AKTUELLE RECHTSASPEKTE DES DNS

ANMERKUNGEN ZU 4 OB 44/22G, NIS2-RL, EIGENTÜMER-IDENTIFIKATION SOWIE SPERRVERFÜGUNGEN

Michael Sonntag

Assoz.-Prof. Johannes Kepler Universität Linz, Institute of Networks and Security
Altenbergerstr. 69, 4040 Linz, AT
michael.sonntag@ins.jku.at; https://www.ins.jku.at/

Schlagworte: ***DNS, Eigentümer-Identifikation, Sperrverfügung, Prüfpflicht***

Abstract: *Im letzten Jahr gab es einige neue rechtliche Entwicklungen in Bezug auf Domainnamen bzw das DNS-System. So wurde durch die Entscheidung des OGH vom 29.3.2022, 4 Ob 44/22g, eine Prüfpflicht von Domain-Registrierungsstellen „eingeführt" – analog zu Inhalten auf Webseiten, bei denen sich in den letzten Jahren eine reine Reaktionspflicht auf Meldungen zu einer gewissen Vorab-Prüfungspflicht zumindest nach Vorfällen hin änderte. Auch auf dem Gebiet der Sperren gibt es Neues – erstmals wurde nicht mehr nur ein bloßer ISP zu Domain-Sperren verpflichtet. Während Domaininhaber schon jetzt zumindest der Registrierungsstelle ihre Identität offenlegen müssen, wird dies mit der NIS2-RL explizit festgeschrieben – allerdings in weitgehend nutzloser Form.*

1. Anwendbarkeit der NIS2-RL auf DNS

Die NIS2-RL[1] betrifft auch DNS-Diensteanbieter. Das bedeutet, dass das Anbieten von Namensauflösung im Internet (sowohl autoritativen, d.h. das Hosten von Nameservern, wie auch rekursiven, d.h. die öffentlich verfügbare Auflösung von Domainnamen nach IP-Adressen für Endnutzer), Registrierungsdienste etc nun als wesentliche Einrichtungen gelten und damit den stärksten Regelungen unterliegen. Während dies für Registries, d.h. die Stellen, die Domainnamen unter einer/mehreren TLDs offiziell vergeben, wie z.B. die Nic.at offensichtlich wichtig und passend ist, scheint die Formulierung sehr weit zu gehen und auch Nameserver von Firmen zu umfassen: Die RL gilt für "DNS-Diensteanbieter"[2], diese sind jedoch (ua) als Anbieter von autoritativer Auflösungsdienste für die Nutzung durch Dritte (mit Ausnahme der Wurzel-Server[3]) definiert (Art 6 Z 20). Jeder autoritative Nameserver dient jedoch dazu, dass beliebige Dritte seine Domainnamen auflösen können, und fällt daher potentiell unter die Regelung. Lediglich rein firmeninterne Auflösung (rekursiv aber auch autoritativ, d.h. rein interne Domainnamen) wäre ausgeschlossen. Evtl ist dies daher so zu interpretieren, dass es sich nicht um technische Dienste handelt, sondern um eine wirtschaftliche Dienstleistung für Dritte, d.h. ein Angebot für Unternehmen, das im Betreiben eines autoritativen Nameservers für diese besteht. Dieser Interpretation widerspricht jedoch der Zusatz "ausgenommen die Wurzel Nameserver", da diese nicht als kommerzielle Dienstleistung für z.B. die dort eingetragenen Einzelstaaten betrieben werden. Die DNS-Server bei ISPs könnten herausfallen, da die (rekursive) Namensauflösung „öffentlich" erfolgen

[1] RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 333, 27.12.2022, S. 80; https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555.

[2] Anhang I Z 8.

[3] Diese sind zwar wichtig, können aber leicht zwischengespeichert werden und der Großteil dürfte sich ohnehin außerhalb der Jurisdiktion der EU befinden.

muss. Ein ISP kann diese jedoch technisch auf seine eigenen Kunden beschränken, was man – selbst bei großen Unternehmen – als nicht-öffentlich ansehen muss. Die Anwendbarkeit gilt sogar unabhängig von der Firmengröße (Art. 2 Abs. 2 lit a Z iii: TLD Registries und Anbieter von DNS Diensten aus Anhang I Z 8; iVm Art 3 Abs 1 lit b), sodass alle DNS-betreibenden Unternehmen betroffen sind. Als einzige Einschränkung verbleibt, ob der Dienst öffentlich für Endbenutzer angeboten wird oder rein für interne Nutzung dient (Art 6 Z 20 lit a), bzw ob der Dienst für Dritte erbracht wird (Art 6 Z 20 lit b), d.h. sie unter die Definition der RL fallen. Da dies für Firmen (sofern sie nicht anderweitig der NIS2-RL unterliegen) großen Aufwand bedeuten kann ist es empfehlenswert, den Betrieb von autoritativen Nameservern auf entsprechende Dienstleister zu übertragen – diese betreuen eine Vielzahl an Domains sodass es für sie leichter ist, die Anforderungen zu erfüllen und was auch vom Zweck der RL her sinnvoll ist.

2. Eigentümer-Identifikation

Zusätzlich müssen nach der NIS2-RL Domänennamen-Registrierungsdatenbanken nun mindestens folgende Angaben umfassen: Den Domänenname (technisch erforderlich und offensichtlich), das Datum der Registrierung (bereits jetzt indirekt erforderlich, da alle Domänennamen nur für begrenzte Zeit vergeben und dann erneuert werden müssen bzw frei werden), sowie Daten zum Inhaber: Name des Registrierenden, sowie dessen E-Mail Adresse und Telefonnummer (ist der Inhaber nicht identisch zum Verwalter, so sind auch dessen E-Mail Adresse und Telefonnummer zu speichern). Hierbei fällt auf, dass explizit nur das Datum der Registrierung gefordert ist und nicht der (exakte) Zeitpunkt, ebenso wenig wie sonstige Daten, z.B. die IP-Adresse von welcher aus die Registrierung erfolgte[4]. Aus Sicherheitsgründen ist dieses Datum daher weitgehend nutzlos. E-Mail Adresse und Telefonnummer sind nach den Endfassung nicht mehr nur zu erheben sondern auch zu verifizieren. Die hierfür verwendeten Methoden sollten (siehe ErwGr 111) den aktuellen Best-Practices der Industrie entsprechen und Fortschritte bei el. Identifikation soweit möglich berücksichtigen. Für Firmen innerhalb der EU könnte dies einen Zwang bedeuten, eine el. Identifikation (→ eID) zu verlangen – oder entsprechend starke alternative Nachweise. Die Qualität wird potentiell dadurch reduziert, dass es sich hierbei auch um ex-post Validierungen handeln kann. Eine Einschränkung hierbei auf existierende Domainnamen erfolgt nicht, sodass dies auch bei Neuregistrierungen anwendbar ist. Zumindest eine Kontaktmöglichkeit soll auch verifiziert werden; in der Praxis dürfte dies meistens die E-Mail Adresse sein, die daher zumindest zum Registrierungszeitpunkt funktional sein muss. Die eingesetzten Identitätsprüfungsverfahren sind öffentlich zu machen. Es wird keine Aktualisierungspflicht festgelegt, bzw dass eine solche mit dem Registrierungsvertrag auf den Inhaber zu übertragen ist[5]. Aus der Pflicht (Art 28 Abs 3), über entsprechende Vorgaben und Verfahren für genaue und vollständige Angaben zu verfügen (und diese wohl auch einzusetzen), kann mM eine Aktualisierungspflicht nicht herausgelesen werden: das Verfahren kann sich auch bloß auf den Registrierungsvorgang beziehen, insb da vielfach Reseller eingebunden sind und die Registrierungsstelle daher uU nie direkten Kontakt zum Inhaber hat. Lediglich Art 28 Abs 1 spricht vom „sammeln und pflegen" der Daten, woraus sich zumindest bei Bekanntwerden von Fehlern (z.B. Unzustellbarkeit einer E-Mail) eine Korrekturpflicht herauslesen lässt.

Während die genaue Identifikation des Inhabers einer Domäne sinnvoll erscheint (z.B. um eine Rechtsverfolgung zu ermöglichen), ist es die Begründung hierfür nicht: Mit Sicherheit hat dies nichts zu tun, da falsche Angaben z.B. ohne weiteres möglich sind, ebenso wie Strohmänner oder Firmen ohne Rückverfolgbarkeit des Eigentümers bzw nur kurzfristige genutzte anonyme E-Mail Adressen/Telefonnummern. Auch ist der bloße Name alleine für sich in sehr vielen Fällen keine eindeutige Identifikation. Denn für die meisten TLD be-

[4] Wird ein Domänenname schon kurz nach der Registrierung "missbraucht" könnten bei ISPs noch Daten über den zugeordneten Anschluss vorhanden sein.

[5] Was zumindest sehr viele Registrierungsstellen jedoch bereits tun: Die E-Mail Adresse muss funktional sein und ist daher zu aktualisieren; der Inhaber muss darunter erreichbar sein (eine Antwortpflicht besteht jedoch nicht!).

stehen keine Einschränkungen der Inhaber – jede Person/Firma weltweit kann eine Domäne registrieren und Firmen-Registrierungsnummer, Adresse, Ausweisnummer, Geburtsdatum oÄ sind alle (zumindest nicht nach der NIS2-RL, evtl jedoch aufgrund von Regeln der TLD bzw des Registrars) nicht erforderlich.

Aus der Veröffentlichungspflicht für Nicht-Personenbezogene Daten (Art 28 Abs 4) ergibt sich nur, dass "geheime" Domainregistrierungen, d.h. Verkauf ohne Eintragung, also effektiv eine Registrierungssperre für Dritte ohne tatsächliche Nutzung, nicht erlaubt sind. Meines Wissens nach war dies nie irgendwo möglich. Für Firmen könnte dies uU von Interesse sein, z.B. um Domainnamen vorsorglich zu registrieren, die erst später zusammen mit einem neuen Produkt öffentlich gemacht werden. Auch bei z.B. Marken besteht dieses Problem, doch kann dort durch gezielte Verzögerung des Anmeldeverfahrens (bzw dessen natürliche Dauer) zumindest ein gewisser zeitlicher Spielraum geschaffen werden. Bei Domainnamen ist dies aufgrund der Automatisierung hingegen unmöglich, doch kann mittels Treuhändern oder Anmeldung über Dritte und rechtzeitigen Erwerb von diesen zumindest die Verbindung zum Unternehmen verschleiert werden. Denn erforderlich ist nur, dass der im Augenblick tatsächliche Rechtsinhaber mit korrekten Daten angeführt wird; wirtschaftliche Berechtigte bzw Domainübertragungen werden durch die Regelung nicht beeinträchtigt.

3. Sperrverfügungen

Abgesehen von kürzlichen Problemen bei Sperrverfügungen durch die Sperre von IP-Adressen anstelle von Domainnamen und daraus resultierendem Overblocking[6] wurde – soweit bekannt – erstmals eine Sperre bei einem der großen DNS-Anbieter (anstatt bei den Endbenutzer-ISPs) erreicht: Der Musikverband IFPI[7] zwang Cloudflare (mit seinem weltweit nutzbaren und genutzten Nameserver 1.1.1.1) über ein Mailänder Gericht[8] zu einer Sperre von Domainnamen von Torrent-Websites. Dies bedeutet, dass die triviale Möglichkeit, DNS-Sperren zu umgehen indem ein anderer DNS-Server eingesetzt wird, schwieriger wird. Real kann ein solcher DNS-Auflösungsdienst auch ohne großen Aufwand[9] selbst betrieben werden, sodass jegliche Zensurmaßnahmen umgangen werden. Doch könnten dies (derzeit) die ISP relativ leicht und nebenwirkungsfrei unterbinden, indem Port 53 gesperrt wird. Meiner Meinung nach wäre eine solche Sperre jedoch unzulässig, da grundsätzlich jeder Datenverkehr einer bestimmten Art (=DNS) unterbunden wird; über eine spezielle Vertragsgestaltung könnte dies evtl möglich sein (eben um Sperren effektiv durchsetzen zu können). Doch mit dem Aufkommen von DoH[10] (DNS over HTTPS) wird dies wieder schwieriger werden: Die Auflösung erfolgt über verschlüsselte Web-Verbindungen und ist damit nur mehr äußerst schwer vom normalem Websurfen zu unterscheiden. Allerdings benötigt DoH (anders als ein "klassischer" eigener DNS-Server) zumindest derzeit[11] einen "Upstream-Server", z.B. wie den von Cloudflare. Es ergibt sich daher bei der Sperr-Umgehung bis auf weiteres ein Problem: Derzeit mögliche Umgehungs-Ansätze sind nicht sehr komplex, könnten aber (technisch!) einfach verhindert werden. Technisch nur schwer verhinderbare Umgehungsstrategien erfordern hingegen einen externen "Dienstleister" – bei welchen neuerdings eine Sperre möglich ist.

---

6 Proschofsky, Überzogene Netzsperre sorgt für Probleme im österreichischen Internet, 29.8.2022, https://www.derstandard.at/story/2000138619757/ueberzogene-netzsperre-sorgt-fuer-probleme-im-oesterreichischen-internet.

7 IFPI, Record companies in Italy take successful action against CloudFlare, 18.7.2022, https://www.ifpi.org/record-companies-in-italy-take-successful-action-against-cloudflare/.

8 Dobiraj, IFPI zwingt DNS-Server von Cloudflare zu Sperren, 22.7.2022, https://tarnkappe.info/artikel/rechtssachen/ifpi-zwingt-dns-server-von-cloudflare-zu-sperren-248064.html.

9 Einfach und ohne Zusatzkosten z.B. auf einem PC für Personen mit IT-Grundkenntnissen – für normale Endnutzer bzw bei Mobilgeräten etc ist dies dennoch derzeit nicht tauglich.

10 Chrome, Edge und Firefox unterstützen dies bereits, zumindest in experimenteller Weise, d.h. nicht als Standardeinstellung.

11 Root Server Operators: Statement on DNS Encryption, March 2021, https://root-servers.org/media/news/Statement_on_DNS_Encryption.pdf.

Ob die Sperre weltweit durchzuführen ist, geht aus den Mitteilungen leider nicht hervor. Aufgrund der technischen Umsetzung des DNS wäre eine räumliche Einschränkung ungefähr auf Italien möglich[12]. Dies ähnelt dem Urteil EuGH 3.10.2019, C-18/18 (Glawischnig vs Facebook), in dem eine internationale Löschung (dort von Inhalten) als prinzipiell möglich festgestellt wurde, wobei die Mitgliedsstaaten dafür sorgen müssen, dass die internationalen Regeln gebührend berücksichtigt werden (Rz. 51, 52). Im Gegensatz zur Inhaltssperre ist bei DNS jedoch eine zumindest regionale Einschränkung tatsächlich und ohne größeren Aufwand möglich, ohne damit andere Gebiete zu beeinträchtigen. Dies erscheint auch sehr wichtig, da ansonsten jedes Land beliebig Domains weltweit sperren könnte, z.B. irgendein Land die Wikipedia wegen unerwünschter Inhalte.

Zu berücksichtigen ist weiters, dass die Root-Nameserver ebenfalls potentiell als Adressaten in Frage kommen: Auch diese lösen Domainnamen für Dritte auf, ähnlich wie Cloudflare. Allerdings betreffen diese theoretisch nur TLDs; Sperren wären daher nur auf diesem Niveau möglich. Doch man muss berücksichtigen, dass sie – eben auch für die Namensauflösung von "darunter" befindlichen Domainnamen – erforderlich sind und technisch gesehen an der Auflösung z.B. der Torrent-Websites mitwirken[13]. Es bleibt also den Gerichten überlassen zu entscheiden, ob die Blockade einer gesamten TLD angemessen bzw erforderlich ist. So könnten z.B. die TLDs ".sex" oder ".gay" ohne weiteres Ziele von konservativen Staaten werden, welche Sperranordnungen erlassen könnten. Auch hier wäre jedoch uU eine regionale Einschränkung technisch möglich.

Der Zugang zu illegalen Inhalten kann daher effektiver behindert werden. Praktisch könnte zwar das Problem auftreten, dass der Betreiber eines solchen Dienstes eine Gerichtsentscheidung einfach ignoriert. Mangels Niederlassung bzw Geschäftstätigkeit in diesem Land wäre eine Durchsetzung dann vielfach unmöglich. Zumindest für die großen und bekannten DNS-Anbieter und die EU dürfte dies jedoch auszuschließen sein. Dem steht gegenüber, dass ein DNS-Server auch mit schwacher Hardware eine hohe Anzahl an Nutzern versorgen kann, d.h. ein weltweiter Betrieb durch einen kleinen Verein erscheint durchaus möglich. Dieser könnte dann (DoH, daher nicht über den Port blockierbar!) nur über IP-Adressen (potentiell mit dem Problem des Overblockings, siehe oben) gesperrt werden.

4. Prüfpflicht bei der Domain-Registrierung?

In der Entscheidung 4 Ob 44/22g vom 29.3.2022[14] entschied der OGH, dass es zwar an sich (siehe schon OGH 13.9.2000, 4 Ob 166/00s – fpoe.at) keine allgemeine Prüfpflicht bei einer Domainnamens-Registrierung gibt, dass aber bei bereits bestehenden aktuellen "Problemen", d.h. nach (im konkreten Fall mehrfachen) begründeten und erfolgreichen Beschwerden, eine spezifische Prüfpflicht möglich ist.

Im hier besprochenen Fall wurden Domainnamen registriert, die dem (auch Domain-)Namen einer österreichischen Rechtsanwaltskanzlei ähnelten, um mit diesen per E-Mail Betrugsversuche durchzuführen (z.B. indem bei Banken mittels der E-Mail Adresse die Verfügungsberechtigung über ein Konto „nachgewiesen" wird). Konkret handelt es sich z.B. um at-bindergrosswang.com, at-binder-groesswang.com, bindergrosswang.com, binder-groesswang-at.com. Diese Betrugsversuche wurden der Kanzlei bezüglich einer ersten Domäne jedoch bekannt, worauf diese eine Löschung des Domainnamens forderte, welche auch durchgeführt wurde. Kurz darauf wurde jedoch eine weitere Domain der obigen Beispiels-Liste registriert und ein neuer Betrugs-

[12] Cloudflare betreibt als Haupt-Dienst „Server vor Ort". Zusammen mit der Technologie Anycast (welche z.B. bei den Root-Servern des DNS eingesetzt wird), könnten nur Anfragen aus Italien (bzw umliegenden Gebieten) zu anderen Daten geleitet werden. Cloudflare verwendet diese Technologie mit Standpunkten in 275 Städten bereits für DNS (https://www.cloudflare.com/de-de/learning/dns/what-is-anycast-dns/). Das Problem ist, das immer der „nächste und am besten verfügbare" Server antwortet – was sich nicht nach Landesgrenzen sondern den Netzwerkverbindungen richtet und sich durch Belastung auch ändert. Eine Gebietsfestlegung schadet daher der Resilienz und ist uU nicht trennscharf möglich.

[13] Je nach eingesetzter Software am Client erfahren sie uU nur die TLD (Einsatz von QNAME Minimization), oder den gesamten Domainnamen (beantworten aber dennoch nur im Hinblick auf die TLD). Im zweiteren Fall wären daher Sperrverfügungen sogar unmittelbar wirksam, wären aber technisch eine uU schwere Belastung für die Server.

[14] Siehe auch JusGuide 2022/22/20240 (OGH).

versuch erfolgte. Trotz jeweils unmittelbarem Hinweis (und Löschung des jeweiligen Domainnamens; nur ein Mal verspätet[15]), erfolgte dies mehrfach (sieben Versuche!). Auch Auskunft über den Domaininhaber wurde begehrt, welcher jedoch erst mit der Klagebeantwortung entsprochen wurde.[16] Relevant ist hier, dass schon beim zweiten Löschungsbegehren zusätzlich verlangt wurde, die Registrierung von allen weiteren Domains, welche die Namen „Binder" und „Grösswang" (oder „Groesswang" oder „Grosswang") beinhalten, und/oder ähnlichen Domains, zu unterlassen.[17]

Der OGH entschied, dass es sich bei der Vergabestelle nicht um den unmittelbaren Täter handelt und keine allgemeine Prüfpflicht besteht – was nicht weiter überrascht und der bisherigen Rechtsprechung entspricht. Neu ist die Entscheidung, dass eine Vergabestelle verpflichtet ist, Maßnahmen zur Verhinderung einer Fortsetzung der Rechtsverletzung, selbst bei Neuregistrierung anderer Domains, vorzunehmen – bzw sie ansonsten zur Unterlassung verurteilt werden kann. Dies erfolgt insb unter Berufung darauf, dass im Fall fpoe.at nur eine händische Prüfung möglich war und eine derartige Prüfung aufgrund der technischen Gegebenheiten damals automatisiert nicht möglich war.

Diese Aussage ist jedoch problematisch: Bereits im Jahr 2000 war es einem IT-Unternehmen problemlos möglich, alle zu „FPÖ" ähnlichen Namen vollautomatisch zu identifizieren. Dass dies bei den Worten „Binder" und „Grösswang" unterschiedlich sein soll, kann durch die zwischenzeitliche Weiterentwicklung der Informatik nicht begründet werden: Beides ist gleich trivial – und auch beide enthalten den für Domainnamen potentiell problematischen identischen Umlaut! Die Entscheidung erwähnt es nebenbei, aber die Begründung sollte mMn hauptsächlich auf das konkrete Unterlassungsbegehren gestützt werden, da hier ein sehr realer Unterschied besteht: In der Entscheidung fpoe.at wurde eine Unterlassung bezüglich „das Namensrecht der Klägerin verletzenden Domains" verlangt, während in diesem Verfahren ein Verbot bezüglich der Kombination zweier konkreter Worte (mit zwei Alternativen bzw geringen Abwandlungen bei einem) begehrt wurde.[18] Im Gegensatz zu einer beliebig gearteten Verletzung des Namensrechts ist (und war) dieses neuere Verlangen durch Software problemlos beurteilbar. Es kann ein Vergleich der konkreten Namen bzw des „Abstands" zu diesen (hierfür existieren schon sehr lange eine Vielzahl an Algorithmen) vorgenommen werden, wonach ggf noch eine manuelle Nachprüfung notwendig ist. Demgegenüber kann das Namensrecht in sehr unterschiedlicher Art verletzt werden: ähnlich aussehende/klingende Namen, verwechselbare Schreibweise, Verwendung des vollen Namens oder der Abkürzung, Verbindung mit abwertenden Begriffen etc.[19] Dies alles auch nur annähernd korrekt und vollständig (!) in einem Programm abzubilden dürfte auch heute noch äußerst schwer sein. Hierfür spricht auch, dass das Berufungsgericht (das bereits identisch zum OGH entschied), aus dem Unterlassungsbegehren den Teil „und/oder ähnliche Domains" strich (vom OGH nicht explizit bestätigt, da dies nur für den Einzelfall Bedeutung besitzt; ein Verbot „ähnlicher" Verletzungen ist jedoch prinzipiell

[15] In einem Fall nur mit fünf Tagen Verzögerung und auf erneute Aufforderung; dies war jedoch nicht Gegenstand des Verfahrens und ist jedenfalls problematisch, da unverzügliche Prüfung und Reaktion erforderlich sind.

[16] Auch dies war nicht (mehr?) Teil des Verfahrens und ist jedenfalls problematisch: Wird der Domainname wegen auch für juristische Laien offensichtlicher Rechtswidrigkeit gelöscht, ist eine Auskunft über den Domaininhaber zu erteilen, da hier das Rechtsverfolgungsinteresse eindeutig das Recht des Inhabers auf Datenschutz übersteigt.

[17] Laut Urteil "absolut", d.h. nicht nur solche, welche das Namensrecht der Klägerin verletzen; dies erscheint pot problematisch (siehe unten); siehe Rz. 57.

[18] Oder wie Tipotsch, Haftung des Domain-Registrars für Verletzungen des Namensrechts, MR 2022, 177 es formuliert: [...] jedoch auf die Prüfung und Sperre weiterer Eintragungen, die *offenkundig in gleicher Weise* das Namensrecht des Verletzten missachten [...] (Hervorhebung durch Verf dieses Artikels, d.h. nicht in jeder beliebigen Art verletzend).

[19] Siehe schon Thiele, Anm zu 4 Ob 44/22g – bindergrosswang, ZIIR 2022, 309–317.

möglich[20]). Verboten ist daher ausschließlich die Registrierung von Domains die sowohl „Binder“ als auch „Grösswang“/“Groesswang“/“Grosswang“ enthalten.[21]

Auch wenn der OGH explizit betont, dass die „Zumutbarkeit“ nicht im Unterlassungsverfahren zu prüfen ist, sondern erst im Falle einer Exekution deren ausnahmsweises Fehlen relevant ist, muss man diese mMn schon hier berücksichtigen: Denn mit dem Verweis auf die technischen Möglichkeiten wird genau auf die Zumutbarkeit abgestellt (denn eine rein manuelle Prüfung ist – abgesehen vom Aufwand – jedenfalls möglich). Weiters schreibt der OGH explizit: „Hingegen kann der Vergabestelle (auch in Anlehnung an die zu verneinende Haftung von Presseunternehmen für wettbewerbswidrige Anzeigen) eine allgemeine Prüfungspflicht nicht zugemutet werden.“ sowie „Der Vergabestelle ist demnach eine derartige allgemeine Prüfung nicht zumutbar.“ Es wird also gerade doch geprüft, ob eine Prüfung an sich überhaupt irgendwie möglich ist, und wenn ja, ob dies vom Aufwand her zumutbar ist. Dies muss gleichfalls für eine nachgelagerte Prüfpflicht gelten, welche einen deutlich größeren Aufwand als eine einmalige Vorprüfung bedeutet, da anstatt eines Domainnamens potentiell tausende (=jeder neu angemeldete) zu prüfen sind.

Die vom Berufungsgericht angeführten Zumutbarkeits-Gründe erscheinen hingegen äußerst problematisch:

– Anmelder ist eine natürliche Person mit Adresse in Frankreich: Warum dies bei Registrierung einer „.com“ Domäne ein auffallender Hinweis auf einen Missbrauch darstellen soll, ist nicht ersichtlich. Im Gegensatz hierzu führt der OGH weiter oben aus, dass die Domainnamen von verschiedenen Personen mit Sitz in Frankreich[22] angemeldet wurden – dies kann daher noch weniger ein Hinweis auf Missbrauch sein. Auch der Wohnort (=Frankreich) erscheint für eine .com -Domäne nicht per se verdächtig.
– Keinerlei Bezug zu dem angemeldeten Namen: Sehr viele Firmen besitzen Marken, welche völlig unabhängig von ihrem Firmennamen sind. Auch Einzelpersonen können Domainnamen registrieren, welche sich von ihrem (Familien-)Namen unterscheiden ohne dass dies per se problematisch ist. Auch heute ist das Bestehen (oder gar der Nachweis) irgendeines Rechts nicht Voraussetzung dafür, einen Domainnamen registrieren zu dürfen.
– Keinerlei Bezug zu der at-Kennung: Die Domainnamen enthalten z.B. „-at“, dies ist jedoch nicht ungewöhnlich, wenn z.B. der derselbe Name unter „.at“ bereits vergeben ist. Weiters muss dies keineswegs auf ein Land hinweisen sondern kann auch diverse andere Bedeutungen besitzen.[23]
– Die Namenskombination ist außergewöhnlich: Es handelt sich um einen Doppelnamen, welche heute weit verbreitet sind. Und während „Grösswang“ ein eher seltener Name ist (jedoch auch bereits in Österreich mehrfach vorkommt), kann dies von „Binder“ nicht gesagt werden. Bei „Außergewöhnlichkeit“ ist, insbesondere aufgrund der Internationalität des Internets, außerordentlich hohe Vorsicht angebracht.[24] Für den konkreten Fall muss auch angemerkt werden, dass z.B. “binder” (→ Domainnamen kennen keine Groß-/Kleinschreibung) im Englischen (→ .com) ein Produkt bezeichnet (Bindemittel, Mappe, Ordner...), sodass es sich um einen Firmen-/Personennamen in Verbindung mit einem Produkt handeln könnte (vgl “blumen-heidi.at”).
– Die Namenskombination hat nichts mit Waren oder Dienstleistungen zu tun: Es gibt sehr viele Domainnamen unter denen weder Waren noch Dienstleistungen angeboten werden, z.B. rein private Websites.

[20] Siehe auch Horak, Unterlassungspflicht der Domain-Vergabestelle, ecolex 2022/379, der speziell hervorhebt, dass eine umso leichtere technische Umsetzbarkeit die Erlassung eines Titels wahrscheinlicher macht. Dies bedeutet jedoch gerade, dass die Zumutbarkeit (zumindest in der Realität, wenn auch nicht in der rechtlichen Begründung) schon bei der Entscheidung einfließt, und nicht erst im Impugnationsverfahren!

[21] Dies bedeutet durchaus noch eine große Anzahl an betroffenen Domains, da z.B. sowohl Binde- als auch Unterstrich zur Verbindung eingesetzt werden können (oder zusammen geschrieben), die Reihenfolge offen ist, und auch weitere beliebige Zusätze keine Erlaubnis begründen. Das Verbot schließt daher nicht alle pot. Verletzungsmöglichkeiten aus, ist aber keineswegs nutzlos.

[22] Rz. 23.

[23] Im konkreten Fall z.B. als Englisches “at” iS einer Ortsbezeichnung des folgenden Teils, z.B. „miller-at-vienna.com“.

[24] Vergleiche: Könnte die Nic.at ebenso problemlos beurteilen, wie ausgefallen ein französischer (Doppel-)Name wäre?

Dies ist auch kein Erfordernis für eine Registrierung. Siehe auch den vorigen Punkt – Englisch kann bei ".com" Domains keinesfalls ausgeschlossen werden.

Als problematische Aspekte, bzw Ansatzpunkte für die automatisierte Prüfung, sollten vielmehr folgende(r) Punkt(e) angesehen werden:

– Gab es schon Beschwerden zu diesem oder einem ähnlichen Domainnamen? Identität ist trivial, aber mittels diverser Algorithmen können auch bestimmte Abwandlungen (Vertipper, phonetisch ähnlich etc) erkannt werden: ist einmal ein bestimmtes Muster bekannt (z.B. Anhängen von „-" und einem Landeskürzel), kann es leicht hinzugefügt werden. Dies wäre auch problemlos individuell für jeden Einzelfall einstellbar, d.h. welche Regeln hier anzuwenden sind.[25] Genau dies ist, was kommerzielle Beobachtungsdienste, wie sie im Urteil angesprochen werden, durchführen.[26]

Erkennbar ist diese Liste sehr kurz, aber weitere Maßnahmen sind nicht ersichtlich bzw wie oben diskutiert problematisch. So könnten etwa geprüft werden, ob es bezüglich des konkreten Anmelders bereits in der (jüngeren) Vergangenheit Beschwerden gab. Dh unabhängig vom Domainnamen könnten Registrierungen von „Wiederholungstätern" verdächtig sein. Dies ist im Prinzip zwar richtig, doch fehlt hier ein konkretes Vergleichsobjekt. Dies würde meiner Meinung nach einer generellen Prüfpflicht entsprechen (da der gewünschte Domainname umfassend, z.B. mit allen Marken weltweit, zu prüfen wäre), welche der OGH weiterhin korrekt ablehnt.[27]

Vergabestellen werden daher in Zukunft nicht umhin kommen, „Negativlisten" zu führen, um automatisiert festzustellen, ob es sich bei einer Neuregistrierung um einen schon einmal (bzw ähnlich zu solchem) beanstandeten Domainnamen handelt. Diese werden anschließend händisch geprüft werden müssen.[28] Weiters könnte z.B. im konkreten Fall jemand mit dem Familiennamen oder einer im Ausland registrierten Marke „Binder-Grösswang" problemlos und legal „binder-groesswang.com" registrieren. Dies stellt jedoch bei der Marke schon das erste praktische Problem dar: Ohne Rücksprache mit dem Anmelder (= Nachforschung!) wird dies auch durch manuelle Prüfung nicht feststellbar sein. Denn der OGH legt als Maßstab auch hier „für einen juristischen Laien ohne weitere Nachforschungen offenkundig" an. Dies bedeutet, dass entweder ein „Begründungsfeld" einzuführen ist (wo problemlos gelogen werden kann – keine Nachforschungen – daher nur bei einem späteren Verfahren z.B. wegen Schadenersatz oder bei der Bearbeitung einer Beschwerde relevant; reine Plausibilitätsprüfung ob die Angaben eine Registrierung stützen könnten), eine tatsächliche individuelle Prüfung mit Nachfragen und z.B. Dokumentenvorlage erfolgen muss, oder solche Domains grundsätzlich abzulehnen sind (unabhängig von einer etwaigen legalen Nutzung durch den Registrierungswerber; siehe oben!). Eine konkrete Lösung hierfür ist nicht ersichtlich, aber alle drei Varianten sind mMn mit dem Urteil vereinbar.

„Vergabestellen" sind in diesem Zusammenhang nicht nur die eigentliche Registrierungsstelle/Registry (=Organisation welche einen Vertrag mit der ICANN besitzt), sondern eben – wie im diskutierten Fall – auch Wiederverkäufer/Vergabestellen/Registrare, d.h. bloße Reseller. Denn es ist nicht erkennbar, warum zwar ein Zwischenhändler zu einer Prüfung verpflichtet sein sollte, nicht aber die ausgebende Stelle. Wichtig ist hier jedoch die „Beschwerdestelle": Eine Prüfpflicht kann nur den treffen, bei dem zuvor eine Beschwerde erfolg-

[25] Über eine Prüfung aller bereits existierenden Domainnamen könnte sogar eine Abschätzung der Fehlalarme durchgeführt werden. Dies ist jedoch pot rechtlich problematisch, da ein solcher Test als „Kenntnis" ausgelegt werden könnte und eine händische Nachprüfung bereits existierender und auf die Regel passender Domainnamen erfordern könnte – uU sehr viel Aufwand und zusätzliche Probleme (Löschung von Domainnamen, über welche keine Beschwerde erfolgte? Information des sich Beschwerenden über evtl weitere Problemfälle? ...).

[26] Da solche Dienste gegen Entgelt typ von Registrierungsstellen angeboten werden, könnte dieses Geschäft stark beeinträchtigt werden. Allerdings bieten sie weiterhin den Vorteil, nicht nur Anmeldungen bei genau dieser einen Registrierungsstelle zu prüfen, sondern weltweit sowie unter allen TLDs. Sie bleiben daher weiterhin als Geschäftszweig erhalten.

[27] Im konkreten Fall ebenso wie generell vermutlich ohnehin wenig zielführend, da einfach verschiedene Personen, z.B. auch Strohmänner (sofern überhaupt eine echte Identitätsprüfung erfolgt; siehe oben zur NIS2-RL), hierfür eingesetzt werden können.

[28] So könnte z.B. der sich Beschwerende weitere pot gefährliche Domainnamen vorbeugend/als Ergänzung registrieren.

te. Da es zu einer Registry viele Registrare geben kann (und meistens auch gibt), ist es daher praktisch sinnvoll, sich mit Beschwerden direkt an die Registry zu wenden: Diese kann eine Anmeldung für alle Registrare weltweit zuverlässig verhindern. Nachteilig kann jedoch deren Sitzort sein: Ist dieses Unternehmen an ein entsprechendes Urteil gebunden, falls sie die Sperre nicht durchführt, bzw wo und nach welchem Recht wäre ein solches Verfahren durchzuführen? Bei der Streitgegenständlichen TLD ".com" wäre dies z.B. Verisign in Virgina, USA, was im Vergleich zur Vergabestelle des Verfahrens in Frankreich Probleme aufwerfen würde.

Ein derartiges Verbot könnte sogar missbraucht werden, da z.B. auch „negative" Domainnamen wie „binder-groesswang-sind-schlechte-anwaelte.com" vom Verbot umfasst wären, sodass der Inhaber selbst eine Registrierung und darauf folgende Beschwerde und folgerichtig Sperre provozieren könnte, um vor derartigen kritischen Domänen geschützt zu sein (absolut, da keine Ausnahme vorgesehen und ohne dass er selbst die Domäne registrieren muss!). Bei der Formulierung der Unterlassungsverpflichtung sollte daher mMn darauf Bedacht genommen werden, nur (auch für juristische Laien offensichtlich) *unberechtigte* Registrierungen zu verhindern, nicht jedoch alle. Ein vollständiges Verbot ohne Ausnahme für legitime Registrierungen Dritter sollte daher nicht erlassen werden.

Weiters können sich im Laufe der Zeit große Mengen an Beschwerden ansammeln: Eine zeitliche Begrenzung ist daher erforderlich. Eine solche wird vom Berufungsgericht auch erwähnt und mit „eine Zeitlang, zumindest aber ca zwei Monate" angegeben. Diese Frist erscheint sinnvoll und praxistauglich und kann problemlos automatisiert werden.

Das Ergebnis des OGH führt daher gerade entweder zu einer – vom ihm explizit abgelehnten – individuellen Detail-Vorprüfungspflicht zumindest in Fällen, wo kurz vorher Probleme auftraten, oder zu einer generellen Einschränkung auch legaler Registrierungs-Möglichkeiten. Weiters bestehen selbst bei absolut eindeutig erscheinenden und unter das Verbot fallenden Namen (z.B. „binder-groesswang.com") durchaus legale Möglichkeiten der Registrierung in vielen Ländern der Welt, welche durch das OGH-Urteil effektiv abgeschnitten werden.

Darüber hinaus stellt sich uU ein großes praktisches Problem: eine Österreichische (bzw wie im konkreten Fall in der EU ansässige) Vergabestelle ist juristisch leicht erreichbar – sollte diese ihren Sitz jedoch im ferneren Ausland haben, könnte sowohl ein Verfahren als auch eine Durchsetzung des Ergebnisses in tatsächlicher Hinsicht problematisch sein. Hiervon zu unterscheiden ist das „betroffene Land". Im konkreten Fall handelte es sich um Domainnamen unter der TLD „.com", doch dürfte dies generell anwendbar sein: Eine Vergabestelle hat Domainnamen unabhängig von der TLD zu prüfen; diese kann jedoch bei der manuellen Nachkontrolle relevant sein.