MR-Int
Medien und Recht International
4/21
18. Jahrgang/Vol. 18

mrintapp.medien-recht.ws/web/
www.medien-recht.com

Pirateriebekämpfung im Schweizer Urheberrecht

MUR
International Media, IP & IT Law Review

Pirateriebekämpfung im Schweizer Urheberrecht

von **Jonas D. Gassmann**

Rechtsdurchsetzung zwischen Datenschutz und (Streaming-)Realität

Das Schweizer Urheberrecht hat unlängst die Dokumentierung von IP-Adressen von Urheberrechtsverletzern legalisiert: IP-Adressen dürfen zur Pirateriebekämpfung (wieder) bearbeitet werden. Rechtsinhaber haben dadurch auf Kosten des Datenschutzes der Anschlussinhaber ein stärkeres Mittel zur Pirateriebekämpfung erhalten. Allerdings hinkt der neu geschaffene Art 77i URG bereits wieder der heutigen (Streaming-) Realität hinterher – und andernorts erschwert der(selbe) Datenschutz die effektive Rechtsdurchsetzung.

1. Einführung

1.1 Worum es geht

[1] Rechtsinhaber sehen sich bei der Verfolgung von Urheberrechtsverletzungen online nicht selten mit der Schwierigkeit konfrontiert, dass sie zwar eine Verletzung erkennen können, aber nicht an die *Identität der Verletzer* gelangen. Regelmäßig verfügen die Websites mit dem urheberrechtsverletzenden Material über kein Impressum (über das die für die Inhalte verantwortliche Person ausfindig gemacht und abgemahnt werden könnte) oder aber Abmahnungen werden von Verletzern schlicht ignoriert.

[2] Analoge Schwierigkeiten entstehen, wo Rechtsverletzungen nicht über eine Website erfolgen, sondern *Peer-to-Peer (P2P)-Netzwerke* (mit spezieller Software direkt miteinander vernetzte private Computer) urheberrechtsverletzend für den Austausch von Inhalten verwendet werden.

[3] Wollen Rechtsinhaber die Verantwortlichen identifizieren und zur Rechenschaft ziehen, bleibt ihnen in diesen Fällen regelmäßig nur ein Vorgehen über das *Strafrecht*.

[4] Ausgangspunkt für eine Identifikation im Online-Kontext ist die Internet-Protokoll-Adresse (IP-Adresse). Diese Adresse wird an das Internet angebundenen Geräten zugewiesen, und macht sie so adressier- und damit erreichbar. *Statische IP-Adressen* sind fix an einen Computer oder Server einer Website vergeben, und als solche vergleichbar mit der festen Telefonnummer oder der Postadresse einer Person.[1]) Demgegenüber können sich *dynamische IP-Adressen*, die ursprünglich infolge der Knappheit der IP-Adressen entwickelt wurden, stetig ändern. Ein Router, der sich mit dem Internet verbindet, erhält eine im betreffenden Zeitpunkt nicht anderweitig verwendete IP-Adresse zugewiesen. Erfolgt später eine neue Einwahl, erhält er (unter Umständen) eine andere (dann wiederum freie) IP-Adresse.[2]) Internet-Service-Provider (ISP) sind gesetzlich verpflichtet, die Vergabe der IP-Adressen an ihre Kunden zu protokollieren[3]), so dass ermittelt werden kann, wem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war.

[5] Weil ein ISP einem privaten Internetnutzer grundsätzlich eine *dynamische* IP-Adresse zuweist, und diese regelmässig wechselt, benötigen die Strafverfolgungsbehörden für die Identifikation der jeweiligen Anschlussinhaberin (und letztlich für die Verfolgung einer bestimmten Urheberrechtsverletzung) nicht nur die mit der Verletzung zusammenhängende IP-Adresse, sondern auch Angaben über *Datum und Uhrzeit* der Verletzung. Die Identifikation bei einer dynamischen Adressierung gestaltet sich insofern schwieriger bzw. aufwändiger als bei einer statischen Adressierung.

[6] Für eine effektive Rechtsdurchsetzung müssen Rechtsinhaber also nicht nur das verletzte Werk identifizieren, sondern auch Datum und Uhrzeit der Verletzung und die jeweilige IP-Adresse dokumentieren. Diese Dokumentierung war zuletzt mit Unsicherheiten behaftet, und die im Schweizer Urheberrecht enthaltenen rechtlichen Instrumente zur Pirateriebekämpfung ungenügend.

1.2 Das „Logistep"-Urteil des Schweizerischen Bundesgerichts und die Bedenken des US-Handelsbeauftragten

[7] Mit (Leit-)Urteil BGE 136 II 508 ff. („Logistep") vom 8. September 2010 hat das Schweizerische Bundesgericht die Dokumentierung von IP-Adressen durch (Urheber-) Rechtsinhaber als mit dem Schweizer Bundesgesetz über den Datenschutz vom 19. Juni 1992[4]) unvereinbar angesehen. Die Logistep AG hatte in P2P-Netzwerken IP-Adressen der Downloader urheberrechtlich geschützter Werke gesammelt und diese Daten den verletzten Rechtsinhabern

Jonas D. Gassmann, LL.M., CIPP/E, ist Managing Associate bei VISCHER in Zürich. Er verfügt über reiche Erfahrung im Bereich der Durchsetzung von IP-Rechten; weitere Kernbereiche seiner Expertise sind das Technologie-, Medien- und Telekommunikationsrecht, das Datenrecht sowie das Wirtschaftsstrafrecht

1) Techopedia Inc, „Static Internet Protocol Address", https://www.techopedia.com/definition/9544/static-internet-protocol-address (zuletzt besucht am 7. Dezember 2021); vgl auch BGE 136 II 508 ff. (514 f), E. 3.3.

2) Techopedia Inc, „Dynamic Internet Protocol Address", https://www.techopedia.com/definition/28504/dynamic-internet-protocol-address (zuletzt besucht am 7. Dezember 2021); vgl auch BGE 136 II 508 ff (514 f), E. 3.3.

3) Art 19 Abs 1 iVm Art 21 Abs 2 lit b der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 15. November 2017 (VÜPF, SR 780.11).

4) Datenschutzgesetz (DSG, SR 235.1). Das DSG wird derzeit total revidiert („revDSG"; es laufen noch die Arbeiten auf Verordnungsebene, d.h. die Konkretisierung der neuen gesetzlichen Bestimmungen), wobei mit einem Inkrafttreten des revidierten Rechts voraussichtlich 2023 zu rechnen ist.

übergeben.[5]) Die konkrete Datensammlung sowie ihr Zweck waren dabei für die Downloader nicht erkennbar. Das Schweizerische Bundegericht hatte im erwähnten Urteil festgehalten, dass die Dokumentierung der IP-Adressen gegen die *Grundsätze der Zweckbindung*[6]) *und der Erkennbarkeit*[7]) verstoße, mithin eine Persönlichkeitsverletzung darstelle, und diese (namentlich durch überwiegendes Interesse der Rechtsinhaber) nicht gerechtfertigt werden könne – die Dokumentierung also mit dem Schweizer Datenschutzrecht unvereinbar sei.[8])

[8] Die gestützt auf diese widerrechtliche Datenbearbeitung gewonnenen Informationen waren in der Konsequenz im Strafverfahren nicht verwertbar. Gemäß Bundesgericht hätte ein *„den neuen Technologien entsprechende[r] Urheberrechtsschutz"* auf dem Gesetzesweg (und nicht durch Rechtsprechung) zu erfolgen.[9])

[9] Mit Artikel 77i des Schweizer Bundesgesetzes über das Urheberrecht und verwandte Schutzrechte vom 9. Oktober 1992[10]) hat der Schweizer Gesetzgeber für die erwähnte Datenbearbeitung per 1. April 2020 eine explizite gesetzliche Grundlage geschaffen.

[10] Der Schweizer Gesetzgeber adressiert mit den implementierten Maßnahmen zur Pirateriebekämpfung nicht zuletzt auch *Bedenken des US-Handelsbeauftragten*, die dieser im sog Special-301-Report des Jahres 2016[11]) erstmals geäußert hatte. Dieser jährliche Bericht über den weltweiten Schutz von Immaterialgüterrechten enthält ua eine sog Watch List. Auf dieser Liste werden Staaten aufgeführt, die aus Sicht der USA Defizite beim Schutz von Immaterialgüterrechten aufweisen. Auf Verlangen der US-Urheberrechtsindustrie wurde die Schweiz (im Bereich Online-Piraterie in einem Zug genannt mit China, Russland, Ukraine, Indien, Brasilien und Kanada) ab 2016 auf diese Watch List gesetzt und blieb dort bis im April 2020. Auch wenn dies keine unmittelbaren rechtlichen, politischen oder wirtschaftlichen Folgen hatte, so belastete dies jedenfalls die bilateralen Beziehungen zwischen der Schweiz und den USA. Seit der Ausgabe 2020 des Special-301-Reports[12]) erscheint die Schweiz nun nicht mehr auf besagter Watch List.

2. Die neue gesetzliche Grundlage

[11] Mit dem neuen Artikel 77i URG hat der Schweizer Gesetzgeber eine gesetzliche Grundlage für die Bearbeitung von Personendaten von Urheberrechtsverletzern geschaffen. Art 77i URG lautet wie folgt:

> *1 Die Rechtsinhaber und -inhaberinnen, die in ihren Urheberrechten oder in ihren verwandten Schutzrechten verletzt werden, dürfen Personendaten bearbeiten, soweit dies zum Zweck der Strafantragsstellung oder der Strafanzeigeerstattung notwendig ist und sie rechtmässig darauf zugreifen können. Sie dürfen diese Daten auch für die adhäsionsweise Geltendmachung von zivilrechtlichen Ansprüchen oder für deren Geltendmachung nach abgeschlossenem Strafverfahren verwenden.*
>
> *2 Sie haben den Zweck der Datenbearbeitung, die Art der bearbeiteten Daten und den Umfang der Datenbearbeitung offenzulegen.*
>
> *3 Sie dürfen die Personendaten nach Absatz 1 nicht mit Daten verknüpfen, die zu anderen Zwecken gesammelt wurden.*

Im Einzelnen:

2.1 Bearbeitung von Personendaten

[12] Als *Personendaten* iSv Art 77i Abs 1 URG gelten alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.[13]) Soweit IP-Adressen eindeutig einem Rechner zugeordnet werden können und damit die Identifikation eines bestimmten Benutzers oder eines Benutzerkreises zulassen, handelt es sich nach Schweizer Recht um Personendaten.[14])

[13] Der Begriff der *Bearbeitung* ist iSv Art 3 lit e DSG (Art 5 lit d revDSG) zu verstehen.[15]) Erfasst wird damit jeder Umgang mit Personendaten, wie das Beschaffen, Aufbewahren, Verwenden, Archivieren oder Bekanntgeben.

2.2 Kein Ausschluss der Personendatenbearbeitung zu anderen Zwecken und zur Verfolgung anderer Rechtsverletzungen

[14] Artikel 77i URG ist eine spezifische Regelung für die Personendatenbearbeitung durch Rechtsinhaber *zwecks*

5) Die Rechtsinhaber reichten in der Folge regelmäßig Strafanzeige gegen unbekannt ein, gelangten via Akteneinsichtsgesuch im Strafverfahren an die Identität des Inhabers des betroffenen Internetanschlusses und verwendeten die so erlangte Identität zur Geltendmachung von Schadenersatzforderungen.

6) Art 4 Abs 3 DSG.

7) Art 4 Abs 4 DSG.

8) BGE 136 II 508 ff (523 ff), E. 6.3.1 ff. Dabei gilt zu berücksichtigen, dass sich das Schweizer vom europäischen Datenschutzrecht konzeptionell grundlegend unterscheidet: Während nach europäischer Datenschutzgrundverordnung (Verordnung [EU] 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, DSGVO) Personendaten nur bearbeitet werden dürfen, wenn dafür eine (Rechts-)grundlage (wie zB Einwilligung, Notwendigkeit für die Vertragserfüllung oder überwiegende private Interessen) besteht (sog „Verbotsregelung"), ist ein Rechtfertigungsgrund nach Schweizer Datenschutzrecht nur erforderlich, wenn entweder die Bearbeitungsgrundsätze nicht eingehalten werden, die betroffene Person der Bearbeitung widersprochen hat oder einem Dritten besonders schützenswerte Personendaten mitgeteilt werden sollen (sog „Missbrauchsregelung"). Dieser grundsätzliche konzeptionelle Unterschied bleibt auch unter dem neuen Schweizer Datenschutzrecht bestehen.

9) BGE 136 II 508 ff (525), E. 6.4. Vgl. zu diesem Urteil auch *David Rosenthal*, Wenn Datenschutz übertrieben wird oder: Hard cases make bad law, in: Jusletter 27. September 2010; *Sabrina Konrad*, Den Piraten auf der Spur: Die neue Norm zur Datenbearbeitung, in: sic! 2020 S. 482 ff. (483 f.).

10) Urheberrechtsgesetz (URG, SR 231.1).

11) https://ustr.gov/sites/default/files/USTR-2016-Special-301-Report.pdf (zuletzt besucht am 7. Dezember 2021).

12) https://ustr.gov/sites/default/files/2020_Special_301_Report.pdf (zuletzt besucht am 7. Dezember 2021).

13) Art 3 lit a DSG (Art 5 lit a revDSG).

14) BGE 136 II 508 ff (515), E. 3.4.

15) Botschaft des Schweizerischen Bundesrats vom 22. November 2017 zur Änderung des URG sowie zur Genehmigung zweier Abkommen der WIPO und zu deren Umsetzung (zit. „Botschaft URG 2017"; S. 650).

Strafantragsstellung bzw. Strafanzeigeerstattung bei der Verletzung von Urheberrechten und verwandten Schutzrechten. Sind die Voraussetzungen dieser Bestimmung erfüllt, ist die mit der entsprechenden Datenbearbeitung einhergehende Persönlichkeitsverletzung iSv Art 13 Abs 1 DSG (Art 31 Abs 1 revDSG) „*durch Gesetz gerechtfertigt*" – eine Interessenabwägung iSv Art 13 Abs 2 DSG (Art 31 Abs 2 revDSG) erübrigt sich also.

[15] Dies bedeutet umgekehrt *nicht*, dass dadurch eine Personendatenbearbeitung zu *anderen* Zwecken und zur Verfolgung *anderer* Rechtsverletzungen ausgeschlossen ist[16] – nur richtet sich diese (andere) Bearbeitung ausschließlich nach dem DSG.[17])

2.3 Verhältnismäßigkeitsprinzip

[16] Die Personendatenbearbeitung muss gemäß Art 77i Abs 1 URG „*zum Zweck der Strafantragsstellung oder der Strafanzeigeerstattung notwendig*" sein. Gemäß Botschaft URG 2017 (S. 650) dürfen die Rechtsinhaber damit nur jene Daten bearbeiten, „die sie objektiv tatsächlich benötigen und die mit Blick auf den Bearbeitungszweck und die Persönlichkeitsbeeinträchtigung in einem vernünftigen Verhältnis stehen."

[17] Zunächst gilt festzuhalten, dass diese Bestimmung ausschließlich auf die Bearbeitung von Personendaten anwendbar ist, die in einem *Strafverfahren* verwendet werden sollen. Die Bearbeitung von Personendaten ausserhalb dieses Zweckes richtet sich – wie gesehen – nach dem DSG.

[18] In diesem Sinne dürfen Rechtsinhaber etwa IP-Adressen aus P2P-Netzwerken sammeln, um die begangenen Urheberrechtsverletzungen zu dokumentieren und diese Daten anschließend den Strafverfolgungsbehörden übermitteln.

[19] Welche Datenbearbeitungen noch „notwendig" in diesem Sinne sind (und welche nicht), wird sich in der Praxis zeigen müssen – es wird letztlich an den Strafverfolgungsbehörden/Gerichten liegen, die sich gegenüberstehenden Interessen sorgfältig abzuwägen und über die Verhältnismäßigkeit (und damit über die Verwertung der erhobenen Daten im Strafverfahren) zu entscheiden. Klar erscheint jedoch, dass es nicht darauf ankommen darf, ob sich die Strafbehörden im Rahmen ihrer Untersuchungstätigkeit letztlich auf die betreffenden Personendaten stützen oder nicht. Ebenfalls klar erscheint, dass die Rechtsinhaber ihre Bearbeitung von Personendaten soweit wie möglich auf den mutmaßlichen Täterkreis zu beschränken haben.

2.4 Rechtmäßige Datenbeschaffung

[20] Nach Art 77i Abs 1 URG dürfen Rechtsinhaber nur Personendaten bearbeiten, auf die sie „*rechtmäßig zugreifen*" können.[18])

[21] Darin ist nicht eine Rückverweisung auf die Personendatenbearbeitung gemäß DSG zu sehen, denn die Bestimmung von Artikel 77i URG ist wie gesehen gerade als spezifische Regelung für die Personendatenbearbeitung zu verstehen. Vielmehr ist damit gemeint, dass die Personendaten nicht durch eine Verletzung von Bestimmungen des Schweizer Rechts (außerhalb des DSG), die direkt oder indirekt den Persönlichkeitsschutz bezwecken[19]), beschafft werden dürfen.[20]) Das Absuchen des Internets nach Urheberrechtsverletzungen ist mit anderen Worten zulässig.

2.5 Rechtsinhaber

[22] Gemäß Wortlaut von Art 77i Abs 1 URG können sich bloss „*Rechtsinhaber und -inhaberinnen, die in ihren Urheberrechten oder in ihren verwandten Schutzrechten verletzt werden*" auf diese Bestimmung berufen.

[23] Über diesen Wortlaut hinaus kann ein Rechtsinhaber jedoch auch eine Drittpartei (Auftragsbearbeiter) mit der Datenbearbeitung beauftragen.[21]) Zudem muss es gemäß teleologischer Auslegung (im Rahmen derer nach dem Sinn und Zweck sowie den zu Grunde liegenden Wertungen, namentlich nach dem durch die Norm geschützten Interesse zu fragen ist[22]) auch *Rechtsvertretern* von Rechtsinhabern möglich sein, Personendaten von Urheberrechtsverletzern zu bearbeiten (und namentlich zu empfangen und weiterzugeben), soll doch mit Art 77i URG eine effektive Pirateriebekämpfung ermöglicht werden. Datenschutzrechtlich sind die Rechtsvertreter ihrerseits (gemeinsam) Verantwortliche (dh gemeinsam mit den Rechtsinhabern als ihren Klienten).

2.6 Offenlegungspflicht

[24] Nach Art 77i Abs 2 URG haben die Rechtsinhaber „*den Zweck der Datenbearbeitung, die Art der bearbeiteten Daten und den Umfang der Datenbearbeitung offenzulegen*".

[25] Für die betroffene Person muss jede Art der Datenbeschaffung und der weiteren Datenbearbeitung erkennbar sein. Erkennbarkeit bedeutet, dass eine betroffene Person aus den Umständen heraus mit einer Datenbeschaffung rechnen musste oder dass sie entsprechend informiert bzw. aufgeklärt wurde.[23])

[26] Gemäß Botschaft URG 2017 (S. 651) soll eine Offenlegung auf der *Website des Datenbearbeiters* (namentlich im Rahmen der Datenschutzerklärung) genügen. Ob die Piraten diese Informationen je sehen (was der Zweck von Art 77i Abs 2 URG eigentlich gebieten würde[24]),

16) Anderer Meinung offenbar *Riedo*, Art. 77i N 8, in: Barrelet/Egloff (Hrsg), Das neue Urheberrecht, Kommentar zum Bundesgesetz über das Urheberrecht und verwandte Schutzrechte, 4. Aufl., Bern 2020, wonach „die Datenbearbeitung zu ausschliesslich zivilrechtlichen Zwecken (...) mindestens nach dem Wortlaut der Bestimmung ausgeschlossen" sein soll.

17) Botschaft URG 2017, S. 649.

18) Derselbe Grundsatz ist auch in Art 4 Abs 1 DSG (Art 6 Abs 1 revDSG) enthalten, wonach Personendaten „nur rechtmässig bearbeitet werden" dürfen.

19) ZB Hacking iSv Art 143bis des Schweizerischen Strafgesetzbuches vom 21. Dezember 1937 (StGB, SR 311.0).

20) So auch Botschaft URG 2017, aaO.

21) Art 10a DSG (Art 9 revDSG).

22) *Emmenegger/Tschentscher*, Art 1 N 290 ff., in: Hausheer/Walter (Hrsg), Berner Kommentar, Zivilgesetzbuch (ZGB), Einleitung (Art 1-9 ZGB), Bern 2012.

23) Botschaft URG 2017, S. 651.

24) Vgl auch Botschaft URG 2017, aaO: „Ohne die vorgesehene Offenlegungspflicht wäre es möglich, dass die Rechtsinhaberinnen und Rechtsinhaber Daten bearbeiten, ohne dass die betroffene Teilnehmerin oder der betroffene Teilnehmer in irgendein-

darf bezweifelt werden.[25]) Jedenfalls aber unzureichend wäre ein bloßer Verweis auf die Normen des DSG, denn die Offenlegungspflicht ergibt sich aus Art 77i Abs 2 URG, und nicht aus dem DSG.[26])

[27] Unter dem revDSG unterstehen Verantwortliche einer weitergehenden Informationspflicht bei der Beschaffung von Personendaten.[27]) Gestützt auf Art 20 Abs 1 lit b revDSG entfällt diese Informationspflicht indes bei einer Personendatenbearbeitung iSv Art 77i URG. Und auch bei einer Personendatenbearbeitung, die zwar ebenfalls im Bereich der Pirateriebekämpfung, aber außerhalb von Art 77i URG erfolgt, dürfte regelmäßig geltend gemacht werden können, die Information würde den Bearbeitungszweck vereiteln, weshalb die Informationspflicht nach Art 19 revDSG gestützt auf Art 20 Abs 3 lit b revDSG entfallen müsse.

2.7 Verbot der Verknüpfung mit anderen Daten

[28] Art 77i Abs 3 URG verankert den *Zweckbindungsgrundsatz* (wobei die Zweckbindung bereits in Art 77i Abs 1 erster Satz festgehalten ist). Demnach dürfen Rechtsinhaber die bearbeiteten Personendaten nicht mit Daten verknüpfen, die zu *anderen* Zwecken gesammelt werden.[28])

[29] Sammelt ein Rechtsinhaber im selben Kontext auch Daten unabhängig von einem Strafverfahren und damit verbundenen zivilrechtlichen Ansprüchen, muss er diese Daten von den gemäß Art 77i bearbeiteten Personendaten *getrennt* halten.[29])

2.8 Keine Grundlage für die Bearbeitung von Personendaten zu zivilrechtlichen Zwecken

[30] *Keinen* Eingang in die neue Bestimmung von Art 77i URG fand die im Gesetzgebungsprozess umstrittene Bearbeitung von Personendaten durch Rechtsinhaber zu rein *zivilrechtlichen* Zwecken (vorausgesetzt ist also stets die Verwendung im Rahmen eines Strafverfahrens). Danach wäre es Rechtsinhabern möglich gewesen, über durch sie gesammelte Personendaten außerhalb eines Strafverfahrens zur Identifikation von Personen zu gelangen, über deren Anschluss schwerwiegende Urheberrechtsverletzungen begangen wurden.

[31] Hintergrund ist, dass eine zusätzliche oder gar reine Lösung über den Zivilweg eine Durchbrechung des Fernmeldegeheimnisses zur Durchsetzung zivilrechtlicher Ansprüche erfordern würde.[30]) Nach heute geltendem Schweizer Recht wird das Fernmeldegeheimnis jedoch nur zur Durchsetzung *strafrechtlicher* Ansprüche durchbrochen.[31])

[32] Ausdrücklich erlaubt ist aber die Verwendung der bearbeiteten Personendaten für die *adhäsionsweise Geltendmachung zivilrechtlicher Ansprüche* im Rahmen eines Strafverfahrens bzw für deren Geltendmachung nach Abschluss des Strafverfahrens. Vorausgesetzt ist also stets ein Konnex zu einem Strafverfahren, mithin eine deliktische Anspruchsgrundlage für den Zivilanspruch. Damit ist klargestellt, dass Art 77i Abs 1 erster Satz URG die Anwendbarkeit der strafprozessrechtlichen Bestimmungen zur Zivilklage[32]) nicht ausschließt.

3. Würdigung: Guter, aber von der (Streaming-) Realität bereits wieder eingeholter Ansatz

[33] Art 77i URG schafft Raum für die (verdeckte) Sammlung von Personendaten zum Zwecke der Bekämpfung der Piraterie im Bereich Urheberrecht. Stets vorausgesetzt ist jedoch ein Konnex zu einem *Strafverfahren*.

[34] Der Schweizer Gesetzgeber hatte bei der Schaffung von Art 77i URG primär den „Logistep"-Fall, und damit die Bekämpfung von Urheberrechtsverletzungen in P2P-Netzwerken, vor Augen.

[35] Der „Logistep"-Fall entspricht jedoch nicht mehr der *heutigen Realität*: Auch wenn P2P-Netzwerke noch immer existieren, erfolgt die Verbreitung illegaler Inhalte heute sehr viel häufiger via Streamingserver und Sharehoster. Während bei Urheberrechtsverletzungen in P2P-Netzwerken bei den einzelnen Anschlussinhabern/Teilnehmern (IP-Adressen) angesetzt werden kann, können sich die User beim Streaming bzw. beim Download über einen One-Click-Hoster weitgehend hinter den Streamingservern bzw. Sharehostern verstecken, die die IP-Adressen der User horten. Diese liegen regelmäßig fernab der Schweizer Gerichtsbarkeit und die entsprechenden Anbieter haben kein Interesse, die IP-Adressen länger als erforderlich zu speichern.

[36] Immerhin: Es sind auch *andere Fälle* denkbar, in denen sich die Personendatenbearbeitung auf Art 77i URG stützen lässt – so zB die im Rahmen der Pirateriebekämpfung erfolgende Datenbearbeitung durch eine private Anbieterin digitaler Forensik oder durch einen Branchenverband.

[37] Fakt ist aber auch, dass es *für Rechtsinhaber zunehmend schwieriger wird, die Verletzer zu identifizieren* – so zuletzt etwa durch die globale, datenschutzrechtlich motivierte Tendenz zur Nicht-Publikation von Personendaten

er Form davon erfährt."

25) So auch *Riedo*, aaO, Art 77i N 11.

26) Botschaft URG 2017, aaO. Eine datenschutzrechtliche Informationspflicht besteht nur, wenn in irgendeiner Form ein Kontakt zwischen der betroffenen Person (vorliegend der Anschlussinhaberin/Teilnehmerin) und dem Verantwortlichen (vorliegend dem Rechtsinhaber) besteht – was im vorliegenden Kontext gerade nicht der Fall ist. Zur weitergehenden Informationspflicht unter dem revDSG siehe sogleich.

27) Art 19 revDSG.

28) Botschaft URG 2017, S. 651 f.

29) Botschaft URG 2017, aaO.

30) Botschaft URG 2017, S. 649.

31) Vgl Art 1 Abs 1 lit a des Schweizerischen Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18. März 2016 (BÜPF, SR 780.1). Die Überwachung des Post- und Fernmeldeverkehrs ist darüber hinaus gemäß Art 1 Abs 1 BÜPF auch zum Vollzug eines Rechtshilfeersuchens (lit. b), im Rahmen der Suche nach vermissten Personen (lit. c), im Rahmen der Fahndung nach Personen, die zu einer Freiheitsstrafe verurteilt wurden oder gegen die eine freiheitsentziehende Maßnahme angeordnet wurde (lit. d) und im Rahmen des Vollzugs des Schweizerischen Bundesgesetzes über den Nachrichtendienst vom 25. September 2015 (NDG, SR 121) (lit e) möglich.

32) Art 122-126 der Schweizerischen Strafprozessordnung vom 5. Oktober 2007 (StPO, SR 312.0).

im Whois-Verzeichnis der Domainnamen.[33]) Während im Schweizer Urheberrecht mit Art 77i URG auf Kosten des Datenschutzes von Anschlussinhabern/Teilnehmern ein stärkeres Mittel zur Pirateriebekämpfung geschaffen wurde, wird andernorts unter Berufung auf den(selben) Datenschutz im Ergebnis die effektive Rechtsdurchsetzung erschwert. Das Interesse der Rechtsinhaber an einer effektiven Rechtsdurchsetzung würde zuweilen etwas mehr Konsequenz in der Rechtsetzung gebieten.

33) So werden seit dem 1. Januar 2021 – wie bereits bei anderen Top-Level Domainnamen – auch etwa hinsichtlich .ch-Domainnamen keine Personendaten mehr im Whois-Verzeichnis publiziert (vgl Art 46 der Schweizerischen Verordnung über Internet-Domains vom 5. November 2014 [VID, SR 784.104.2]).

Verstoßen Upload-Filter gegen die Meinungsäußerungsfreiheit?

von **Christoph Steindl**

Anmerkung zu den Schlussanträgen des GA Saugmandsgaard Øe zur Rs C-401/19 (EK/Polen) vom 15.07.2021

1. Einleitung

Die Verwirklichung des digitalen Binnenmarkts ist schon seit 2014 ein stetig verfolgtes Ziel der Europäischen Kommission.[1]) Am 14.09.2016 begann ein langwieriger Diskussionsprozess mit einem von der EK veröffentlichten „Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über das Urheberrecht im digitalen Binnenmarkt".[2]) Auf europäischer Ebene kam es zu unzähligen Verhandlungen und Anpassungen des Entwurfs,[3]) wobei praktisch jede Aktualisierung des Normsetzungsverfahrens von Protesten begleitet wurde.[4]) Man befürchtete, dass es durch die DSM-RL[5]) zu einer Einführung von sog „Upload-Filtern" kommen würde. Diese würden zu einer Zensur des Internets führen,[6]) den Einsatz von Überwachungstechnologien fördern[7]) und eine Einschränkung der Meinungsäußerungsfreiheit bedeuten.[8]) Das Ziel der Proteste, die Streichung des gesamten Artikels über den „Upload-Filter",[9]) wurde nicht erreicht, jedoch nahmen sie sehr wohl Einfluss auf die finale Ausgestaltung des Artikels.[10])

Durch die Anwendung von „Upload-Filtern" wird nicht nur das Recht auf Meinungsäußerung (Art 11 GRC) der „aktiven" Nutzer möglicherweise eingeschränkt, da ihr Upload verhindert wird, sondern auch die Rechte „passiver" Nutzer, die den Content anderer betrachten,[11]) sind betroffen.[12]) Dem Gesetzgeber kommt die Aufgabe zu, in der Gesellschaft einen Meinungspluralismus zu gewährleisten.[13]) Durch ein mögliches „overblocking" scheint der Gedanke einer Einschränkung der Meinungsäußerungsfreiheit auf den ersten Blick plausibel.

Die DSM-RL verpflichtet „Diensteanbieter für das Teilen von Online-Inhalten"[14]) (idF DTO) dazu, gewisse Pflichten neben der Einholung einer Erlaubnis von den Rechteinhabern zu erfüllen, damit sichergestellt werden kann, dass bestimmte Werke auf deren Plattformen nicht verfügbar sind. Wie genau diese Pflichten zu verstehen sind, ist nicht nur in der Fachliteratur, sondern auch in der öffentlichen Diskussion, höchst umstritten. Dies gipfelte in der Klage Polens vor dem EuGH, da in der Anwendung des Art 17 Abs 4 lit b und c DSM-RL eine gesetzlich verbotene präventive allgemeine Überwachungspflicht, und eine daraus resultierende Einschränkung der Meinungsäußerungsfreiheit, vermutet wurde.

Polen klagte im Mai 2019 vor dem EuGH[15]) auf Nichtigerklärung des

Christoph Steindl, LL.B., LL.M. (WU), ist Rechtspraktikant am Bezirksgericht Klosterneuburg

1) *Staudegger*, Die Realisierung des Digitalen Binnenmarkts - aktuelle Entwicklungen des IT-Rechts im Überblick, jusIT 2019, 173 (173).
2) EK (2016) 593 final, 2016/0280 (COD).
3) *Hochleitner/Wimmer*, jusIT 2019, 135 (136); *Staudegger*, jusIT 2019, 173 (176).
4) *Hofmann*, EuZW 2020, 397 (397); *Gielen/Tiessen*, EuZW 2019, 639 (639).
5) RL 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der RL 96/9/EG und 2001/29/EG.
6) Social Media Plattformen werden von einem Großteil der Bevölkerung für die Weitergabe und den Empfang von Ideen oder Nachrichten verwendet.
7) *Staudegger*, jusIT 2019, 173 (176).
8) *Hochleitner/Wimmer*, jusIT 2019, 135 (136); *Gerpott*, MMR 2019, 420 (420).
9) Dieser wird in der RL nicht ausdrücklich verlangt, ist aber das wahrscheinlichste Mittel, um die in der RL geforderten Ziele zu erreichen; *Handig*, ÖBl 2019, 212 (215); Hochleitner/*Wimmer*, jusIT 2019, 135 (137).
10) *Hofmann*, ZUM 2019, 617 (617).
11) Da Art 11 GRC auch die Informationsfreiheit umfasst.
12) *Spindler*, GRUR 2020, 253 (257); Müller-Terpitz, ZUM 2020, 365 (368 f).
13) *Müller-Terpitz*, ZUM 2020, 365 (367).
14) Siehe Art 2 Z 6 UAbs 1 DSM-RL.
15) EuGH C-401/19.