Upload-Filter – Sinnhaftigkeit und Machbarkeit

Korrekt ins Netz

Der Plan ist klar nachvollziehbar und notwendig: Unrechtmäßig genutzte, urheberrechtlich geschützte oder gar illegale Inhalte dürfen im Internet keine Plattform zur Verbreitung finden. Bisher geschieht das durch Analyse bereits hochgeladener Inhalte. Die Europäische Union möchte aber am liebsten verhindern, dass entsprechendes Material überhaupt ins Netz gelangt. Das ruft sogenannte Upload-Filter auf den Plan, die bereits beim Versuch des Hochladens eine Blockade setzen. So weit, so gut, jedoch lassen sich durch solche Filter zu leicht auch „unliebsame" Inhalte blockieren – Kritikern solcher Pläne scheint ein Machtmissbrauch durch Kontrolle der zur Veröffentlichung freigegebenen Inhalte vorprogrammiert. Vor diesem Hintergrund beleuchtet folgender Beitrag den Sinn, die technische Umsetzung und Machbarkeit sowie die Risiken von Upload-Filtern.

Das Internet als weltweites Netzwerk von Servern dient schon lange nicht mehr rein der Beschaffung von Informationen oder der persönlichen Kommunikation. Es werden vermehrt mediale Inhalte (Bilder, Audio- und Videodateien) in sozialen Netzwerken gepostet. Ein Großteil dieser Inhalte dient der Selbstdarstellung des Nutzers in Chroniken, Timelines, Stories etc. Allein auf Facebook werden pro Tag etwa 350 Millionen Bilder und 100 Millionen Stunden Videomaterial von Nutzern hochgeladen.[1] Bei YouTube sind es sogar 400 Stunden Videomaterial pro Minute.[2]

In dieser Masse von Daten sind auch unrechtmäßig genutzte, urheberrechtlich geschützte oder illegale Inhalte vorhanden. Diese unerwünschten Inhalte können mit voller Absicht oder aus Versehen und ohne kriminellen Hintergedanken hochgeladen werden. Doch egal aus welchem Grund, solche Inhalte müssen so früh wie möglich entdeckt und gelöscht werden oder sollten gar nicht erst hochgeladen werden können. Aktuelle Lösungen basieren auf einer nachträglichen Erkennung bereits hochgeladener Inhalte durch Erkennungswerkzeuge oder den Menschen. Dieses Vorgehen ist bereits etabliert und allseits anerkannt. Eine Erweiterung durch gesetzliche Vorgaben, die das Melden, Deaktivieren und Prüfen vereinfacht und beschleunigt, wäre hier ein logischer nächster Schritt. Doch eine Prüfung und Bewertung aller Inhalte von Uploads während des Upload-Prozesses in Echtzeit wird zurzeit favorisiert und stellt eine neue, besondere Herausforderung dar. Daher könnten in Zukunft Upload-Filter weltweit zum Einsatz kommen. Bild 1 zeigt schematisch den Unterschied zwischen einem Upload ohne Upload-Filter – links unten – und einem Upload mit Upload-Filter

Bild: ©depositphotos.com/wowomnom

– links oben. Hierbei ist die Verbindung des Upload-Filters mit dem Internet nicht obligatorisch.

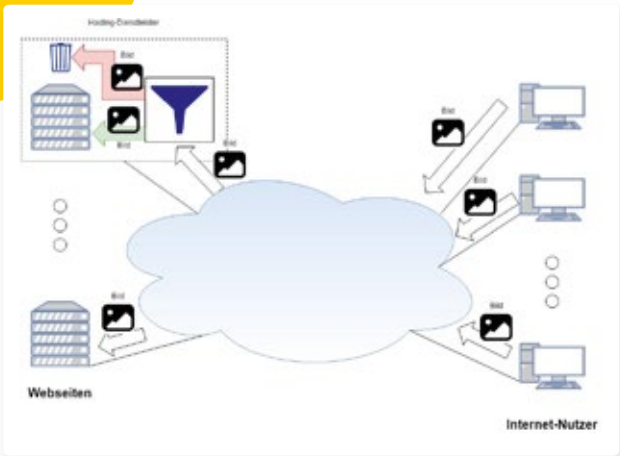


Bild 1 Konzeptionelle Darstellung eines Upload-Prozesses mit und ohne Filter. (Quelle: ifis)

Ein Upload-Filter wird als eigenständige, unumgängliche Instanz in den Upload-Prozesses integriert. Seine Aufgabe besteht in der Klassifizierung der Inhalte von Uploads. Kriterien hierfür sind vor allem das Bestehen eines Urheberschutzes für den Upload von Musik, Bildern oder Filmen, und ein eventueller Konflikt mit dem Strafrecht – zum Beispiel Kinderpornografie oder Rassismus.

Vorangetrieben wurde das Thema von der EU – genauer durch die Richtlinie (EU) 2019/790. Der hierin enthaltene Artikel 17 sieht vor, die Plattformen zu verpflichten, Lizenzverträge mit den Inhabern von Urheberrechten zu schließen. Kommen diese nicht zustande, muss die Plattform dafür sorgen, dass entsprechende Inhalte nicht hochgeladen und veröffentlicht werden können. Dieser Artikel war und ist immer noch hoch umstritten. Die EU will damit die unerlaubte Nutzung urheberrechtlich geschützter Werke auf Webseiten verhindern. Kritiker sehen darin das freie Internet durch eine Zensurmöglichkeit in Gefahr, sollte eine diktatorische Regierung Einfluss auf die Upload-Filter haben.

Ein Jahr zuvor hat die EU bereits eine Handlungsempfehlung für wirksame Maßnahmen im Umgang mit illegalen Online-Inhalten herausgebracht. Die Empfehlung (EU) 2018/334 sieht in ihren Punkten 18 bis 20 den Einsatz von proaktiven Maßnahmen als auch die Sicherstellung der Fehlerfreiheit eines solchen Upload-Filters vor. Hierzu soll die negative Bewertung eines Uploads durch eine solche automatisierte Maßnahme mit einer menschlichen Nachkontrolle bestätigt oder revidiert werden.

Diese beiden Dokumente skizzieren die Aufgaben von Upload-Filtern jedoch nur grob. Es soll ein Upload-Filter zur Bewertung und Klassifizierung von allen Inhalten realisiert werden, welche auf eine Plattform hochgeladen werden. So soll eine unerlaubte Nutzung urheberrechtlich geschützter Werke oder illegaler Inhalte auf Plattformen verhindert werden. Da zur konkreten Umsetzung keine Aussagen getroffen werden, erstreckt sich die Spanne der möglichen Technologien zur Bewertung von einem einfachen Hashwert-Vergleich bis zur künstlichen Intelligenz. Auch eine topologische Anordnung oder ein Betreibermodell wird nicht thematisiert.

Ziele von Upload-Filtern

Die allgemeinen Ziele von Upload-Filtern betreffen die spezifischen Aufgaben und die notwendigen IT-Systeme. Dabei gelten folgende Aspekte:

Fehlerfreiheit

Der Upload-Filter muss die Masse von Uploads nicht nur bewältigen können, sondern bei der Bewertung auch korrekte Ergebnis erzielen. Eine nominal kleine Fehlerquote mag als ausreichend erscheinen, aber angesichts riesiger Datenmengen bleiben dennoch in absoluten Zahlen sehr viele Fehlbewertungen. Um das Beispiel von Facebook noch einmal aufzugreifen: Eine Fehlerquote von nur 1 Prozent bedeutet, dass immer noch 40 Bilder pro Sekunde falsch eingeordnet werden. Hierbei muss zwischen False Positives (FP) und False Negativs (FN) unterschieden werden. Nehmen wir ein Verhältnis FP:FN als 50:50 an. Da jedes negativ bewertete Bild händisch nachkontrolliert werden muss, um nachträglich freigeschaltet werden zu können, ist der personelle Aufwand sehr groß. Doch ein positives Ergebnis hat eine sofortige Freigabe eines Uploads zur Folge. Somit werden pro Sekunde etwa 20 Bilder freigegeben, die eigentlich als negativ hätten bewertet werden müssen. Das sind auf einen Tag hochgerechnet gut 1,7 Millionen Bilder. Aus diesem Grund muss die Fehlerquote sehr viel besser sein als 1 Prozent. Andernfalls macht das Verfahren keinen Sinn.

Hochverfügbarkeit

Der Upload-Filter muss 24/7 volle Leistung bringen können, um einen Datenstau zu vermeiden. Ein vollständiger oder teilweiser Ausfall des Filters schwächt das gesamte Web-System. Jedoch ist das Problem der Hochverfügbarkeit von Diensten oder Ins-

tanzen in der Informatik nicht neu. Hier kann auf bereits bestehende Lösungen zurückgegriffen werden – Redundanz, Fehlertoleranz etc.

Performance

Der eingesetzte Upload-Filter darf keine Verzögerung im Upload-Prozess verursachen. Viele mediale Inhalte werden gepostet, um eine aktuelle Situation zu teilen. Eine Verzögerung durch einen Upload-Filter wäre hier nicht akzeptabel für die Nutzer. Der Upload-Filter muss auf die jeweilige Menge der zu erwartenden Uploads ausgelegt sein. Zum Beispiel müssen alle Upload-Filter von Facebook etwa 4.000 Bilder und 1.150 Stunden Videomaterial pro Sekunde analysieren und bewerten können. Anderenfalls bildet sich ein stetig wachsender „Datenstau".

Neutralität

Der Upload-Filter trifft die Entscheidung, ob ein Upload zugelassen wird oder nicht. Doch wer bringt dem Upload-Filter bei, was erlaubt ist und was nicht? Es muss sichergestellt werden, dass sich die Entscheidungen an allgemeinen, objektiven, gesetzlichen und ethischen Regelungen orientieren und nicht an subjektiven Ansichten von Personen, Unternehmen oder Staaten.

Sicherheit

Ein Upload-Filter soll das Internet sicherer, besser und vertrauenswürdiger machen. Doch auch der Upload-Filter selbst muss sicher umsetzt werden, um Manipulationen zu vermeiden. Schutzziele, wie Integrität, Authentizität und Vertraulichkeit, sind allgemein bekannt und werden hier nicht weiter beleuchtet. Sie dürfen jedoch nicht außer Acht gelassen werden. Ein Upload-Filter stellt aufgrund seiner zentralen Position und der Vorhaltung der Vergleichsdaten ein attraktives Ziel für Angreifer dar. Eine Manipulation der Bewertung oder der Vergleichsdaten beeinflusst, was der Upload-Filter durchlässt und was nicht.

Umsetzung eins Upload-Filters

Bei der Umsetzung eins Upload-Filters kommt es nicht auf die Neuentwicklung von Technologien oder Konzepten an, sondern vielmehr auf eine geeignete Kombination bereits vorhandener Lösungen. So besteht ein Upload-Filter im Kern aus der Technologie zur Bewertung der Inhalte von Uploads, der Technologie zur Vorhaltung von Vergleichsdaten und der sicheren Kommunikation dieser beiden Komponenten. Eine leistungsstarke IT-Infrastruktur spielt ebenfalls eine wichtige Rolle. Die Vergleichsdaten müssen von den zuständigen Quellen bereitgestellt, ständig aktualisiert und zur Datenbank transportiert werden. Außerdem muss der Upload von der Plattform oder direkt vom Uploader zum Filter hin und das Ergebnis vom Filter zur Plattform transportiert werden.

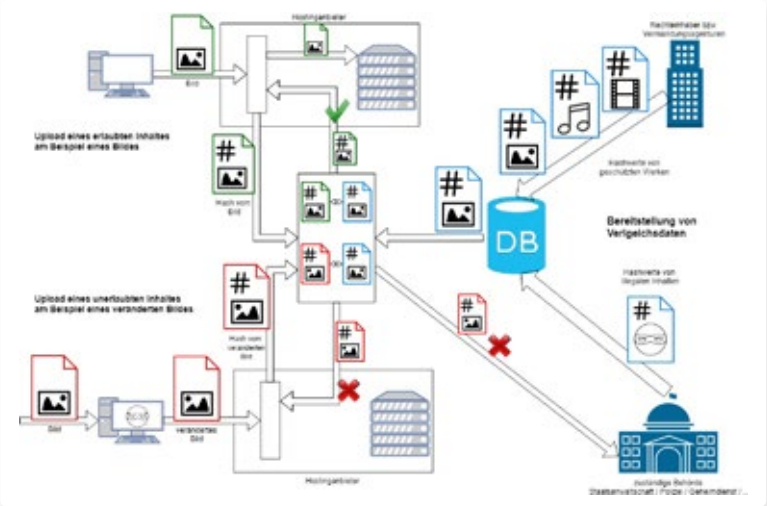


Bild 2: Ablauf von jeweils einem erlaubten – oben links – und einem unerlaubten Upload – unten links. (Quelle: ifis)

Erkennen von nicht gewünschten Inhalten

Der Filter soll die hochgeladenen Inhalte bewerten und entsprechend klassifizieren. Sowohl diese Aufgaben als auch die entsprechenden Lösungen sind in der Informatik nicht neu. Das Bewerten und gegebenenfalls Wiedererkennen von Daten ist eine bekannte Aufgabenstellung. Hierzu werden Hashwerte oder digitale Fingerabdrücke für diese Daten erstellt. Die Hashwerte sind in der Praxis eindeutig. Dass jedoch ein kleiner Unterschied in der Eingabe bei einer Hashwert-Funktion immer einen sehr großen Unterschied im Ergebnis hat, ist eine wichtige und gewollte Eigenschaft, wenn es rein um den Vergleich auf exakte Gleichheit von Daten geht. Ein Upload-Filter soll aber auch in der Lage sein, leichte Veränderungen des Uploads im Vergleich zu den bereits bekannten Daten zu entdecken. Dies ist mit einer gängigen Hash-Funktion nicht möglich.

Erkennen von bekannten ungewünschten Inhalten

Microsoft hat zum Beispiel mit seinem Algorithmus PhotoDNA eine Lösung für diese Aufgabenstellung. Bei der PhotoDNA-Lösung wird ein Farbbild zuerst in ein Schwarz-Weiß-Bild überführt, um Farbveränderungen unwirksam zu machen. Anschließend wird ein Raster über das Bild gelegt und für jede Einheit ein einzelner Hashwert berechnet. Die Verknüpfung aller Hashwerte ergibt dann die „DNA" des Bildes. So will Microsoft auch Veränderungen oder ein bekanntes Muster in einem anderen Bild finden.[3] Auch YouTube hat mit „Content ID" einen eigenen Algorithmus entwickelt, um Urheberrechtsverstöße zu finden. Zu jedem hochgeladenen Video im Upload-Filter wird ein digitaler Fingerabdruck erstellt und mit den bereits abgespeicherten Fingerabdrücken anderer Videos im Upload-Filter verglichen. Wird das Video akzeptiert, wird der Fingerabdruck gespeichert. Andernfalls bekommt zurzeit der rechtmäßige Eigentümer des Inhaltes eine Benachrichtigung über den Verstoß und kann das weitere Verfahren bestimmen.[4] Beide Algorithmen sind auf das

Wiedererkennen bereits gesehener Inhalte ausgelegt. Noch unveröffentlichte Inhalte können bei diesen Verfahren nicht berücksichtigt werden.

Erkennen von noch nicht bekannten Inhalten

Illegale Inhalte sind oft noch unbekannt und müssen trotzdem als illegal eingestuft werden können. Eine entsprechende Identifizierungstechnologie nutzt zum Beispiel neuronale Netze für die Bewertung von Inhalten. Die neuronalen Netze werden mit einer Menge von Daten trainiert. Die darin entdeckten Muster werden in Form von Verbindungen zwischen einzelnen Knoten des Netzes dargestellt. Auch neuronale Netze produzieren keine hundertprozentigen Antworten, aber eine sehr starke Tendenz.

Auch eine Kombination aus digitalen Fingerabdrücken und der Identifizierung mit neuronalen Netzen ist denkbar. So könnte ein neuronales Netz die Eingabe aufbereiten und sie in eine „Normalform" bringen. Anschließend kann sie einfacher und vor allem aussagekräftiger mit einem digitalen Fingerabdruck versehen und verglichen werden.

Ein weiterer wichtiger Punkt sind die Daten, auf deren Grundlage die Bewertung unabhängig von der verwendeten Technologie erfolgen soll. Diese Vergleichsdaten dienen entweder als direkter Vergleich für digitale Fingerabdrücke oder als Trainingsdaten für neuronale Netze. Bereitgestellt werden sie von unterschiedlichen Parteien. An der Wahrung des Urheberschutzes haben die Rechteinhaber beziehungsweise deren Vermarktungsgesellschaften ein finanzielles Interesse. Ihr Anliegen ist daher, die Vergleichsdaten zu ihren eigenen Werken permanent zu aktualisieren. Für illegale Inhalte sind die Staatsanwaltschaften, Polizei und Geheimdienste zuständig, also auch für die Bereitstellung entsprechender Vergleichsdaten.

Ein weiterer Punkt ist der Speicherort der Vergleichsdaten. Hier gibt es zwei Ansätze: Filter und Datenbank bilden eine Einheit, oder sie sind getrennt. Gehören sie nicht zusammen, sind sie zumindest räumlich, wenn nicht sogar organisatorisch getrennt. Eine räumliche Trennung ist immer mit dem Risiko einer unzuverlässigen Kommunikation verbunden. Auch steigt dadurch der Traffic – sowohl für den Filterbetreiber als auch für das Internet. Außerdem würde hier der Prozess des Filterns auseinandergerissen werden. Das Erkennen des Inhalts und das Abgleichen mit den Vergleichsdaten sollten jedoch als zusammengehörig betrachtet werden. Gehören Filter und Datenbank nicht zum selben Unternehmen, ist der Betreiber des Filters ein Kunde des Betreibers der Datenbank. In diesem Fall ist die Datenbank ein geteiltes Medium und wird von anderen Kunden ebenfalls genutzt, was zu Verzögerungen in der Bearbeitung führen kann. Daher gehen wir im weiteren Verlauf davon aus, dass sich Filter und Datenbank sowohl in räumlicher als auch organisatorischer Nähe befinden und als Einheit betrachtet werden. Somit besteht eine sichere und zuverlässige Kommunikation sowie volle Kontrolle über die Datenbank.

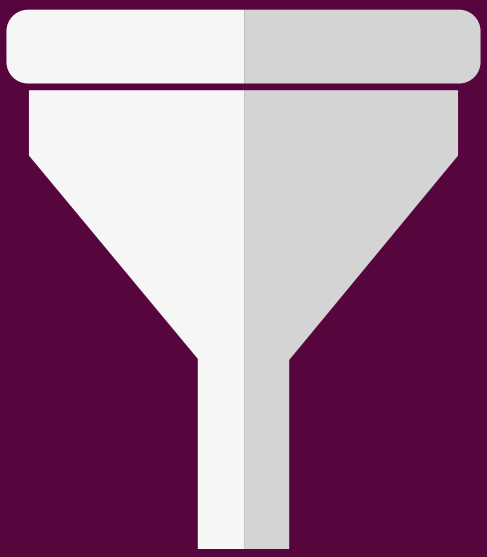
Doch neben der topologischen Anordnung der Datenbank gilt es auch, sich mit der Positionierung des Filters zu beschäftigen. Dieser muss in die bereits bestehende Infrastruktur des World Wide Web integriert werden. Somit werden bestehende Endpunkte um einen Filter erweitert, oder es entstehen neue Endpunkte. Die Erweiterung eines bestehenden Endpunktes hat einen dedizierten Filter zur Folge. Der Filter ist einer Plattform direkt zugeordnet. Diese hat dann sowohl die volle Kontrolle als auch die alleinige Verantwortung für den Betrieb, und Einhaltung der Anforderungen und Ziele. Das Gegenteil

wäre ein geteilter Filter. Hierbei könnte es sich um einen externen Anbieter handeln, bei dem die Plattform als Kunde für die Filter-Dienstleistung bezahlt. Somit werden die Kosten pro Plattform reduziert und die Verantwortung vollständig ausgelagert.

Doch der Preis ist der Kontrollverlust über die Verarbeitung der Uploads der eigenen Nutzer. Des Weiteren würden auch hier die Uploads erneut durch das Internet transportiert werden. Dabei ist es egal, ob die Plattform die Daten selbstständig zum Filter schickt oder die Umleitung bereits im Upload-Formular integriert. Der Upload muss in voller Qualität mindestens zweimal über das Internet versendet werden, zuzüglich der Entscheidung des Filters. Damit wird die Belastung durch mediale Inhalte für das Internet verdoppelt. Sollte der Upload von der Plattform aus zum Filter weitergeleitet werden, steigt ebenfalls der Traffic für die entsprechende Plattform signifikant. Gerade bei kleineren Plattformen möglicherweise ohne eigene Server muss hierbei auf die Anbindung geachtet werden, damit die Anwendung nicht zum Flaschenhals wird.

Eine Beispielrechnung soll das Problem noch verdeutlichen

Ein Bild mit 2 MByte wird zum Server geladen. Dies dauert bei einem 100-MBit/s-Anschluss beim Client und einem 1-GBit/s-Anschluss am Server etwa 0,18 Sekunden. Das Weitersenden eines lediglich 256 Byte großen Hashwertes zum Filter dauert weitere etwa 6 Millisekunden. Die Verarbeitung im Filter wird auf eine Sekunde geschätzt. Das Zurücksenden der Antwort von angenommenen 1 KByte nimmt weiter 6 Millisekunden in Anspruch. Somit dauert der gesamte Upload-Prozess über eine Sekunde. Nach Schätzungen werden pro Tag rund 7 Milliarden Bilder hochgeladen. Das bedeutet, ein einziger Filter ist etwa 978 Tage mit den Bildern belegt, die in nur einer Sekunde weltweit hochgeladen werden. Diese Rechnung und die Tatsache, dass neben Bildern auch Musik und Videomaterial in ähnlichen Größenordnungen hochgeladen werden, führt zu dem Schluss, dass die Zahl der Upload-Filter weltweit immens hoch sein muss.



Notwendigkeit von Upload-Filtern

Die Umsetzung eines Upload-Filters gestaltet sich offensichtlich als sehr umfangreich und aufwendig. Das rückt die Frage nach der Notwendigkeit verstärkt ins Licht. Die EU begründet im Kern die Notwendigkeit dieser Richtlinie mit der Anpassung von Regelungen an den aktuellen Stand der Technik, der Schließung von Gesetzeslücken und der Wahrung des Rechteverhältnisses zwischen Urheberrechtsinhaber und Nutzern.

Um diese Argumente zu unterstreichen, hat die EU ein Papier zu Filmpiraterie herausgebracht.[6] Hierin stellt sie dar, dass legale Käufe von Filmen ausbleiben, weil sie auf illegalen Wegen heruntergeladen oder gestreamt werden. Die negative Verdrängungsrate beträgt hier laut Papier etwa 27 Prozent. Das bedeutet, dass pro 100 illegal gesehenen Filmen 27 Mal ein legaler Umsatz ausgeblieben ist – also verdrängt wurde. Hierbei bezieht sich die EU auf eine selbst in Auftrag gegebene Studie, welche eben solche Verdrängungseffekte repräsentativ auf EU-Ebene untersuchen sollte.[5] Eben diese Studie stellt eine negative Verdrängungsrate von 27 Prozent bei Filmen fest. Doch ist das lediglich der Durchschnitt. Bei Blockbustern gibt es hingegen eine positive Verdrängungsrate von 40 Prozent. Also zehn illegal geschaute Filme führen zu vier legalen Käufen. Bei Musik ist die Verdrängungsrate bei 0 Prozent, da die früheren Raubkopien von physischen Tonträgern durch Aufzeichnung oder Live-Streams von Konzerten abgelöst wurden. E-Books leiden ebenfalls unter einer negativen Verdrängungsrate. Hier liegt sie bei 38 Prozent. Da E-Books aber insgesamt einen sehr geringen Marktanteil haben, kann dieses Feld vernachlässigt werden. Spiele verzeichnen eine durchweg positive Verdrängungsrate von etwa 24 Prozent.

Beide positiven Verdrängungsraten können ein Indiz für eine gute Marketingstrategie sein. Der Film beziehungsweise das Spiel wird zum Kennenlernen kostenlos herausgegeben. In beiden Fällen werden anschließend Käufe angeregt. Daher ist in diesen Fällen der illegale Konsum geduldet. Alles in allem kann diese Studie keine Notwendigkeit für Upload-Filter bestätigen!

Auch das Max-Planck-Institut hat in einer Studie das Verhalten von ca. 5.500 Deutschen in Bezug auf die Nutzung von

kreativen Online-Inhalten untersucht.[7] Hier wurde die jeweils letzte Nutzung von Online-Inhalten betrachtet und festgestellt, dass deutlich mehr kostenfreie als kostenpflichtige Angebote genutzt wurden. Gründe hierfür sind Bequemlichkeit, Ausprobieren vor dem Kauf oder einfach die bloße Möglichkeit, es zu können. Auch die Bereitschaft, für solche Online-Inhalte zu bezahlen, schwindet. Gründe hierfür sind unter anderem ein zu hoher Preis, fehlende legale Quellen, nicht ausreichende Kennzeichnung illegaler Nutzung oder auch das geringe Risiko erwischt zu werden. Auch diese Studie kann keine Notwendigkeit weiterer gesetzlicher Regelungen feststellen. Hingegen sei es besser, die bestehenden Gesetze und rechtlichen Sanktionsmöglichkeiten effizienter zu nutzen.

Risiko von Upload-Filtern

Mit Upload-Filtern besteht das Risiko, dass diese zu einem groß angelegten Zensurwerkzeug umfunktioniert werden. Da ein Upload-Filter bei jedem Upload passiert werden muss, kommt diesem eine zentrale Rolle zu. Bekommt ein diktatorisches Regime Zugriff auf den/die Upload-Filter im eigenen Land, können so zum Beispiel politische Gegner klein gehalten oder sogar vollständig unterdrückt werden. Auch große Plattformen mit eigenem Upload-Filter können in eine ähnliche Situation kommen. Vor allem dann, wenn sie nicht nur Uploads auf der eigenen Plattform analysieren, sondern auch als Dienstleister für andere kleinere Plattformen arbeiten. Auf diese Art und Weise kann auch ein einzelnes Unternehmen als Zensor auftreten.

Doch was sind die möglichen Alternativen zu Upload-Filtern? Wie eingangs erwähnt, werden bereits heute Inhalte analysiert und gegebenenfalls deaktiviert oder gelöscht. Hier könnte mit einer höheren Automatisierung des Prozesses ein besseres Ergebnis bei notwendigen Löschungen erzielt werden. Die Risiken, mit welchen Upload-Filter behaftet sind, kommen so gar nicht erst auf.

Fazit

Insgesamt lässt sich festhalten: Upload-Filter sind und bleiben eine Herausforderung. Nicht nur die Umsetzung von Upload-Filtern gestaltet sich technisch und konzeptionell schwierig. Auch eine objektive Notwendigkeit lässt sich nicht lückenlos begründen.

Beginnend mit der verwendeten Technologie zur Bewertung der Daten steht schon die erste essenzielle und nicht einfache Entscheidung an. Für eine Identifizierung von gleichen oder stark ähnlichen Inhalten urheberrechtlich geschützter Werke reichen angepasste Algorithmen zur Berechnung robuster digitaler Fingerabdrücke. Illegale Inhalte indes folgen bestimmten Mustern, die auf der Basis von modernem maschinellem Lernen mit neuronalen Netzen mit immer größerer Wahrscheinlichkeit gefunden werden können. Doch eine Kombination aus beidem sollte ebenfalls in Betracht gezogen werden. Als nächstes muss das Betreibermodell festgelegt werden – die Filter-Plattform selbst betreiben oder als Filter-as-a-Service. Beide Modelle haben ihre Vor- und Nachteile, und die Entscheidung muss jede Plattform selbst treffen. Unabhängig von den getroffenen Entscheidungen besteht immer das Risiko, dass ein Upload-Filter zum Werkzeug für Zensur wird. Neben der Entscheidungsfindung über die konkrete Umsetzung ist die Diskussion über die Notwendigkeit und die weit auseinandergehenden Meinungen besonders wichtig. Hier besteht noch viel Bedarf für Diskussionen, Auseinandersetzungen und Kompromisse, um eine angemessene Lösung zu etablieren. ■

Literatur

[1] *Kit Smith: „Facebook in Zahlen: 53 interessante Statistiken", unter: https://www.brandwatch.com/de/blog/facebook-statistiken/ (aufgerufen am 16.09.2019)*

[2] *Kit Smith: „52 interessante Zahlen und Statistiken rund um YouTube", unter: https://www.brandwatch.com/de/blog/statistiken-YouTube/ (aufgerufen am 16.09.2019)*

[3] *Jan-Peter Kleinhans: „DNA und Tagesdecken im Kampf gegen Kindesmissbrauchs-Dokumentation Online", unter: https://netzpolitik.org/2013/dna-und-tagesdecken-im-kampf-gegen-kindesmissbrauchs-dokumentation-online/ (aufgerufen am 30.09.2019)*

[4] *YouTube: „So funktioniert Content ID"; unter: https://support.google.com/YouTube/answer/2797370?hl=de (aufgerufen am 30.09.2019)*

[5] *Martin van der Ende, Joost Poort, Robert Haffner, Patrick de Bas, Anastasia Yagafarova, Sophie Rohlfs, Harry van Til; „Estimating displacement rates of copyrighted content in the EU – Final Report"; published: 05/2015*

[6] *Benedikt Herz und Kamil Kilijanski: „Movie Piracy and Displaced Sales in Europe: Evidence from Six Countries"; published 09/2016*

[7] *Dietmar Harhoff, Reto M. Hilty, Roland A. Stürz, Alexander Suyer: „Nutzung urheberrechtlich geschützter Inhalte im Internet durch deutsche Verbraucher – Ergebnisübersicht einer repräsentativen quantitativen Erhebung"*

TOBIAS SPIELMANN
studiert im Master Internet-Sicherheit am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit Upload-Filtern.

NORBERT POHLMANN,
Informatikprofessor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.