WIEN / 10. Juli 2026

Netzsperren im Glücksspielgesetz

Telekommunikationsgesetz, Änderung (125/ME)

Für epicenter.works
Thomas Lohninger
Sebastian Kneidinger
Elise Zimmermann

EPICENTER .WORKS
for digital rights

VORWORT UND KURZFASSUNG

Wir bedanken uns für die Möglichkeit, im Rahmen des Begutachtungsverfahrens[1] nachfolgende Stellungnahme abgeben zu können. Gleichzeitig erlauben wir uns anzumerken, dass die Begutachtungsfrist von lediglich zwei Wochen angesichts der technischen und grundrechtlichen Komplexität des Entwurfs deutlich zu kurz bemessen ist und demokratiepolitisch kritisch zu bewerten ist.

Der vorliegende Entwurf verfolgt das legitime Ziel, wirksamer gegen illegale Glücksspielangebote vorzugehen. Mehrere der vorgesehenen Maßnahmen, insbesondere jene, die unmittelbar gegen rechtswidrige Anbieter oder deren wirtschaftliche Grundlage gerichtet sind, sind aus unserer Sicht grundsätzlich zu begrüßen. **Der Entwurf sieht jedoch unter dem Terminus „Sperrverfügungen" auch Netzsperren vor**. Diese Regelungen greifen in die Infrastruktur des Internets ein und werfen grundlegende netzpolitische und grundrechtliche Fragen auf. Aus diesem Grund setzt sich die vorliegende Stellungnahme ausschließlich mit den Bestimmungen zu Netzsperren auseinander.

Netzsperren unterscheiden sich grundlegend von anderen Maßnahmen der Rechtsdurchsetzung. Sie verpflichten Anbieter der Internetinfrastruktur, den Zugang zu bestimmten Online-Angeboten zu sperren. Anders als Maßnahmen gegen die eigentlichen Rechtsverletzer greifen sie damit bei der Infrastruktur des Internets ein. **Dadurch können ihre Auswirkungen weit über die betroffenen Angebote hinausreichen und auch unbeteiligte Dienste, Inhalteanbieter und Internetnutzer erfassen.** Netzsperren greifen deshalb besonders sensibel in die Meinungs- und Informationsfreiheit sowie das Grundrecht auf Datenschutz ein und können auch die Offenheit und das freie Funktionieren des Internets beeinträchtigen. **Der Gerichtshof der Europäischen Union stellt daher hohe Anforderungen an ihre Ausgestaltung. Diesen Anforderungen wird der Entwurf aus unserer Sicht nicht gerecht.**

Weil Netzsperren auch Unbeteiligte treffen können, besteht das Risiko, dass rechtmäßige Inhalte oder Dienste von einer Sperrmaßnahme erfasst werden (**Overblocking**). Der Entwurf enthält keine ausreichenden Vorkehrungen gegen solche Fehlsperren und sieht **keinen wirksamen Rechtsschutz für betroffene Internetnutzer** vor. Gleichzeitig begrenzt er nicht ausreichend, welche technischen Maßnahmen zur Umsetzung von Netzsperren eingesetzt werden dürfen. Besonders problematisch sind Verfahren wie **Deep Packet Inspection**, bei denen der Datenverkehr analysiert werden muss. Solche Maßnahmen greifen tief in die Vertraulichkeit der Kommunikation ein und begegnen erheblichen grundrechtlichen Bedenken.

Schließlich erscheint auch der Anwendungsbereich der Sperranordnungen überschießend. Insbesondere die Einbeziehung von **VPN-Diensten und Internet-Austauschknoten** überzeugt weder technisch noch grundrechtlich. Internet-Austauschknoten sind für die Umsetzung zielgerichteter Netzsperren gänzlich ungeeignet. VPN-Dienste sind ein wichtiges Instrument für Datenschutz und IT-Sicherheit. Darüber hinaus ermöglichen sie Menschen in Staaten mit umfassender Internetzensur den freien Zugang zu Informationen und leisten damit einen wichtigen Beitrag zur Meinungs- und Informationsfreiheit. **Die vorgeschlagenen Sperranordnung gegen VPNs lassen Anbietern keine andere Wahl, als das Kernversprechen ihres Produkts aufzugeben oder den Österreichischen Markt zu verlassen.**

1 https://www.parlament.gv.at/gegenstand/XXVIII/ME/125

Der Entwurf wird den besonderen grundrechtlichen Anforderungen an Netzsperren in seiner derzeitigen Ausgestaltung nicht gerecht. Die entsprechenden Bestimmungen sollten daher nicht beschlossen, sondern grundlegend überarbeitet werden.

Inhaltsverzeichnis

ALLGEMEINE ANMERKUNGEN

epicenter.works unterstützt das Ziel des Gesetzgebers, wirksame Maßnahmen gegen illegale Glücksspielangebote zu schaffen. Positiv hervorzuheben sind insbesondere jene Regelungen des Gesetzesentwurfs, die unmittelbar an den rechtswidrigen Angeboten oder deren wirtschaftlicher Grundlage ansetzen. Soweit der Gesetzesentwurf hingegen Sperranordnungen gegenüber Anbietern von Vermittlungsdiensten vorsieht, ergeben sich jedoch **erhebliche technische und grundrechtliche Probleme**. Anders als Maßnahmen, die unmittelbar gegen die für das rechtswidrige Angebot verantwortlichen Akteure gerichtet sind, setzen Sperranordnungen bei Dritten an, die Informationen im Internet übermitteln, speichern oder deren Auffindbarkeit ermöglichen. Ihre Ausgestaltung bedarf daher besonderer technischer und rechtlicher Sorgfalt.

Sperrverfügungen gegenüber Anbietern von Vermittlungsdiensten können insbesondere das **Grundrecht auf Datenschutz sowie die Meinungs- und Informationsfreiheit der Internetnutzer berühren.** Aufgrund dieser erheblichen Grundrechtsrelevanz unterliegen sie strengen Anforderungen des Verhältnismäßigkeitsgrundsatzes.

Die erhebliche Grundrechtsrelevanz von Sperrverfügungen spiegelt sich auch in der Rechtsprechung des Gerichtshofs der Europäischen Union wider, wie im Folgenden noch ausgeführt werden wird. Dieser hat sich bereits mehrfach mit den unionsrechtlichen Anforderungen an Sperranordnungen auseinandergesetzt und strenge Maßstäbe für deren Zulässigkeit entwickelt. Der vorliegende Gesetzesentwurf wirft aus Sicht von epicenter.works in mehreren Punkten die Frage auf, ob diesen Anforderungen ausreichend Rechnung getragen wird.

Ein wesentliches Risiko von Sperrverfügungen besteht im sogenannten Overblocking. **Darunter ist die Mitbetroffenheit rechtmäßiger Inhalte oder Dienste durch eine Sperrmaßnahme zu verstehen**. Dadurch können auch Internetangebote oder Kommunikationsvorgänge beeinträchtigt werden, die in keinem Zusammenhang mit den rechtswidrigen Glücksspielangeboten stehen. Die Vermeidung eines solchen Overblockings ist daher ein zentrales Kriterium für die Beurteilung der Verhältnismäßigkeit von Sperranordnungen.

SPERRVERFÜGUNGEN

Der Gesetzesentwurf sieht mit den §§ 56c und 56d Glückspielgesetz (GSpG) Sperrverfügungen gegenüber unterschiedlichen Kategorien von Anbietern von Vermittlungsdiensten vor. Während § 56c Sperrverfügungen gegenüber Anbietern von Hostingdiensten, Cachingdiensten und Online-Suchmaschinen vorsieht, richtet sich § 56d an Anbieter von Diensten der reinen Durchleitung. Nach den Erläuterungen umfasst dies insbesondere auch Internet-Austauschknoten, drahtlose Zugangspunkte, virtuelle private Netze (VPNs), DNS-Dienste und DNS-Resolver, Dienste von Namenregistern der Domäne oberster Stufe, Registrierungsstellen sowie Zertifizierungsstellen, die digitale Zertifikate ausstellen.

Im Mittelpunkt der nachfolgenden Ausführungen steht zunächst § 56d GSpG. Der weit gefasste persönliche Anwendungsbereich der Bestimmung sowie die sehr unterschiedlichen technischen Gegebenheiten der erfassten Anbieter von Diensten der reinen Durchleitung werfen erhebliche technische, datenschutzrechtliche und grundrechtliche Fragen auf. Auf die Besonderheiten des § 56c GSpG wird anschließend gesondert eingegangen.

Sperrverfügungen gegenüber Anbietern von Diensten der reinen Durchleitung (§ 56d GspG)

A. Zur Umsetzung von Sperrverfügungen

§ 56d Abs. 2 GSpG verpflichtet Anbieter von Diensten der reinen Durchleitung zur Umsetzung „*angemessener und technisch verfügbarer Maßnahmen*“, welche den Zugang zu verbotenen Ausspielungen verhindern oder erschweren. Nach den Erläuterungen liegt die Auswahl der sachgerechten und angemessenen technischen Maßnahmen im Ermessen der Telekom-Control-Kommission, die dabei auch die Verhältnismäßigkeit der gewählten Maßnahmen zu prüfen hat. Weder der Gesetzestext noch die Erläuterungen konkretisieren jedoch, welche technischen Maßnahmen diesen Anforderungen entsprechen.

Die Auswahl der Sperrmaßnahme ist jedoch nicht nur eine technische, sondern zugleich eine grundrechtliche Frage. Der Gerichtshof der Europäischen Union hat sich bereits mehrfach mit Sperranordnungen gegenüber Anbietern von Vermittlungsdiensten auseinandergesetzt und hervorgehoben, dass diese einen angemessenen Ausgleich zwischen den betroffenen Grundrechten gewährleisten müssen. Sperranordnungen müssen daher wirksam sein, dürfen jedoch nicht über das zur Erreichung ihres Ziels Erforderliche hinausgehen und keine unverhältnismäßigen Auswirkungen auf rechtmäßige Inhalte oder die Grundrechte der Internetnutzer entfalten.

Vor diesem Hintergrund ist zunächst zu untersuchen, welche technischen Maßnahmen Anbietern von Diensten der reinen Durchleitung überhaupt zur Verfügung stehen und ob diese den Anforderungen der Verhältnismäßigkeit entsprechen:

Domainsperren

Bei Domainsperren wird der Domainname eines Internetangebots durch DNS-Dienste oder Internetzugangsanbieter gesperrt oder auf eine Stoppseite umgeleitet.

Aus Sicht von epicenter.works stellen Domainsperren grundsätzlich die zielgerichtetste und zugleich grundrechtsschonendste Form der Umsetzung einer Sperranordnung dar.

IP-Adresssperren

Bei IP-Adresssperren werden einzelne Internet-Protokoll-Adressen gesperrt, über die Internetangebote erreichbar sind.

IPv4-Adressen stehen heute nur mehr in begrenzter Anzahl zur Verfügung und werden daher regelmäßig von einer Vielzahl unterschiedlicher Internetangebote gemeinsam genutzt. Die Sperre einer einzelnen IP-Adresse birgt somit ein erhebliches Risiko des sogenannten Overblockings, also der Mitbetroffenheit rechtmäßiger Inhalte oder Dienste durch eine Sperrmaßnahme. Es gab bereits Fälle von Netzsperren in Österreich, bei denen hunderttausende rechtmäßige Internetangebote, darunter auch ausländische Regierungsseiten, betroffen waren[2].

Der Gerichtshof der Europäischen Union verlangt in seiner Rechtsprechung, dass Sperranordnungen einen angemessenen Ausgleich zwischen den betroffenen Grundrechten gewährleisten[3]. Sperrmaßnahmen, die in erheblichem Umfang auch rechtmäßige Inhalte erfassen, begegnen daher erheblichen Bedenken im Hinblick auf den Grundsatz der Verhältnismäßigkeit. IP-Adresssperren erscheinen vor diesem Hintergrund regelmäßig nicht als angemessene Maßnahme im Sinne des § 56d GSpG.

URL- und SNI-/TLS-Sperren

URL- und SNI-/TLS-Sperren ermöglichen zwar eine zielgenauere Sperre einzelner Inhalte oder Angebote. Ihre Umsetzung setzt jedoch regelmäßig den Einsatz von Deep Packet Inspection (DPI) oder vergleichbaren Technologien voraus.

Zur Umsetzung derartiger Sperranordnungen müssten Anbieter von Diensten der reinen Durchleitung den Datenverkehr sämtlicher Nutzer analysieren, um jene Verbindungen zu identifizieren, die von einer Sperranordnung erfasst sind. Dies geht über die bloße Weiterleitung des Datenverkehrs hinaus und stellt einen erheblichen Eingriff in das Grundrecht auf Datenschutz dar.

Der Gerichtshof der Europäischen Union hat in der Rechtssache C70/10 *Scarlet Extended* klargestellt, dass ein Filtersystem, welches unterschiedslos die gesamte elektronische Kommunikation sämtlicher Nutzer überwacht, gegen das Unionsrecht verstößt. Derartige Maßnahmen führen zu einer allgemeinen Überwachungspflicht und gewährleisten keinen angemessenen Ausgleich zwischen dem Schutz geistiger Eigentumsrechte einerseits sowie dem Datenschutz, der unternehmerischen Freiheit und der Informationsfreiheit andererseits. Diese Grundsätze sind auf Sperranordnungen nach § 56d GSpG gleichermaßen zu berücksichtigen.

Aus Sicht von epicenter.works scheiden URL- und SNI-/TLS-Sperren, deren Umsetzung den Einsatz von Deep Packet Inspection oder vergleichbaren Überwachungstechnologien voraussetzt, daher regelmäßig als angemessene Maßnahmen im Sinne des § 56d GSpG aus.

Wir empfehlen daher eine gesetzliche Klarstellung, wonach nur solche Maßnahmen angeordnet werden dürfen, die von den Diensteanbietern tatsächlich wirksam und unter

2 https://www.derstandard.at/story/20001386619757/ueberzogene-netzsperre-sorgt-fuer-probleme-im-oesterreichischen-internet

3 Vgl etwa Rs UPC Telekabel C-314/12

Wahrung der Grundrechte umgesetzt werden können. Aus Sicht von epicenter.works kommen hierfür grundsätzlich lediglich Domainsperren in Betracht.

B. Zu den erfassten Anbietern

Wie dargestellt, setzt die Anordnung angemessener und technisch verfügbarer Sperrmaßnahmen voraus, dass die verpflichteten Anbieter von Diensten der reinen Durchleitung diese Maßnahmen technisch überhaupt umsetzen können. Gerade dies erscheint bei mehreren der nach den Erläuterungen von § 56d erfassten Anbieter zweifelhaft.

Nach den Erläuterungen soll § 56d neben klassischen Internetzugangsanbietern insbesondere auch Internet-Austauschknoten, drahtlose Zugangspunkte, virtuelle private Netze (VPNs), DNS-Dienste und DNS-Resolver, Dienste von Namenregistern der Domäne oberster Stufe, Registrierungsstellen sowie Zertifizierungsstellen, die digitale Zertifikate ausstellen, erfassen[4]. Diese Aufzählung orientiert sich an Erwägungsgrund 29 des Digital Services Act (DSA) und der Öffnungsklausel des Art. 4 Abs. 3 DSA.

Für zahlreiche der damit erfassten Anbieter erscheint eine Umsetzung von Sperrverfügungen jedoch technisch nicht oder nur unter Inkaufnahme erheblicher Grundrechtseingriffe möglich.

Virtuelle private Netze (VPNs)

VPN-Dienste dienen dazu, den Internetverkehr ihrer Nutzer verschlüsselt und grenzüberschreitend zu übertragen und deren Privatsphäre zu schützen. Viele Anbieter verfolgen bewusst ein datenschutzfreundliches Design und verzichten auf eine Protokollierung oder Lokalisierung ihrer Nutzer. Dadurch ist es ihnen regelmäßig nicht möglich festzustellen, ob sich eine Nutzerin oder ein Nutzer in Österreich befindet oder ob eine Sperranordnung überhaupt zur Anwendung gelangen müsste. Auch wenn eine Nutzerin oder ein Nutzer sich aus Österreich mit einem VPN Dienst verbindet, bedeutet dies nicht notweniger weise, dass sich die Person in Österreich befindet. Schließlich können auch mehrere VPN-Dienst hintereinander geschalten werden.

VPN-Dienste stellen darüber hinaus ein wesentliches Instrument zur Vermeidung staatlicher Internetzensur in Ländern wie Russland, Iran oder China dar. **Würden VPN-Anbieter verpflichtet, nationale Sperranordnungen technisch umzusetzen, bestünde die Gefahr, dass sie ihr Angebot für Nutzer in Österreich einschränken oder sich gänzlich vom österreichischen Markt zurückziehen, anstatt ihr datenschutzfreundliches Dienstekonzept grundlegend zu verändern**[5].

Internet-Austauschknoten (Internet Exchanges)

Auch für Internet-Austauschknoten erscheint die Umsetzung zielgerichteter Sperranordnungen technisch kaum praktikabel. Über diese zentralen Knoten fließt ein erheblicher Teil des Internetverkehrs zwischen den Netzen unterschiedlicher Betreiber. Eine granulare Sperre einzelner Internetangebote würde erhebliche technische Eingriffe und Rechenkapazitäten erfordern. Praktisch kämen vielfach lediglich IP-Adresssperren in Betracht. Wie bereits oben dargestellt, bergen diese jedoch ein erhebliches Risiko des Overblockings und erscheinen daher regelmäßig nicht als angemessene Maßnahme im Sinne des § 56d GSpG.

4 Siehe Seite 20 der Erläuterungen 125/ME XXVIII. GP - Ministerialentwurf

5 Vgl. etwa die Ankündigungen von Proton (Schweiz) und Signal (UK), sich aus einzelnen Märkten zurückzuziehen, sollten geplante Überwachungsgesetze im Bereich verschlüsselter Messenger umgesetzt werden.

> Der Gesetzesentwurf orientiert sich bei der Bestimmung der erfassten Anbieter an der Definition der Dienste der reinen Durchleitung in Art. 3 lit. g Z i DSA sowie den in Erwägungsgrund 29 genannten Beispielen[6]. Die Zulässigkeit eines solchen nationalen Anordnungsregimes ergibt sich dabei aus Art. 4 Abs. 3 DSA, der als unionsrechtliche Öffnungsklausel zu verstehen ist. Er erlaubt es den Mitgliedstaaten, gegenüber Anbietern reiner Durchleitungsdienste ein Anordnungsregime vorzusehen, ohne dass dies mit der harmonisierten Haftungsfreistellung in Konflikt gerät.
>
> Diese Öffnungsklausel verpflichtet die Mitgliedstaaten jedoch gerade nicht dazu, sämtliche in Erwägungsgrund 29 beispielhaft genannten Kategorien von Diensten der reinen Durchleitung tatsächlich in ein solches Regime einzubeziehen. Welche Anbieter erfasst werden, obliegt vielmehr dem nationalen Gesetzgeber. Dieser hat dabei insbesondere den Grundsatz der Verhältnismäßigkeit sowie die technische Umsetzbarkeit der angeordneten Maßnahmen zu berücksichtigen.

Vor diesem Hintergrund erscheint der persönliche Anwendungsbereich des § 56d GSpG überschießend. Aus Sicht von epicenter.works sollte er auf jene Anbieter von Vermittlungsdiensten beschränkt werden, bei denen angemessene und technisch verfügbare Maßnahmen im Sinne des § 56d tatsächlich umgesetzt werden können.

Sperrverfügungen gegenüber Anbietern von Hostingdiensten, Cachingdiensten und Online-Suchmaschinen (§ 56c GSpG)

§ 56c GSpG ermöglicht Sperrverfügungen gegenüber Anbietern von Hostingdiensten, Cachingdiensten und Online-Suchmaschinen. Besonders kritisch erscheint jedoch die Bestimmung, wonach Sperranordnungen unter bestimmten Voraussetzungen auch sonstige Leistungen eines Diensteanbieters erfassen können, wenn eine vollständig unterscheidbare und nach Angeboten getrennte Abwicklung technisch nicht möglich ist.

Konkret lautet es in 56c Abs 1 letzter Satz:

„Wenn ein Unternehmen über elektronische Medien neben verbotenen Ausspielungen (§ 2 Abs. 4), zur Teilnahme vom Inland aus, auch sonstige Leistungen in der Weise anbietet, die es den an der Herstellung eines Zuganges beteiligten Anbietern im Sinne des Abs. 1 nicht ermöglicht, diesen Zugang vollständig unterscheidbar und getrennt nach den Angeboten abzuwickeln, kann das Amt für Betrugsbekämpfung zudem anordnen, dass die Mitwirkung an der Herstellung eines Zuganges auch für die sonstigen Leistungen einzustellen ist.“

Anders als bei § 56d GSpG, wo ein **Overblocking** als Folge bestimmter technischer Sperrmaßnahmen eintreten kann, ermöglicht § 56c GSpG ausdrücklich die Sperrung rechtmäßiger Inhalte oder Dienste, sofern eine technische Trennung nicht möglich ist. Die Mitbetroffenheit rechtmäßiger Inhalte wird damit nicht lediglich als technische Folge einer Sperrmaßnahme in Kauf genommen, sondern durch die gesetzliche Ausgestaltung selbst ermöglicht.

Diese Regelung begegnet aus Sicht von epicenter.works **erheblichen unions- und grundrechtlichen Bedenken**. Art. 9 DSA sieht Anordnungen grundsätzlich in Bezug auf rechtswidrige Inhalte vor. Die **ausdrückliche Erstreckung einer Sperranordnung auf**

6 Siehe Seite 20 der Erläuterungen 125/ME XXVIII. GP - Ministerialentwurf

rechtmäßige Inhalte überschreitet diesen unionsrechtlichen Ansatz und wirft Fragen hinsichtlich ihrer Vereinbarkeit mit dem DSA auf.[7]

Darüber hinaus führt eine derart weitreichende Sperranordnung zu erheblichen Eingriffen in die Meinungs- und Informationsfreiheit. Der Europäische Gerichtshof für Menschenrechte hat in seiner Rechtsprechung zu Netzsperren wiederholt hervorgehoben, dass Sperrmaßnahmen, die als Nebeneffekt wahllos auch rechtmäßige Inhalte erfassen, einen schwerwiegenden Eingriff in die Meinungs- und Informationsfreiheit darstellen und nur unter engen Voraussetzungen mit Art. 10 EMRK vereinbar sind. Technische Schwierigkeiten bei der Trennung rechtmäßiger und rechtswidriger Inhalte können einen derart weitreichenden Grundrechtseingriff nicht rechtfertigen.[8]

Aus Sicht von epicenter.works sollte § 56c GSpG daher auf Sperranordnungen beschränkt werden, die sich ausschließlich auf rechtswidrige Inhalte beziehen. Soweit eine technisch getrennte Umsetzung im Einzelfall nicht möglich ist, darf dies nicht zu einer Ausweitung der Sperranordnung auf rechtmäßige Inhalte führen.

RECHTSSCHUTZ BETROFFENER INTERNETNUTZER

Wie bereits ausgeführt, können Sperrverfügungen, insbesondere infolge eines Overblockings, auch rechtmäßige Inhalte oder Dienste erfassen und dadurch die Meinungs- und Informationsfreiheit sowie den Zugang zu Informationen unbeteiligter Internetnutzer beeinträchtigen. Gerade aufgrund dieser erheblichen Grundrechtsrelevanz bedarf es eines wirksamen Rechtsschutzes auch für jene Personen, die von der Umsetzung einer Sperranordnung betroffen sind.

Der vorliegende Gesetzesentwurf sieht jedoch keine ausdrückliche Möglichkeit vor, dass betroffene Internetnutzer die Rechtmäßigkeit einer Sperranordnung oder ihrer konkreten Umsetzung überprüfen lassen können.

Der Gerichtshof der Europäischen Union hat sich in der Rechtssache C 314/12 *UPC Telekabel Wien* ausdrücklich mit dieser Frage auseinandergesetzt und den Rechtsschutz betroffener Internetnutzer als Voraussetzung für die unionsrechtliche Zulässigkeit von Sperranordnungen hervorgehoben:

„Damit die im Unionsrecht anerkannten Grundrechte dem Erlass einer Anordnung wie der im Ausgangsverfahren fraglichen nicht entgegenstehen, ist es deshalb erforderlich, dass die nationalen Verfahrensvorschriften die Möglichkeit für die Internetnutzer vorsehen, ihre Rechte vor Gericht geltend zu machen, sobald die vom Anbieter von Internetzugangsdiensten getroffenen Durchführungsmaßnahmen bekannt sind."[9]

Der Gerichtshof macht damit deutlich, dass ein wirksamer Rechtsschutz für betroffene Internetnutzer nicht bloß eine verfahrensrechtliche Ergänzung, sondern eine **wesentliche Voraussetzung für die unionsrechtliche Zulässigkeit von Sperranordnungen** darstellt. Zwar bezog sich diese Aussage auf das im Ausgangsverfahren maßgebliche zivilgerichtliche Verfahren. Der zugrunde liegende unionsrechtliche Grundsatz ist jedoch auf den vorliegenden Gesetzesentwurf gleichermaßen übertragbar. Auch Sperranordnungen nach §§ 56c und 56d GSpG können erhebliche Auswirkungen

7 Vgl MMR – Zeitschrift für das Recht der Digitalisierung, Digitalwirtschaft und IT | MMR 2025, 832 „Glücksspielrechtliche Sperranordnungen gegenüber Access-Provider" von Marc Liesching, HTWK Leipzig

8 Vgl https://verfassungsblog.de/dsa-netzsperren/

9 Rn 57, C 314/12 *UPC Telekabel Wien*

auf die Grundrechte von Internetnutzer entfalten und müssen daher von einem wirksamen Rechtsschutz begleitet werden.

Aus Sicht von epicenter.works sollte der Gesetzesentwurf daher ausdrücklich eine wirksames Rechtsmittel für von Sperranordnungen betroffene Internetnutzer vorsehen. Nur so kann sichergestellt werden, dass die unionsrechtlichen Anforderungen an Sperranordnungen sowie die effektive Wahrnehmung der Grundrechte der betroffenen Internetnutzer gewährleistet sind.

VERFAHRENSRECHTLICHE ASPEKTE

§ 56c GSpG sieht ein zweistufiges Verfahren vor. Zunächst teilt das Amt für Betrugsbekämpfung dem betroffenen Diensteanbieter die Anhaltspunkte für dessen Mitwirkung mit und räumt eine zwei Wochen nicht übersteigende Frist zur Stellungnahme sowie zur freiwilligen Einstellung der Mitwirkung ein. Erst wenn diese Frist ungenützt verstreicht, erlässt das Amt einen Bescheid, der dem Diensteanbieter die konkreten Maßnahmen aufträgt und dafür wiederum eine zwei Wochen nicht übersteigende Frist setzt.

§ 56d Abs. 2 GSpG sieht vor, dass die Telekom-Control-Kommission für die Umsetzung einer Sperrverfügung eine zwei Wochen nicht übersteigende Frist festsetzt. Darüber hinaus ermöglicht § 56d Abs. 6 GSpG unter bestimmten Voraussetzungen den Erlass einer Sperranordnung im Verfahren nach § 57 AVG mittels Mandatsbescheid. **Grundsätzlich begrüßen wir die Konstruktion der Sperrverfügung durch Einbindung der Telekom-Control-Kommission für Sperranordnungen gem 56d GSpg**. Dies schafft Rechtssicherheit für die Betreiber auch im Sinne der Netzneutralitätsvorgaben der Europäischen Union durch Verordnung (EU) 2015/2120 und bündelt die Kompetenzen in einer technisch versierten unabhängigen Behörde.

Vor dem Hintergrund der technischen Komplexität von Sperrverfügungen sowie ihrer erheblichen Auswirkungen auf die Grundrechte begegnen diese Verfahrensgestaltungen aus Sicht von epicenter.works Bedenken.

Bereits die Auswahl einer angemessenen und technisch verfügbaren Sperrmaßnahme erfordert eine sorgfältige technische und rechtliche Prüfung. Der verpflichtete Diensteanbieter muss beurteilen können, welche konkreten Maßnahmen technisch überhaupt umsetzbar sind, welche Auswirkungen diese auf andere Dienste und Nutzer haben und ob die angeordneten Maßnahmen den unions- und grundrechtlichen Anforderungen entsprechen. Gerade bei komplexen Vermittlungsdiensten können diese Fragen einen erheblichen technischen und organisatorischen Prüfungsaufwand erfordern.

Vor diesem Hintergrund erscheint eine Frist von höchstens zwei Wochen regelmäßig zu kurz bemessen. Sie birgt die Gefahr, dass Diensteanbieter zur Einhaltung der Frist vorsorglich weitergehende Sperrmaßnahmen ergreifen, als technisch oder rechtlich erforderlich wären. Dies könnte wiederum das Risiko eines Overblockings erhöhen und die Grundrechte betroffener Nutzer beeinträchtigen. Diese Problematik wird auch durch die sehr hohe Strafdrohung von 1 000 000 Euro verstärkt.

Besonders kritisch ist in diesem Zusammenhang die Möglichkeit, Sperrverfügungen gem 56d GSpG im Wege eines Mandatsbescheides nach § 57 AVG, daher **ohne vorangegangenem Ermittlungsverfahren, zu erlassen. Gerade bei technisch und grundrechtlich komplexen** Maßnahmen sollte den betroffenen Diensteanbietern grundsätzlich Gelegenheit gegeben werden, ihre technischen und rechtlichen Einwendungen bereits vor Erlassung einer Sperranordnung wirksam

vorzubringen. Ein effektives rechtliches Gehör ist wesentlicher Bestandteil eines fairen Verwaltungsverfahrens und gewinnt angesichts der erheblichen Grundrechtsrelevanz von Sperranordnungen besondere Bedeutung.

Aus Sicht von epicenter.works sollten die verfahrensrechtlichen Garantien des § 56d GSpG daher gestärkt werden. Dies betrifft insbesondere ausreichend bemessene Umsetzungsfristen sowie die effektive Wahrung des rechtlichen Gehörs der verpflichteten Diensteanbieter vor Erlassung einer Sperranordnung.