebung** im staatsanwaltlichen Bereich vom Bezirksanwalt bzw. von der Bezirksanwältin zum Staatsanwalt bzw. zur Staatsanwältin und im gerichtlichen Bereich vom Bezirksgericht zum Landesgericht sowie in Bezug auf die §§ 121, 122 StGB eine entsprechende Verschiebung der Zuständigkeit für das Hauptverfahren von den

Bezirksgerichten auf die Landesgerichte. Hingegen ist bei Begehung des § 126c StGB in Bezug auf § 148a Abs. 1 StGB nunmehr der Bezirksanwalt bzw. die Bezirksanwältin und das Bezirksgericht zuständig.

Auch in Bezug auf die §§ 11 und 12 UWG kommt es im Hinblick auf das Hauptverfahren zu einer Zuständigkeitsverschiebung: Für dieses ist nunmehr die **(Sonder-)Zuständigkeit des Einzelrichters des Landesgerichts** normiert (§§ 11 Abs. 3 und § 12 Abs. 3 UWG).

2. Umgestaltung in Ermächtigungsdelikte

Die **§§ 121, 122 und 123 StGB** sowie die **§§ 11 und 12 UWG** sind nunmehr als **Ermächtigungsdelikte** (anstelle von Privatanklagedelikten) ausgestaltet. Damit entsteht ein (bisher nicht existierender) neuer Tätigkeitsbereich auf Ebene der **Staatsanwaltschaften**.

II. Zu einzelnen Tatbeständen im Detail

1. Änderung des § 126c StGB

In § 126c StGB wird wie auch bei den anderen Cybercrime-Delikten ieS die **Strafdrohung** grundsätzlich von einer Freiheitsstrafe bis zu sechs Monaten oder Geldstrafe bis zu 360 Tagessätzen auf **Freiheitstrafe bis zu zwei Jahren** angehoben (**Abs. 1a**). Der Systematik des StGB folgend, wonach ein Vorbereitungsdelikt nicht strenger bestraft wird als das jeweilige Schädigungsdelikt, betrifft die Anhebung der Strafdrohung allerdings nicht die Begehung des § 126c StGB in Bezug auf § 126a Abs. 1 und § 126b Abs. 1 StGB. Diese Erwägung gilt auch für § 148a Abs. 1 StGB, auf den § 126c Abs. 1 Z 1 StGB nunmehr auch verweist. Bei Missbrauch von Computerprogrammen oder Zugangsdaten in Bezug auf die §§ 126a Abs. 1, 126b Abs. 1 und 148a Abs. 1 StGB beträgt die Strafdrohung daher bis zu sechs Monaten Freiheitsstrafe oder bis zu 360 Tagessätzen Geldstrafe (§ 126c Abs. 1 Z 1 StGB).

In Einklang mit den anderen Cybercrime-Delikten ieS, die einen **Qualifikationstatbestand** im Zusammenhang mit **kritischer Infrastruktur** vorsehen (vgl. §§ 126a Abs. 4 Z 2, 126b Abs. 4 Z 2 StGB), wird ein solcher auch im Hinblick auf Missbrauch von Computerprogrammen oder Zugangsdaten eingeführt. Nach **§ 126c Abs. 3 StGB** ist demnach mit einer Freiheitsstrafe bis zu drei Jahren zu bestrafen, wer die Tat nach Abs. 1 oder Abs. 1a in Bezug auf ein Computersystem 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 StGB) zu verursachen.

Bei der nach § 126c Abs. 3 StGB geforderten Eignung werden nicht nur die technischen Gegebenheiten zu beachten sein, sondern insbesondere auch, ob der:die Täter:in die qualifizierenden Umstände auch in seinen:ihren Vorsatz aufgenommen hat.

2. Strittige Fragestellungen in Zusammenhang mit § 118a StGB

Bei § 118a StGB wird nur die Strafdrohung angehoben; der Tatbestand bleibt inhaltlich unverändert. Das Bundesministerium für Justiz nimmt die Gesetzesänderung dennoch zum Anlass, unvorgreiflich der unabhängigen Rechtsprechung, seine Rechtsansicht zu in der Literatur bisweilen strittigen Fragestellungen in Zusammenhang mit § 118a StGB darzulegen.

2.1. Ausnützen von Sicherheitslücken

§ 118a StGB erfordert in objektiver Hinsicht, dass der:die Täter:in sich durch „Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem“ Zugang dazu verschafft. Verlangt wird damit neben einem gesicherten System, dass der:die Täter:in dieses überwindet, und damit Anstrengungen setzt, um sich über die spezifische Sicherheitsvorkehrung hinwegzusetzen.

Eine **spezifische Sicherheitsvorkehrung im Computersystem** im Sinne des § 118a StGB liegt nach allgemeiner Ansicht dann vor, wenn das System vor unbefugten Eingriffen geschützt wird, so etwa durch Computerpasswörter, Zugangscodes oder biometrische Sicherungen (*Reindl-Krauskopf* in *Höpfel/Ratz*, WK^2 StGB § 118a Rz 22 ff [Stand 1.3.2022, rdb.at]). Keine spezifische Sicherheitsvorkehrung wäre bloß das Versperren eines Raumes, in dem sich ein Computer befindet, oder das Vorsehen von Alarmanlagen (EBRV 1166 BlgNR 21. GP 24; *Leukauf/Steininger/Tipold*, StGB^4 § 118a Rz 5 [Stand 1.10.2016, rdb.at]; *Fabrizy/Michel-Kwapinski/Oshidari*, StGB^{14} § 118a Rz 3 [Stand 10.3.2022, rdb.at]).

Der Begriff des „**Überwindens**“ wurde mit dem Strafrechtsänderungsgesetz 2008, BGBl. I Nr. 109/2007, in den Tatbestand des § 118a StGB aufgenommen. Ziel war es, bestimmte technische Angriffsarten einzubeziehen, die zu keiner Verletzung der Datenintegrität führen. Ein Überwinden erfordert das Setzen von Anstrengungen und damit den Einsatz eines gewissen Maßes an krimineller Energie. Darunter fällt unter anderem das Wählen einer technischen Zugriffsvariante, die dem vorgesehenen Zulassungsverfahren nicht entspricht (*Reindl-Krauskopf* aaO Rz 26). Auch das widerrechtliche Erlangen eines Computerpassworts durch Mitlesen von Datenverkehr im Internet oder das Durchprobieren aller Passwort-Kombinationen („bruteforce-Methode“) ist als Überwinden im Sinne des § 118a StGB zu qualifizieren (*Reindl-Krauskopf* aaO Rz 27).

Ob auch das Ausnützen einer aus einem Programmfehler resultierenden **Sicherheitslücke** auch nach § 118a StGB tatbestandsmäßig ist, wird in der Literatur kritisch diskutiert und bisweilen unterschiedlich beantwortet.

Nach einer Ansicht soll das Nutzen von Fehlern, die standardmäßig in einem Programm enthalten sind, nicht als Überwinden spezifischer Sicherheitsvorkehrungen gewertet werden können. Begründend wird darauf verwiesen, der:die Täter:in würde bildlich gesprochen durch eine **offene Türe** gehen; der Zugriff sei mit einem solchen auf ein ungesichertes System vergleichbar. Dies soll auch dann gelten, wenn die Sicherheitslücke erst unter Einsatz technischen Know-Hows eruiert worden sei. In derartigen Konstellationen würde ein „Überwinden" zwar unter Umständen angenommen werden können, es sei allerdings **keine spezifische Sicherung** gegeben (*Reindl-Krauskopf* aaO Rz 29; *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht Rz 2.28 [Stand 1.9.2018, rdb.at]; *Reindl-Krauskopf*, Cyber Crime – der digitalisierte Täter, ALJ 2017, 110 [114 f]).

Nach anderer Ansicht ist unter Berücksichtigung der **Art der Sicherheitslücke** zu differenzieren: Ist die Sicherheitslücke geradezu offensichtlich, so kann ihr Ausnützen nicht als Überwinden einer spezifischen Sicherheitsvorkehrung im Sinne des § 118a StGB qualifiziert werden. Muss der:die Täter:in demgegenüber ein erhebliches Maß an technischem Know-How und damit konkret auch krimineller Energie einsetzen, um die Sicherheitslücke erst ausfindig zu machen, so kann dieses Vorgehen – bei Erfüllung der weiteren tatbestandsmäßigen Voraussetzungen – Strafbarkeit nach § 118a StGB begründen (*Salimi*, Cybercrime 2018 - Kryptowährungen, Internet of Things und Co als Herausforderungen für das Strafrecht, in JB Wirtschaftsstrafrecht und Organverantwortlichkeit 2018, 7 [16 f]).

Soweit ersichtlich besteht bislang keine höchstgerichtliche Rechtsprechung dazu, ob das Ausnützen einer Sicherheitslücke den Tatbestand des § 118a StGB erfüllt. Aus Sicht des Bundesministeriums für Justiz ist – auch unter Berücksichtigung des Schutzzwecks des § 118a StGB – der zuletzt wiedergegebenen Literaturansicht zu folgen, und demnach – bei Erfüllung der weiteren Tatbestandsmerkmale – von einer Strafbarkeit auszugehen. Eine inhaltliche Überarbeitung des § 118a StGB durch BGBl I Nr. 99/2023 war vor diesem Hintergrund nicht angezeigt.

2.2. „Ethische Hacker"

„Ethisches Hacking" (auch: „friendly hacking") bezeichnet den Zugriff auf Computersysteme zum Zweck der Suche nach Programmfehlern in Computersystemen, die im Weiteren allerdings nicht für kriminelle Zwecke genutzt, sondern den Betroffenen mit dem Ziel der Verbesserung ihrer Sicherheitsstandards mitgeteilt werden sollen. Die Hacker:innen gehen dabei einerseits eigeninitiativ vor, andererseits setzen Unternehmen diese auch spezifisch

ein oder rufen unter Auslobung von Preisen allgemein dazu auf („Bug-Bounty-Programme“).

Ethisches Hacking nach der vorangehenden Definition erfüllt nach Ansicht des Bundesministeriums für Justiz nicht den Tatbestand des § 118a StGB. Wird der:die Hacker:in eigens durch das Unternehmen dazu beauftragt, etwaige Sicherheitslücken, Programmfehler und dergleichen im Computersystem ausfindig zu machen, so ist damit eine **tatbestandsausschließende Verfügungsbefugnis** gegeben. So erfordert Strafbarkeit nach § 118a StGB, dass der:die Täter:in über das Computersystem, zu dem er:sie sich Zugang verschafft, nicht oder nicht allein verfügen darf. Wer verfügungsbefugt ist und damit nicht unberechtigt zugreift, kommt nicht als Täter:in in Betracht (vgl. *Reindl-Krauskopf* in *Höpfel/Ratz*, WK^2 StGB § 118a Rz 10 [Stand 1.3.2022, rdb.at]; *Thiele* in SbgK § 118a Rz 32).

Wurde der:die Hacker:in hingegen nicht beauftragt, sondern handelt er:sie eigeninitiativ, so sind in der Regel die nach § 118a StGB geforderten **subjektiven Tatbestandsvoraussetzungen** nicht gegeben. § 118a StGB erfordert neben dem Tatbildvorsitz einen besonderen erweiterten Vorsatz in Form der Absicht (§ 5 Abs. 2 StGB). In Betracht kommt dabei entweder die **bloße Spionageabsicht** nach § 118a Abs. 1 Z 1 StGB, also die Absicht, sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzen, oder die **Verwendungsabsicht** nach § 118a Abs. 1 Z 2 StGB. Die Verwendungsabsicht umfasst die Absicht, einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, oder durch die Verwendung des Computersystems einen Nachteil zuzufügen. Dem:der Täterin muss es auf die Spionage (Z 1) oder nachteilige Verwendung (Z 2) geradezu ankommen; dass er:sie diese Umstände bloß verwirklichen wollen, reicht demgegenüber nicht aus (vgl. zum Vorsatzerfordernis der Absichtlichkeit u.a. *Reindl-Krauskopf* in *Höpfel/Ratz*, WK^2 StGB § 5 Rz 24 [Stand 1.8.2015, rdb.at]).

Ein:e eigeninitative:r „ethische:r“ Hacker:in wird definitionsgemäß tätig, um Sicherheitslücken im Sinne der jeweiligen Betroffenen aufzudecken, die aufgrund der übermittelten Informationen ihre Sicherheitsstandards verbessern und Programmfehler beheben können sollen. Demgegenüber werden in diesen Fällen die nach § 118a StGB geforderten subjektiven Tatbestandsmerkmale nach Ansicht des Bundesministeriums für Justiz – unvorgreiflich der einzelfallbezogenen Beurteilung durch die unabhängige Rechtsprechung – in der Regel nicht gegeben sein.