Prof. Dr. Benjamin Raue / Prof. Dr. Martin Steinebach[1]

Uploadfilter – Funktionsweisen, Einsatzmöglichkeiten und Parametrisierung

Erstveröffentlichung in: Zeitschrift für Urheber- und Medienrecht 2020, S. 355 – 364.

Art. 17 Abs. 4 lit. b DSM-RL verpflichtet Diensteanbieter für das Teilen von Onlineinhalten (DTO) nach ganz überwiegender Ansicht jedenfalls für solche Schutzgegenstände Uploadfilter einsetzen, für die funktionierende und marktgängige Softwarelösungen existieren. Dieser Beitrag will aus technischer und juristischer Sicht beleuchten, wie Uploadfilter funktionieren und wie durch die richtige Parametrisierung die legitimen Interessen der Rechteinhaber, Plattformnutzer und -betreiber berücksichtigt werden könne. Er will gemäß einem „more technological approach" einen Beitrag zu einem techniksensiblen Urheberrecht leisten.

I. Einleitung

Diensteanbieter für das Teilen von Online Inhalten (DTO) nehmen nach Art. 17 Abs. 1 DSM-RL eine eigene urheberrechtlich relevante Handlung vor, wenn ihre Nutzer urheberrechtlich geschütztes Material auf der Plattform hochladen. Sie können aber nach Art. 17 Abs. 4 DSM-RL ihre Haftung vermeiden, wenn sie alle Anstrengungen („*best efforts*") unternehmen, eine Erlaubnis einzuholen und sicherzustellen, dass von Rechteinhabern benannte Schutzgegenstände nicht verfügbar sind.

DTO definiert Art. 2 Nr. 6 DSM-RL als Anbieter eines Dienstes der Informationsgesellschaft, der große Mengen von urheberrechtlich geschützten Schutzgegenständen speichert, die von Nutzern hochgeladen wurden, und der Öffentlichkeit Zugang zu ihnen verschafft. Auf YouTube etwa werden jede Minute Videos mit einer gesamten Dauer von ca. 500 Stunden hochgeladen.[2] Daher können DTO ihrer Kontrollobliegenheiten faktisch nur dadurch nachkommen, dass sie auf technische Hilfe in Form von Uploadfiltern zurückgreifen.[3] Deswegen besteht die Befürchtung, dass Technik

---

1 *Benjamin Raue* ist Inhaber der Professur für Zivilrecht, Recht der Informationsgesellschaft und des Geistigen Eigentums sowie Direktor des Instituts für Recht und Digitalisierung Trier (IRDT) an der Universität Trier, *Martin Steinebach* ist Leiter der Abteilung Multimedia Sicherheit und IT Forensik am Fraunhofer SIT und Inhaber der Honorarprofessur für Multimedia Sicherheit und IT Forensik an der TU Darmstadt.

2 Zahlen aus Mai 2019, https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/.

3 Nahezu allgemeine Meinung in der Literatur vgl. etwa *Dreier* GRUR 2019, 771 (776); *F. Hofmann* GRUR 2019, 1219 (1221); *Kaesling* JZ 2019, 586 (590); *Pravemann* GRUR 2019, 783 (784); *Senftleben* ZUM 2019, 369 (371); *Spindler* CR 2019, 277 (285); *C. Volkmann* CR 2019, 376 (380).

faktisch Recht schafft und Uploadfilter in der praktischen Rechtsanwendung Nutzerrechte untergraben.

Es soll im Folgenden gezeigt werden, wie Uploadfilter funktionieren und wie die verschiedenen Nutzerinteressen durch deren Parametrisierung berücksichtigt werden können. Es ist dann Aufgabe von Gesetzgeber und Gerichten, im Sinne eines techniksensiblen Urheberrechts,[4] diese Möglichkeiten bei der Ausgestaltung der deutschen Umsetzung von Art. 17 DSM-RL bzw. bei der Konkretisierung der Verkehrspflichten und anderer unbestimmter Rechtsbegriffe zu berücksichtigen.[5]

II. Auszugleichende Interessen

Bei materieller Betrachtung hat der Unionsgesetzgeber mit Art. 17 DSM-RL Verkehrspflichten für DTO festgelegt und Kriterien für die Konkretisierung von Sorgfaltsstandards formuliert.[6] Für die nähere Ausgestaltung macht die Norm drei Zielvorgaben: Es müssen die Interessen der Rechteinhaber, der Nutzer und der Plattformbetreiber miteinander in Ausgleich gebracht werden. Bei der Auslegung und Anwendung der Vorgaben müssen nach der Rechtsprechung des EuGH die entgegenstehenden Grundrechtspositionen berücksichtigt werden.[7]

1. Interessen der Rechteinhaber

Das Urheberrecht ist als Recht des Geistigen Eigentums nach Art. 17 Abs. 2 GRCh geschützt. Zudem hat die EU die Mitgliedstaaten in verschiedenen Richtlinien verpflichtet, ein hohes Schutzniveau für Urheber sicherzustellen.[8] Art. 17 DSM-RL ist als Konkretisierung dieser Pflichten zu verstehen. Er soll die Durchsetzung von Urheberrechten auf Plattformen stärken (Erwgr. 61 DSM-RL) und den DTO einen Anreiz geben, Urheberrechtsverletzungen zu verhindern. Die Interessen der Rechteinhaber sind insbesondere in solchen Fällen stark betroffen, in denen hochgeladene Inhalte in Konkurrenz zu anderen Verwertungsaktivitäten treten. Deswegen kann ein wesentliches Kriterium für die „Schärfe" der Filtereinstellungen sein, ob sich die Schutzgegenstände in der primären Verwertungsphase befinden (z.B. aktuelle Kinofilme oder aktuell in den Charts befindliche Musikstücke); Inhalte des *long tail* müssen dagegen nicht in demselben Maße geschützt werden (dazu unten IV.2.d). Darüber hinaus tangieren längere

---

4 Dazu *Grünberger/Podszun* ZGE 2014, 269 f.; *Grünberger* ZUM 2015, 273 (275 f.); *F. Hofmann* ZGE 2016, 482 ff.; *Specht* GRUR 2019, 253 (255).

5 Ähnlich *M. Becker* ZUM 2019, 636 (645): „automatisierbare Freiheitsregeln, also Freiheitsregeln, die für Maschinen geschaffen sind".

6 Dazu ausführlich *F. Hofmann* ZUM 2019, 619 (622, 626); *F. Hofmann* GRUR 2019, 1219 f. Ferner *Wandtke* NJW 2019, 1841 (1846).

7 Vgl. nur EuGH ZUM 2019, 759 Rn. 20, 38 – Spiegel Online/Volker Beck m. w. N.

8 Erwgr. 24 SatCab-RL; Erwgr. 1, 4, 9, 10 InfoSoc-RL; Erwgr. 12 Schutzdauer-RL.

Filmausschnitte, ganze Musikstücke und stark nachgefragte Inhalte ihre Interessen stärker als kurze Film- oder Musikschnipsel oder kaum abgerufene Beiträge (dazu unten IV.2.e).

2. Interessen der Nutzer

Bei nutzergenerierten Inhalten ist es in vielen Fällen schwierig, zwischen einer Urheberrechtsverletzung und einer aufgrund von Urheberrechtsschranken erlaubten Nutzung zu unterscheiden.[9] Daher stehen DTO vor dem Dilemma, entweder zu viele Urheberrechtsverletzungen zuzulassen (*under-enforcement*) oder erlaubte Nutzerhandlungen zu unterbinden (*over-enforcement*).[10] Weil im ersten Fall die Haftung nach Art. 17 Abs. 1 DSM-RL droht, im zweiten Fall aber nicht, wird die berechtigte Sorge artikuliert, dass Plattformen im Zweifel eher Inhalte sperren als sie zuzulassen.[11] Allerdings können sich auch die Nutzer von Plattformen für die Verbreitung von Inhalten auf ihre Kommunikationsfreiheiten (Meinungs- und Kunstfreiheit, Art. 11 Abs. 1, 13 GRCh) berufen.[12] Zudem wird die Informationsfreiheit (Art. 11 Abs. 1 GRCh) durch zu strenge Uploadfilter eingeschränkt. Deswegen hat der Unionsgesetzgeber in Art. 17 Abs. 7 DSM-RL für die nähere Ausgestaltung der Verkehrspflichten vorgegeben, dass die von den DTO eingesetzten Maßnahmen nicht bewirken dürfen, „dass von Nutzern hochgeladene Schutzgegenstände, bei denen kein Verstoß gegen das Urheberrecht oder verwandte Schutzrechte vorliegt, nicht verfügbar sind“. Insbesondere rechtmäßige Nutzerhandlungen, die durch Schranken gedeckt sind, dürfen die Plattformen also nicht auf urheberrechtlicher Grundlage unterbinden.

Dieser Beitrag will einige Optionen aufzeigen, mit denen die Interessen der Nutzer dadurch berücksichtigt werden können, dass die Uploadfilter durch eine Parametrisierung in differenzierter Weise auf unterschiedliche Arten von Nutzeruploads reagieren. Insbesondere bei der Festlegung von Ähnlichkeitsschwellenwerten, bei denen die Uploadfilter den Upload eines Inhalts verhindern, muss die Kommunikationsfreiheit der Nutzer berücksichtigt werden (dazu unten IV.2.a). Darüber hinaus muss berücksichtigt werden, inwieweit der hochgeladene Inhalt die Interessen der Rechteinhaber beeinträchtigen kann (dazu unten IV.2.e). Weil es dem Gesetzgeber in erster Linie darum ging, alternative, von den Rechteinhabern lizen-

---

9 *F. Hofmann* GRUR 2019, 1219 (1221).

10 Vgl. dazu *F. Hofmann* GRUR 2019, 1219 (1221).

11 *Gielen/Tiessen* EuZW 2019, 639 (645); *Kaesling* JZ 2019, 586 (589); *Pravemann*, GRUR 2019, 783 (784); *Senftleben* ZUM 2019, 369 (372); *Spindler* CR 2019, 277 (289); *Suwelack* MMR 2018, 582 (585); *C. Volkmann* CR 2019, 376 (380).

12 Zur (mittelbaren) Grundrechtsbindung von sozialen Netzwerken, *Raue* JZ 2018, 961 (964 ff.); *Spindler* CR 2019, 238 (242 ff.).

zierte Angebote zu stärken (vgl. Erwgr. 62 S. 2 DSM-RL), ist es nicht erforderlich, Inhalte streng zu filtern, die nur wenig abgerufen werden. Bei ihnen können großzügigere Filterkriterien angelegt werden. Auch wenn lediglich kleine Ausschnitte von Musikstücken oder Filmen in andere Werke integriert werden, kann es unverhältnismäßig sein, deswegen den Upload zu verhindern. Darüber hinaus ist es möglich, die Selbsteinschätzung von Nutzern zu berücksichtigen, bevor der Upload automatisch blockiert wird (dazu unten IV.2.b). Die Kommunikations- und Informationsfreiheit ebenfalls beeinträchtigen können *Copyfrauds*, die sich Rechte anmaßen, die ihnen überhaupt nicht oder jedenfalls nicht in dem Umfang zustehen. Hier kann es angemessen sein, den Plattformbetreibern aufzugeben, deren Inhalte zukünftig nicht mehr automatisch herausfiltern zu dürfen.

Der Nutzer kann die Rechte, die ihm nach Art. 17 Abs. 9 DSM-RL zustehen, nur geltend machen, wenn ihm die Reaktion des Uploadfilters auf das (geplante) Hochladen mitgeteilt wird.[13] Deswegen müssen entsprechende Nutzer-Schnittstellen eingerichtet werden (dazu unten III.2.e).

3. Interessen der Plattformbetreiber

Außerdem müssen bei den Anforderungen an die „*best efforts*" die Interessen der Diensteanbieter berücksichtigt werden, deren unternehmerische Betätigung ebenfalls grundrechtlich geschützt ist (Art. 16 GRCh). Von ihnen dürfen nach Art. 17 Abs. 5 DSM-RL daher nur verhältnismäßige Maßnahmen gefordert werden.[14] Dementsprechend sind nach Art. 17 Abs. 5 lit. b DSM-RL auch die Kosten zu berücksichtigen, die den Anbietern für ihre Sorgfaltsanstrengungen entstehen. Das kann Einfluss auf die Art der Filtertechnik haben, die von den Plattformen verlangt werden. Je nach Medium können genauere Verfahren teilweise erhebliche Mehrkosten verursachen (dazu unten III.4.). So können nach momentanem Stand der Technik einzelne Standbilder von Videos nicht mit verhältnismäßigem Aufwand erkannt werden. Unmögliches kann von den Plattformen – selbstverständlich – nicht verlangt werden.[15] Nach momentanem Stand der Technik können etwa nicht einzelne Klangelemente eines Musikstücks erkannt werden, die z. B. beim Sampling einem Musikstück beigemischt werden.

---

13 Vgl. auch BVerfG NJW 2018, 1667 Rn. 46 f. – Stadionverbot.

14 Vgl. dazu auch *Kaesling* JZ 2019, 586 (587); *F. Hofmann* GRUR 2019, 1219 (1225). Kritisch *Spindler* CR 2019, 277 (287).

15 *Spindler* CR 2020, 50 (54); *Gielen/Tiessen* EuZW 2019, 639 (645); *Stieper* ZUM 2019, 211 (216).

Es wird befürchtet, dass die (mittelbare) Verpflichtung zur Nutzung von Uploadfiltern gerade solche marktmächtigen, großen Plattformen weiter stärkt, die über entsprechende Technologien verfügen.[16] Dieser Aspekt muss auch jenseits des „Start-Up-Privilegs" (Art. 17 Abs. 6 DSM-RL) bei der Auslegung des Verhältnismäßigkeitsgrundsatzes beachtet und weniger leistungsstarke Plattformen weniger strengen Pflichten unterworfen werden.[17] Die Entwicklung und der Betrieb eines eigenen Uploadfilters erfordern hohen technischen Sachverstand und Betriebsressourcen. Das ist nicht allen Anbietern zumutbar, so dass diese nur insoweit zum Einsatz von Uploadfiltern verpflichtet werden können, als es am Markt externe Dienstleister gibt, die zu zumutbaren Preisen die notwendigen Filter zur Verfügung stellen.[18] Je nach Preismodell der Anbieter kann es die Zumutbarkeit der Filterung für kleinere Anbieter erhöhen, wenn diese nicht alle Inhalte, sondern nur besonders populäre überprüfen müssen (dazu unten IV.2.e).

Um die Zumutbarkeit für die Plattformanbieter zu erhöhen, sind sie zudem nicht verpflichtet, jegliche urheberrechtlich geschützten Gegenstände von ihren Plattformen fernzuhalten, sondern nur solche, zu denen der Rechteinhaber „einschlägige und notwendige Informationen bereitgestellt" hat (Art. 17 Abs. 4 lit. b DSM-RL). Hier wird zu diskutieren sein, in welcher Form Rechteinhaber die Informationen bereitstellen müssen, also insbesondere, ob sie auf die Plattformen zugehen müssen oder ob es ausreicht, dass sie entsprechende Repertoire-Datenbanken zur Verfügung stellen.[19] Die Bundesregierung favorisiert die Einrichtung öffentlicher und transparenter Plattformen, die nicht in der Hand einiger marktmächtiger Plattformen stehen.[20] Ebenfalls geklärt werden muss, ob die Schutzgegenstände als solche oder nur deren Hashwerte bzw. vergleichbare identifizierende Merkmale zur Verfügung gestellt werden. Bei Letzteren ist dann erforderlich, eine einheitliche Methode zur Gewinnung der Merkmale zu definieren oder das Format und die Eigenschaften der Merkmale festzulegen. Nur so können unterschiedliche Methoden der Merkmalsgewinnung

16 Etwa *Gielen/Tiessen* EuZW 2019, 639 (644); *Suwelack* MMR 2018, 582 (585).

17 *F. Hofmann* GRUR 2019, 1219, 1226 f.; *F. Hofmann* ZUM 2019, 617 (625); *Gielen/Tiessen* EuZW 2019, 639 (644). Kritisch dagegen *Spindler* CR 2019, 277 (287); *Spindler* CR 2020, 50 (51, 53), der „Pflichtenreduktionen" im Einzelfall aber ebenfalls für zulässig hält.

18 Vgl. etwa *Gielen/Tiessen* EuZW 2019, 639 (644).

19 Vgl. *Spindler* CR 2019, 277 (286); *Spindler* CR 2020, 50 (51).

20 Vgl. Protokollerklärung „Erklärung der Bundesrepublik Deutschland zur Richtlinie über das Urheberrecht und verwandte Schutzrechte im Digitalen Binnenmarkt; insbesondere zu Artikel 17 der Richtlinie" v. 15.4.2019, Nr. 5 (abrufbar unter: https://www.bmjv.de/SharedDocs/Downloads/DE/News/PM/041519_Protokollerklaerung_Richtlinie_Urheberrecht.pdf?__blob=publicationFile&v=1).

untereinander kompatible Merkmale erzeugen, die gemeinsam auf einer Plattform genutzt werden können.

III. Funktion und Aufbau von Uploadfiltern

Unter dem Begriff „Uploadfilter" werden Systeme verstanden, die digitale Inhalte beim Hochladen auf die Plattform eines Onlinedienstes untersuchen und basierend auf dem Untersuchungsergebnis eine Entscheidung über die nachfolgende Verfahrensweise mit diesem Inhalt treffen.

Bekannt ist dabei der Onlinedienst YouTube mit seinem Verfahren „Content ID"[21], das hochgeladene Videoinhalte Rechteinhabern zuordnen kann und diesen verschiedene Möglichkeiten bietet, auf den Upload ihrer Inhalte zu reagieren.

Der Kern eines Uploadfilters ist dabei immer eine Software, die digitale Inhalte entweder wiedererkennen oder klassifizieren kann. Wiedererkennen bedeutet hier, dass ein Schutzgegenstand vorher auf eine Sperrliste eingetragen sein muss und der Uploadfilter dann durch geeignete Methoden diesen Schutzgegenstand als identisch mit dem hochgeladenen Inhalt erkennen kann.

Werden Uploadfilter zur Verhinderung von Urheberrechtsverletzungen eingesetzt, ist ihre Aufgabe üblicherweise auf das Wiedererkennen von Schutzgegenständen ausgelegt. Rechteinhaber stellen ihre geschützten Inhalte bereit, der Uploadfilter leitet aus diesen die zum Erkennen notwendigen Merkmale ab und speichert sie in einer Datenbank. Ggf. reicht es auch aus, dass die Rechteinhaber nicht die Schutzgegenstände als solche, sondern lediglich (standardisierte) Merkmale zur Verfügung stellen. Mit diesem Eintrag wird dann später ein hochgeladenes Werk verglichen.

1. Kryptografische vs. robuste Hashverfahren

Allgemein ist ein Hashverfahren eine Abbildung von Daten beliebiger Länge auf Daten fixer Länge. Hierfür gibt es zahlreiche Anwendungen mit unterschiedlichen Ausprägungen. Eine der ersten Nutzungen erfolgte im Datenbankbereich zur Indexierung. Im Kontext von Urheberrechten müssen hier kryptografische und robuste Hashverfahren unterschieden werden. Kryptografische Hashverfahren[22] sind darauf angelegt, Dateien mit identischem Inhalt zu identifizieren. Sie verwenden mathematische Funktionen, die aus Dateien beliebiger Länge eine Bitfolge festgelegter Länge

---

21 https://www.youtube.com/t/contentid.

22 *Preneel*, Cryptographic hash functions, European Transactions on Telecommunications 1994, 431 ff.

erzeugen, die eine Reihe von Eigenschaften haben, welche für Sicherheitsanwendung von Bedeutung sind. Aufgrund dieser Eigenschaften sind sie aber für die Zwecke von Art. 17 DSM-RL nicht sonderlich geeignet, da Dateien mit geschützten Inhalten bereits bei nur geringfügigen Änderungen nicht mehr erkannt werden können.

Um dementsprechend auch Dateien mit geringfügig geänderten Inhalten erkennen zu können, müssen sogenannte robuste Hashverfahren[23] eingesetzt werden. Diese Hashfunktionen erzeugen ebenfalls aus beliebig großen Medien, beispielsweise einem Bild oder einer vorgegebenen Spieldauer einer Audiodatei, einen Hash mit einer festgelegten Länge. Diese Hashverfahren orientieren sich an der menschlichen Wahrnehmung und streben an, solange den gleichen Hashwert zu erzeugen, wie ein menschlicher Betrachter eine Datei als gleich ansehen würde.

2. Komponenten eines Uploadfilters

Uploadfilter bestehen typischerweise aus den folgenden Komponenten:

a) Datenbank

In der Datenbank werden die Merkmale zu den einzelnen Schutzgegenständen gespeichert. Darüber hinaus werden hier auch Metadaten hinterlegt, beispielsweise der Rechteinhaber und der Name des Werks. Es ist noch ungeklärt, in welcher Form die Rechteinhaber die nach Art. 17 Abs. 4 lit. b DSM-RL notwendigen Informationen bereitstellen müssen (dazu bereits oben II.3.)

b) Merkmalsextraktion

Bei der Merkmalsextraktion werden aus den geschützten Gegenständen eindeutig identifizierende Beschreibungen erstellt, die effizient in der Datenbank gespeichert werden können. Durch diese wird die benötigte Datenmenge zur Beschreibung eines Schutzgegenstands deutlich reduziert.

c) Merkmalsvergleich

Robuste Hashfilter erkennen hochgeladene Schutzgegenstände nicht nur, wenn sie identisch mit den hinterlegten Merkmalen sind. Auch bei einer vorher festgelegten Ähnlichkeit der verglichenen Gegenstände kann das

---

23 *Venkatesan/Koon/Jakubowski/Moulin*, Robust image hashing Proceedings 2000 International Conference on Image Processing, 664 ff. (abrufbar unter: https://www.researchgate.net/publication/224067859_Robust_image_hashing).

System Maßnahmen treffen. Daher sind Methoden notwendig, die Merkmale in der Datenbank mit denen eines neuen Inhalts vergleichen und ein Ähnlichkeitsmaß feststellen können.

d) Schnittstelle zum Rechteinhaber

Uploadfilter bieten oft mehr Funktionen als nur das Sperren von Inhalten. Sie können dem Rechteinhaber eine Reihe weiterer Reaktionsmöglichkeiten gewähren, wenn Inhalte hochgeladen werden, in denen seine Schutzgegenstände vorkommen. Beispielsweise kann er das Hochladen erlauben, um an den Werbeeinnahmen zu partizipieren oder um die Popularität des Inhalts zu steigern. In beiden Fällen kann er sich vorbehalten, erst ab einem bestimmten Schwellenwert weitere Maßnahmen zu ergreifen.

Im Falle von ContentID beispielsweise kann der Rechteinhaber erkannte Inhalte entweder sperren, monetarisieren und somit über Werbung die Nutzung bezahlen lassen oder nur beobachten und die Entscheidung auf einen späteren Zeitpunkt verschieben.

e) Schnittstelle zum Nutzer

Erkennt der Uploadfilter beim Hochladen, dass der Inhalt in der Datenbank hinterlegt ist, und reagiert er (oder der Rechteinhaber) darauf, kann dem Nutzer über eine Nutzer-Schnittstelle die Entscheidung mitgeteilt und transparent gemacht werden.[24] So können insbesondere die erkannten Schutzgegenstände genannt und die vom Rechteinhaber getroffenen Maßnahmen aufgezeigt werden. Dem Nutzer muss jedoch auch die Möglichkeit gegeben werden, gegen Entscheidungen „Einspruch“ einzulegen (Art. 17 Abs. 9 DSM-RL).

3. Erkennen von Ausschnitten oder veränderten Schutzgegenständen

Die eigentliche Aufgabe des Uploadfilters ist das Erkennen von Inhalten, deren Merkmale vorher in der Datenbank gespeichert worden sind. Dabei soll der Filter nicht nur vollständige Werke erkennen, da auch schöpferische Ausschnitte[25] und veränderte Schutzgegenstände bis zur Grenze des § 24 UrhG in den Schutzbereich des Urheberrechts fallen. Bei Leistungs-

---

24 Vgl. auch *Spindler* CR 2020, 50 (58).

25 Ausschnitte und Teile eines Werks werden nur geschützt, wenn sie ihrerseits individuelle Züge aufweisen, EuGH ZUM 2009, 945 Rn. 39 – Infopaq; BGH ZUM 2011, 151 Rn. 54 – Perlentaucher; Dreier/Schulze/*Schulze*, UrhG, 6. Aufl. 2018, § 2 Rn. 76 m. w. N.

schutzrechten kann grundsätzlich bereits die Übernahme kurzer Sequenzen, etwa einer Tonaufnahme, in das Leistungsschutzrecht eingreifen.[26] Das System muss daher hinterlegte Schutzgegenstände auch in abgeänderter Form wiedererkennen, etwa bei Bildern Teilbereiche und bei Video- bzw. Audiodateien zeitliche Abschnitte. Darüber hinaus sollte eine Erkennung möglich sein, wenn ein Gegenstand nachbearbeitet wurde, also beispielsweise ein Video gespiegelt, ein Musikstück schneller bzw. langsamer läuft oder ein Bild verzerrt wird.

Auch wenn geschützte Inhalte in anderen Werken in nicht-freier Weise verwendet werden, greift dies in die Rechte des Rechteinhabers ein. Musikstücke können als Hintergrund in Videos verwendet oder Videos können als Element in einem Teilbereich eines anderen Videos eingeblendet werden. Bei Musikstücken kann es auch darum gehen, die Notenfolge oder den Text zu erkennen.

4. Medienabhängiger Aufwand

Vor dem in 3. geschilderten Hintergrund können die Anforderungen an die Merkmalsextraktion und den Merkmalsvergleich sehr komplex werden. Die Kosten für die Filtermaßnahmen sind bei der Zumutbarkeit der Anstrengungen zu berücksichtigen, die von den Plattformbetreibern berücksichtigt werden können (Art. 17 Abs. 5 lit. b DSM-RL).

Merkmale, die zur Erkennung von Werken herangezogen werden, unterscheiden sich in Abhängigkeit von dem Medium, für das sie eingesetzt werden. Dabei sind zwar einige Medien miteinander verwandt, aus Effizienzgründen werden aber unterschiedliche Methoden der Merkmalsgewinnung eingesetzt.

a) Bilder

Ein Vergleich eines Bildes mit einem anderen ist mit einfachen Verfahren möglich. Insbesondere für Bilder ist eine Vielzahl von Verfahren bekannt, die auf Basis extrahierter Merkmale ein Wiedererkennen von Bildern erlauben.

aa) Blockhash-Algorithmen

Einfache und dennoch zuverlässige Methoden sind die sogenannten Blockhash-Algorithmen. Hier wird ein Bild beliebiger Größe auf eine feste

---

[26] EuGH ZUM 2019, 738 Rn. 29 ff. – Pelham/Hütter. Das gilt allerdings nicht bei „geänderter und beim Hören nicht wiedererkennbarer Form“, EuGH ZUM 2019, 738 Rn. 31 – Pelham/Hütter.

Größe von 16x16 Pixel herunterskaliert und in Graustufen umgerechnet. Von den entstehenden 256 Helligkeitswerten wird der Median der Helligkeit bestimmt. Dann werden die Pixel anhand einer einfachen Vorschrift in eine binäre 256 Stellen lange Sequenz umgewandelt. Jeder Pixel, dessen Helligkeit über dem Median liegt, wird zu einer 1, jeder, welcher kleiner oder gleich dem Median ist, eine 0. Die Ähnlichkeit zweier Bilder wird dann über die Hamming-Distanz berechnet. Zwei Bitsequenzen werden miteinander an jeder Position verglichen. Es werden die Stellen gezählt, an denen sich die beiden Sequenzen unterscheiden. Die Anzahl der sich unterscheidenden Stellen entspricht dann der Hamming-Distanz der beiden Sequenzen. Bei einer Länge von 256 Bit hätten zwei zufällige Sequenzen eine durchschnittliche Distanz von 128. Zwei Bilder werden üblicher Weise als gleich angesehen, wenn ihre Distanz geringer als 33 ist oder anders gesagt 7 von 8 Bit übereinstimmen.

Abbildung 1: Beispiel Blockhash. Links das Ausgangsbild, welches erst in Graustufen umgewandelt und dann auf 16x16 Pixel verkleinert wird. Der Median der Grauwerte bildet dann die Grenze für die binäre Einordnung rechts.

Ein entsprechendes Verfahren kann sehr effizient und zuverlässig vollständige Bilder identifizieren,[27] scheitert aber daran, Ausschnitte aus Bildern zu erkennen. Einen Bildausschnitt zu erkennen, erfordert das Hinzuziehen von Verfahren, die das ursprüngliche Verfahren resistent gegen Segmentierung machen. Sie lassen die notwendige Rechenleistung bei der Extraktion und dem Vergleich steigen, da ein Bild nicht mehr als Ganzes betrachtet werden kann, sondern erst in Bildobjekte aufgeteilt werden muss, die jeweils einzeln behandelt werden. Das Aufteilen ist oft aufwändiger als die Merkmalsextraktion selbst. Die Merkmale müssen nun nicht nur für ein Bild, sondern für mehre Teile des Bildes bestimmt werden. Dies führt zu einem höheren Speicherbedarf in der Datenbank und mehr Aufwand beim Merkmalsvergleich, da die Merkmale mehrere Segmente mit den Einträgen der Datenbank verglichen werden müssen.

27 *Zauner/Steinebach/Hermann*, Rihamark: Perceptual Image Hash Benchmarking, Media Watermarking, Security, and Forensics III, Vol. 7880, 78800X.

bb) Weitere robuste Verfahren

Alternativ zu den robusten Hashverfahren können auch komplexere Methoden zum Extrahieren und Vergleichen von Merkmalen eingesetzt werden. Bekannt sind hier insbesondere SIFT (*Scale-invariant feature transform*)[28] und SURF (*Speeded Up Robust Features*)[29]. Sie bestimmen besonders prägnante Stellen im Bild anhand von Kantenerkennung. Ihr Vorteil ist eine hohe Robustheit gegen Bildoperationen wie Rotation oder Verzerrung. Varianten von ihnen sind auch geeignet, einzelne Bildausschnitte zu erkennen. Nachteil der Verfahren ist ein deutlich höherer Rechen- und Speicheraufwand, der jeweils durchaus ein Hundertfaches der einfachen Blockhashverfahren betragen kann.

b) Videos

Ein Video könnte als eine Folge von Bildern betrachtet werden. Daher ließe sich ein Video auch mit einem Verfahren zum Erkennen von Bildern behandeln. Dazu müssten aber für jedes Video sehr viele Einzelbilder verarbeitet werden. Bei 30 Bildern pro Sekunde und 3 Minuten Spieldauer lägen bereits 5.400 Hashes vor. Daher sind Methoden zur Merkmalserkennung üblicherweise mit steigender Spieldauer oder Datenmenge immer stärker verallgemeinernd oder ungenauer. So würde man in einem Video nicht mehr ein ganzes Bild betrachten, sondern beispielsweise lediglich die Schwankung der durchschnittlichen Helligkeit von einem Bild zum nächsten. Ein einzelnes Bild wird dann nur noch durch einen Helligkeitswert dargestellt.

---

28 *Lowe*, Distinctive Image Features from Scale-Invariant Keypoints, International Journal of Computer Vision, 60(2), 91 ff. (abrufbar unter: https://robo.fish/wiki/images/5/58/Image_Features_From_Scale_Invariant_Keypoints_Lowe_2004.pdf).

29 *Bay/Tuytelaars/Van Gool*, SURF: Speeded up Robust Features, European Conference on Computer Vision, 404 ff. (abrufbar unter: https://www.vision.ee.ethz.ch/~surf/eccv06.pdf).

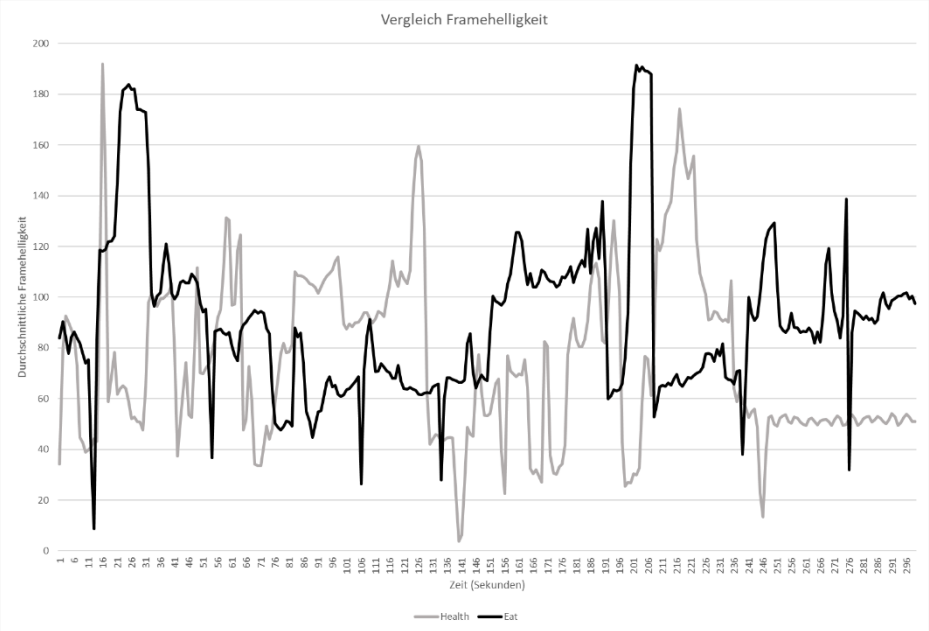

Abbildung 2: Bereits einfach Merkmale wie die durchschnittliche Helligkeit der Videobilder können als Ausgangspunkt einer Erkennung dienen. Das Beispiel zeigt die durchschnittliche Helligkeit zweier Videos (health, eat) jeweils pro Sekunde über 5 Minuten Spieldauer hinweg.

Für Videodaten werden Methoden[30] benötigt, die deren hohes Datenvolumen effizient handhaben können. Ideal sind dabei Ansätze, die direkt auf den komprimierten Daten arbeiten können und beispielsweise nur grundlegende Helligkeitsinformationen extrahieren oder sich an den Bewegungsvektoren von Bildobjekten orientieren. Einzelne Standbilder können so nicht erkannt werden, da hier die gespeicherten Daten nicht ausreichen. Ein vollständiges Video ist allerdings üblicherweise nicht notwendig, da auch Ausschnitte ab einer verfahrensabhängigen Länge erkannt werden können.

c) Audios

Bei Audiodaten gelten ähnliche Rahmenbedingungen wie für Videos. Ziel von Verfahren zur Merkmalserkennung ist, ausreichend lange Abschnitte zu erkennen, nicht aber einzelne Klangelemente, wie dies beim Erkennen von Sampling notwendig wäre. Bekannte Verfahren setzen hier beispielsweise einen Vergleich der Energie von Frequenzbändern im Abstand von Halbtonschritten ein[31] oder bestimmen für mehrere Frequenzbänder, ob diese eher einem Rauschen oder einem Sinuston gleichen.

---

30 *Oostveen/ Kalker/ Haitsma*, Visual hashing of digital video: applications and techniques, Applications of digital image processing XXIV, Vol. 4472, 121 ff.

31 *Haitsma/Kalker/Oostveen*, Robust Audio Hashing for Content Identification, International Workshop on Content-Based Multimedia Indexing, Vol. 4, 117 ff.

d) Texte

Auch für Texte sind robuste Merkmalserkennungen bekannt.[32] Sie sind toleranter gegen Änderungen als herkömmliche Verfahren zum Wiedererkennen von Text, wie sie beispielsweise bei der Plagiatssuche eingesetzt werden. Sie können auch ähnliche Texte erkennen, bei denen einzelne Worte durch Synonyme ersetzt werden. Umgesetzt werden sie beispielsweise durch das Bilden von Histogrammen von Zeichenfolgen oder das Abbilden von Substantiven auf eine binäre Sequenz anhand einer Zuordnungstabelle. So wird aus einem Text eine Bitfolge, deren Länge der Anzahl der Substantive im Text entspricht. Hier besteht die Schwierigkeit darin, dass gerade bei Gebrauchstexten nur die konkrete Form, nicht aber der Inhalt geschützt ist und bei Texten der kleinen Münze schon kleine Änderungen aus dem Schutzbereich führen.[33]

5. Eigen- oder Fremdbetrieb

Die konzeptionell einfachste Umsetzung eines Uploadfilters für einen Diensteanbieter ist eine lokale Variante, bei der er alle Komponenten eines Systems selbst betreibt. Er muss dann Rechteinhabern ermöglichen, Schutzgegenstände in die Datenbank einzutragen, durch Nutzer eingehende Medien durch einen Merkmalsvergleich prüfen und Reaktionsmöglichkeiten anbieten. Dies erfordert allerdings einen hohen technischen Sachverstand, da für den Medientyp der Plattform geeignete Algorithmen zu Merkmalsextraktion und -vergleich ausgewählt und die notwendigen Ressourcen für einen verzögerungsfreien Betrieb geplant und bereitgestellt werden müssen.

Alternativ kann ein Betreiber einen externen Dienstleister einsetzen, der für ihn die Merkmalsüberprüfung und die Pflege der Datenbank übernimmt. Wenn die Verfahren zur Merkmalsextraktion lokal beim Betreiber zur Verfügung stehen, müssen nur verhältnismäßig geringe Datenvolumen zum Dienstleister übertragen werden. Dieser prüft dann und meldet das Ergebnis zurück. Vorteil für Rechteinhaber und Betreiber ist dabei, dass beide auf eine einzelne, vom Dienstleister betriebene zentrale Datenbank zurückgreifen können.

(abrufbar unter: https://pdfs.semanticscholar.org/7615/c9e0df48b1353ac67d483e349abb60f3635a.pdf?_ga=2.167827110.62386334.1582269610-683348854.1582269610).

32 *Steinebach/Klöckner/Reimers/Wienand/Wolf*, Robust Hash Algorithms for Text, IFIP International Conference on Communications and Multimedia Security, 135 ff.

33 BGH GRUR 1993, 34 (35) – Bedienungsanweisung; Dreier/Schulze/*Schulze*, UrhG, 6. Aufl. 2018, § 2 Rn. 34.

IV. Interessenausgleich durch Parametrisierung der Uploadfilter

Im Folgenden soll gezeigt werden, wie die unter III. vorgestellten Parameter eines Uploadfilters für den in Art. 17 DSM-RL angelegten, oben unter II. dargestellten Interessenausgleich herangezogen werden können. Die folgenden Ausführungen verstehen sich als Toolbox, auf die Gesetzgeber und Gerichte für die Konkretisierung des angemessenen Interessenausgleichs zurückgreifen können.

Normativer Anknüpfungspunkt dafür ist Art. 17 Abs. 5 DSM-RL. Dieser legt Kriterien fest, mit denen die von Art. 17 Abs. 4 DSM-RL geforderten „Anstrengungen" „nach Maßgabe hoher branchenüblicher Standards für die berufliche Sorgfalt" konkretisiert werden können. Dabei ist nach Art. 17 Abs. 5 lit. a DSM-RL zunächst die Art, das Publikum und der Umfang der Dienste sowie die Art der hochgeladenen Schutzgegenstände, also das *Beeinträchtigungspotenzial* eines Uploads zu berücksichtigen. Nach Art. 17 Abs. 5 lit. b DSM-RL sind die Verfügbarkeit geeigneter und wirksamer Mittel, also die *Möglichkeit der Filterung*, sowie die Kosten der Filtermaßnahmen, also die *Zumutbarkeit* für die Diensteanbieter, zu berücksichtigen.

1. Robustheit des Hash-Filters

Robuste Hash-Verfahren zeichnen sich dadurch aus, dass sie einen hinterlegten Schutzgegenstand auch dann erkennen, wenn er verändert oder lediglich ausschnittsweise hochgeladen worden ist (oben III.). Die Auswahl der Schwellenwerte, bei denen der Filter anschlägt und automatisch einen Upload verhindert, hat dabei ganz erheblichen Einfluss darauf, ob und in welchem Ausmaß Nutzerrechte verwirklicht werden können.

Im Vergleich zur geltenden Rechtslage würde es die Rechtsdurchsetzung für Rechteinhaber bereits erleichtern, wenn identische oder nahezu identische Kopien der von ihnen hinterlegten Schutzgegenstände automatisch von Plattformen entfernt würden. Darüber hinaus können sich Nutzer im Regelfall nicht auf gesetzliche Schranken berufen, wenn sie vollständige Werke und andere Schutzgegenstände in nicht abgewandelter Form auf Plattformen einstellen. Die Nutzerfreiheit wird daher nur geringfügig eingeschränkt, wenn der Filter den Upload eines Inhalts verhindert, der vollständig mit einem vom Rechteinhaber hinterlegten und nicht lizenzierten Schutzgegenstand übereinstimmt. Hier bleibt zwar das Problem des *Copyfrauds*, also des unberechtigten Berühmens von Urheberrechten. Dem könnte der Gesetzgeber aber durch entsprechende Sanktionen vorbeugen.[34] Auch Plattformbetreiber sollten ermächtigt und ggf. verpflichtet

[34] *Spindler* CR 2020, 50 (55).

werden, Sanktionen gegen *Copyfrauds* zu ergreifen, die in der Vergangenheit Rechte geltend gemacht haben, die ihnen nicht oder nicht in dem Umfang zustanden (dazu auch unten 2.b).[35]

Wenn Uploadfilter allerdings nur bei 1:1-Kopien eingreifen würden, wäre es ein Leichtes, sie zu umgehen. Deswegen müssen auch leicht gekürzte, gespiegelte, verzerrte Bilder, Videos oder andere Schutzgegenstände von den Systemen erkannt werden (oben III.3.). Maßgeblichen Einfluss auf die Nutzerrechte hat dann die Festlegung der entsprechenden Schwellenwerte.

[35] Alternativ können die Grundsätze der unberechtigten Schutzrechtsverwarnung herangezogen werden, *F. Hofmann* GRUR 2019, 1219 (1228) m. w. N.

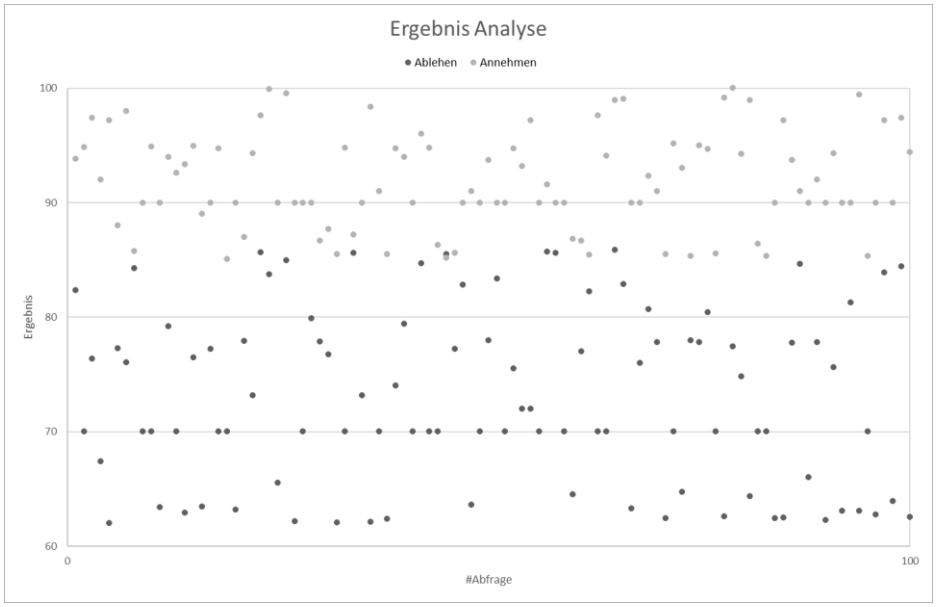

Abbildung 3: Beispiel Schwellwertberechnung für Werte zwischen 60 und 100. Die schwarzen Punkte sollten abgelehnt, die grauen Punkte erkannt werden. An welchem Wert soll die Grenze zwischen Ablehnen und Annehmen verlaufen?

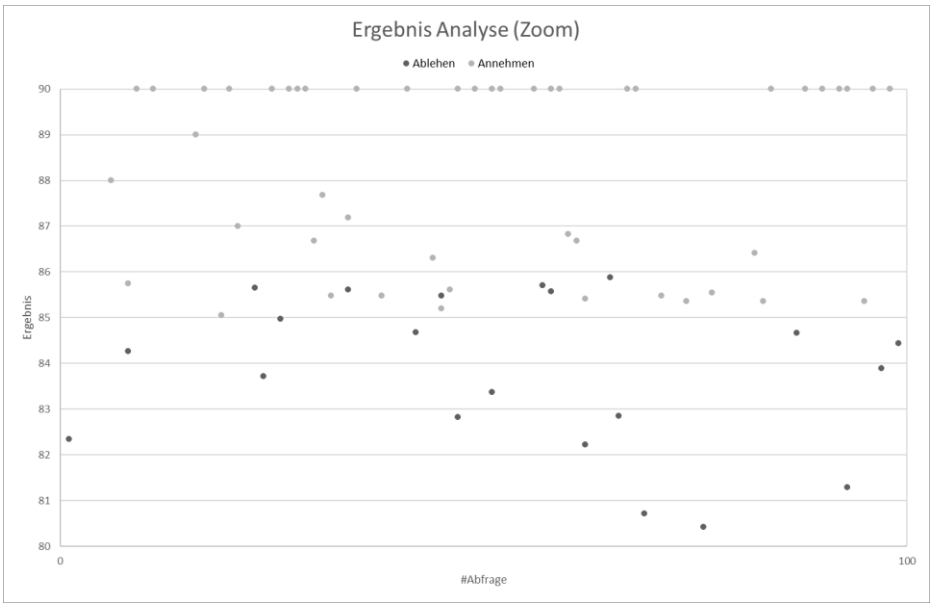

Abbildung 4: Es existiert kein Wert, zu dem alle Abzulehnenden kleiner und alle Anzunehmenden größer/gleich sind. Das wäre ein perfekter Schwellwert. In der Praxis gilt aber: Niedriger Schwellwert = viele falsch Positive, hoher Schwellwert = viele falsch Negative.

Es muss dem System vorgegeben werden, welche Abweichungen vom hinterlegten Hashwert eine Upload-Blockade auslösen und ab wann Ähnlichkeiten entweder hingenommen werden oder aber zusätzliche Prüfungen durch den Rechteinhaber bzw. Mitarbeiter des DTO auslösen müssen (dazu unten 2.a).

Hier liegt eine entscheidende Stellschraube für den Gesetzgeber und für Gerichte. So können beispielsweise für die Schwellenwerte der Filter Vorgaben dahingehend gemacht werden, dass diese nur einen bestimmten Prozentwert an false positives, also fälschlicherweise als Rechtsverletzung identifizierte Uploads, auswerfen dürfen. Zudem könnte den DTO aufgegeben werden, ihre Schwellenwerte regelmäßig zu überprüfen und bei zu vielen false positives die Schwellenwerte anzupassen.

2. Reaktionsalternativen des Uploadfilters

Wie oben dargestellt, darf man sich Uploadfilter nicht als binäre Systeme vorstellen, die entweder den Upload blockieren oder zulassen (oben III.2.). Sie sind zu differenzierten Reaktionen in der Lage und können daher so verwendet werden, dass sie Nutzerbeeinträchtigungen so gering wie möglich halten und trotzdem den Rechteinhabern effektive Reaktionsmöglichkeiten zur Verfügung stellen.[36]

a) Ausmaß der Übereinstimmung

Zunächst kann man die Reaktion des Uploadfilters von dem Ausmaß der Übereinstimmung zwischen hinterlegtem und hochgeladenem Gegenstand abhängig machen.[37] So kann eine automatische Herausfilterung gegebenenfalls nur bei eindeutigen oder sehr hohen Übereinstimmungswerten gerechtfertigt sein, die nur wenige false positives ausgeben, bei niedrigeren Schwellenwerten mit vielen false positives dagegen nicht. In letzterem Fall kann es eine angemessene Reaktion sein, dass sowohl dem Uploader als auch dem Rechteinhaber lediglich mitgeteilt wird, dass ein hochgeladener Gegenstand Ähnlichkeiten mit einem hinterlegten Schutzgegenstand aufweist. Beiden kann dann die Möglichkeit zur Stellungnahme gegeben werden.

b) Person des Uploaders bzw. des Rechteinhabers

Außerdem kann die Reaktion von der Person des Uploaders abhängig gemacht werden. So können Plattformen trusted user bestimmen, etwa Zeitungen oder Rundfunkanstalten, bei denen im Regelfall sichergestellt ist, dass ihre Inhalte lizenziert sind, oder Nutzer, die in der Vergangenheit keine Urheberrechtsverletzungen begangen haben.[38]

---

36 Vgl. auch *M. Becker* ZUM 2019, 636 (645).
37 Vgl. auch *Spindler* CR 2020, 50 (53).
38 *Spindler* CR 2020, 50 (53).

Umgekehrt kann es angemessen sein, dass Plattformen nach Kategorien von Rechteinhabern unterscheiden, wenn sie in der Vergangenheit Probleme mit Copyfrauds gehabt haben. Nach der Protokollerklärung der Bundesregierung soll es etwa erforderlich sein, dass der Rechteinhaber seine Berechtigung hinreichend belegen muss, solange er nicht als „trusted flagger" eingestuft werden kann.[39] Dann kann ein automatischer Uploadstopp nur bei vertrauenswürdigen Rechteinhabern gerechtfertigt sein, die über ein großes Repertoire und über einen seriösen Trackrekord verfügen.

c) Selbsteinschätzung des Uploaders

Darüber hinaus kann auch die Selbsteinschätzung des Uploaders ein Kriterium sein, das bei den Reaktionsmöglichkeiten des Systems berücksichtigt wird. Die Bundesregierung will laut ihrer Protokollerklärung zur DSM-RL über Verfahrensgarantien nachdenken, nach denen Nutzer beim Upload mitteilen können, dass sie den Inhalt erlaubterweise hochladen.[40] Wenn ein Upload als Parodie, Pastiche oder Zitat „geflagged" wird, kann es daher angemessen sein, den Upload vor der Sperrung erst dem Rechteinhaber zu melden oder von einem Mitarbeiter der Plattform überprüfen zu lassen.[41] Bei der Selbsteinschätzung von Nutzer und Rechteinhaber könnte zudem auf beiden Seiten berücksichtigt werden, ob sie sich in der Vergangenheit zu Unrecht auf Erlaubnistatbestände berufen bzw. deren Anwendbarkeit verneint haben.[42] Ein solcher delayed take down ist mit der Richtlinie vereinbar.[43]

d) Zeitkritikalität

Die Frage, ob ein umstrittener Inhalt als Grundreaktion von der Plattform entfernt werden oder weiter verfügbar bleiben soll, entscheidet über die weiteren Handlungslasten und damit in vielen Fällen faktisch darüber, ob ein Inhalt verfügbar ist oder nicht. Dies hat in einigen Fällen erheblichen Einfluss auf die Eingriffsintensität: Auf Seiten der Rechteinhaber ist ein Upload besonders belastend, wenn er die primäre Auswertung des Schutzgegenstandes beeinträchtigt, etwa wenn ein aktueller Kinofilm oder aktu-

---

39 Protokollerklärung, Nr. 8 (abrufbar unter: https://www.bmjv.de/SharedDocs/Downloads/DE/News/PM/041519_Protokollerklaerung_Richtlinie_Urheberrecht.pdf?__blob=publicationFile&v=1); *Spindler* CR 2019, 277 (286).

40 Protokollerklärung, Nr. 8 (abrufbar unter: https://www.bmjv.de/SharedDocs/Downloads/DE/News/PM/041519_Protokollerklaerung_Richtlinie_Urheberrecht.pdf?__blob=publicationFile&v=1).

41 *Spindler* CR 2019, 277 (290); *Dreier* GRUR 2019, 771 (777); *F. Hofmann* GRUR 2019, 1219 (1227 f.).

42 Vgl. dazu auch *F. Hofmann* GRUR 2019, 1219 (1228).

43 *Dreier* GRUR 2019, 771 (777); *F. Hofmann* GRUR 2019, 1219 (1228).

eller Hit hochgeladen werden soll. Hier ist eine Uploadblockade in größerem Umfang berechtigt als bei älteren Inhalten und dem long tail. Umgekehrt beeinträchtigt die Verhinderung des Uploads die Meinungsfreiheit in besonderem Maße, wenn ein Post zur Diskussion eines aktuellen Themas beitragen soll, etwa die Blockade eines Memes über einen Kandidaten in der heißen Phase eines Wahlkampfs oder das Verhindern eines Live-Streams.[44] Hier kann ein delayed take down geboten sein.[45]

e) Gefährdungspotential des hochgeladenen Inhalts

Nach Art. 17 Abs. 5 lit. a DSM-RL ist das Gefährdungspotenzial des hochgeladenen Inhalts zu berücksichtigen (s. o. unter IV.). Das kann als normativer Anknüpfungspunkt dafür herangezogen werden, dass Uploads großzügiger behandelt werden, solange sie nur wenig abgerufen werden. Solche Inhalte treten nur in geringem Ausmaß in Konkurrenz zu lizenzierten Angeboten der Rechteinhaber und beeinträchtigen deren Interessen also nur wenig. Es war aber Anliegen des Gesetzgebers, in erster Linie solche Plattformen und damit auch nur solche Inhalte zu erfassen, die mit den von den Rechteinhabern lizenzierten Online-Inhalte-Diensten um dieselben Zielgruppen konkurrieren (Erwgr. 62 S. 2 DSM-RL). Das ermöglicht, die Meinungs-, Kunst- und Informationsfreiheit in denjenigen Bereichen großzügiger zu behandeln, die die Interessen der Rechteinhaber weniger beeinträchtigen. Es kann daher angemessen sein, abgewandelte Inhalte (oben a)) jedenfalls solange nicht automatisch herauszufiltern, wie sie wenig abgerufen werden. Darüber hinaus kann es insbesondere für kleinere Plattformen die Kosten für die Filterung senken und damit die Zumutbarkeit erhöhen, wenn sie nicht alle ihre Inhalte (und insbesondere den long tail) filtern müssen, sondern nur solche, die bestimmte Schwellenwerte erreichen.

Auch kurze Musik- oder Filmausschnitte konkurrieren im Regelfall nicht mit der Hauptauswertung der Schutzgegenstände, so dass auch hier die automatische Uploadblockade unverhältnismäßig sein kann.[46]

---

44 Vgl. dazu *Gielen/Tiessen* EuZW 2019, 639 (645); *Senftleben* ZUM 2019, 369 (372 f.); *Weiden* GRUR 2019, 370 (371 f.) („Zensur qua Zeitablauf").

45 Vgl. *F. Hofmann* GRUR 2019, 1219 (1228).

46 Ähnlich *M. Becker* ZUM 2019, 636 (645).

V. Fazit

Uploadfilter sind nicht gleich Uploadfilter. Sie bestehen aus unterschiedlichen Komponenten[47] und sind je nach Medientyp unterschiedlich leistungsfähig[48]. Die unterschiedlichen Interessen von Rechteinhabern, Nutzern und Plattformbetreiber können durch die Einstellung der „Empfindlichkeit" des Uploadfilters[49] sowie durch dessen unterschiedliche Reaktionsmöglichkeiten[50] ausbalanciert werden. Dieser Beitrag versteht sich als Toolbox für Gesetzgeber und Gerichte. Er enthält Instrumente, die als Teil eines techniksensiblen Urheberrechts bei der Umsetzung von Art. 17 DSM-RL bzw. bei der Konkretisierung von dessen Verkehrspflichten und anderer unbestimmter Rechtsbegriffe eingesetzt werden können.

Eine erste entscheidende Weichenstellung kommt dem Ähnlichkeitsmaß und damit dem Schwellenwert zu, ab dem ähnliche, zum Upload vorgesehene Inhalte als Eingriff in den Schutzbereich eines hinterlegten Schutzgegenstands angesehen werden.[51] Anschließend kommt es auf die Reaktion des Uploadfilters an, weil nicht jede Ähnlichkeit eines Uploads mit einem hinterlegten Schutzgegenstand automatisch zu dessen Sperrung führen muss. Uploadfilter sind zu differenzierten Reaktionsmöglichkeiten in der Lage, die an folgende Kriterien anknüpfen können: das Ausmaß der Übereinstimmung zwischen hinterlegtem und hochgeladenem Gegenstand, die Person des Uploaders bzw. des Rechteinhabers, die Selbsteinschätzung des Uploaders, die Zeitkritikalität sowie das Gefährdungspotenzial des hochgeladenen Inhalts.[52]

---

47 Dazu III.2.
48 Dazu III.4.
49 Dazu IV.1.
50 Dazu IV.2.
51 Dazu IV.1.
52 Dazu IV.2.