Westfälische Hochschule - Gelsenkirchen Bocholt Recklinghausen - 45877 Gelsenkirchen

Studiengang: M. Sc. Internet-Sicherheit

Sommersemester 2019

3. Fachsemester

Upload-Filter

Masterseminar

Abgabedatum:

2. August 2019

Aktualisierungsdatum:

2. August 2019

Autor:

Tobias Spielmannn (Matr. 201222808) – tobias.spielmann@studmail.w-hs.de

Betreuer:

Prof. N. Pohlmann

Inhaltsverzeichnis

1 Einführung

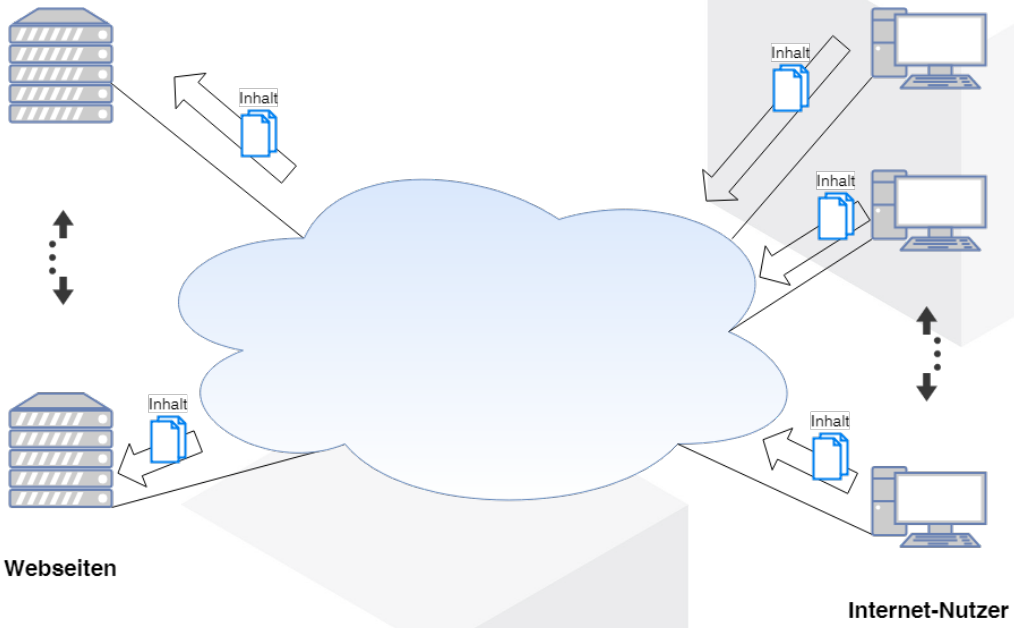

Abbildung 1: Upload ohne Filter

Das Internet als weltweites Netzwerk von Servern dient schon lange nicht mehr rein zur Beschaffung von Informationen oder persönlichen (1:1-) 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, Stroies etc. Alleine auf Facebook werden pro Tag ca 350 Mio. Fotos und 100 Mio Std. Videos von Usern hochgeladen.Smith [2019b] Und bei Youtube sind es sogar 400 Mio. Std. pro Tag. Smith [2019a] In dieser Masse von Daten befinden sich nicht wenige urheberrechtlich geschützte oder illegale Inhalte. Diese werden entweder mit voller Absicht oder aus Versehen und ohne kriminellen Hintergedanken hochgeladen. Doch egal aus welchem Grund, solche Inhalte müssen so früh wie möglich entdeckt und dürfen am besten gar nicht erst freigeschaltet werden. Bereits hochgeladene Inhalte werden auch heute schon durch Erkennungswerkzeuge oder aufmerksame menschliche Nutzer gefunden und gemeldet. Doch eine Prüfung und Bewertung beim Upload-Prozess in Echtzeit stellt eine neue Herausforderung dar. Hierbei kämen sogenannte Upload-Filter zum Einsatz.

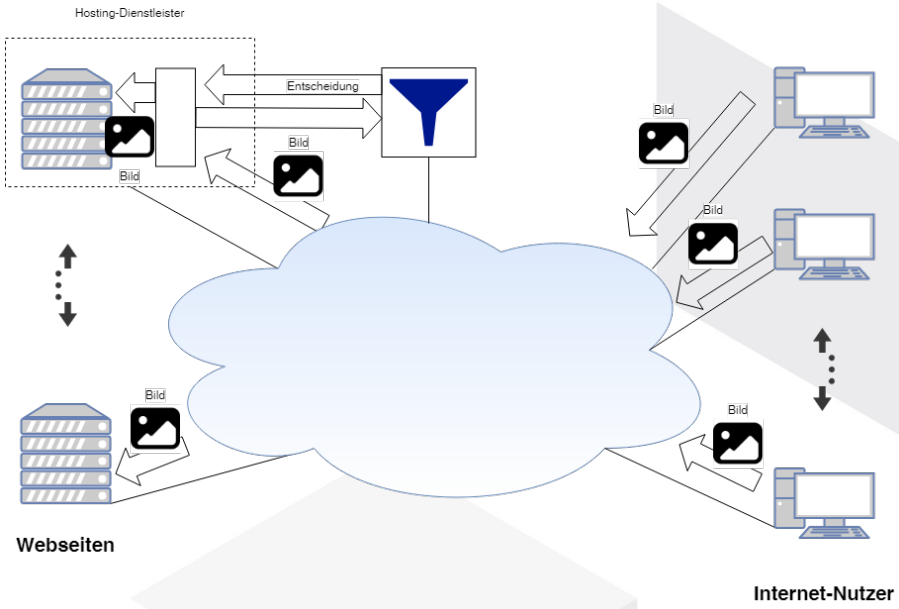

Abbildung 2: Upload mit Filter

1.1 Was ist ein Upload-Filter?

Unter Upload-Filtern versteht man in der Regel automatisierte Systeme zur Prüfung von Inhalten vor bzw. während des Upload-Vorgangs. Auf Grund der Flut an Inhalten, welche täglich hochgeladen werden, besteht keine Möglichkeit mehr diese adäquat von Hand prüfen zu können.

- Doch was für Daten sind das überhaupt, die da geprüft werden müssen?
- Wo kommen diese her?
- Und wie kann man möglichst effizient und korrekt diese Daten bewerten?

Diese Fragen sind ausschlaggebend für eine neutrale Bewertung von Upload-Filtern und deren Umsetzung. Die Art der zu bewertenden Inhalte lässt auch direkt auf deren unterschiedliche Herkunft und Brisanz schließen. Herausgefiltert werden sollen auf der einen Seite urheberrechtlich geschützte Werke und auf der Seite strafrechtlich illegale Daten. Beide Arten stammen aus unterschiedlichen Quellen und verdienen jeweils eine unterschiedliche Behandlung. So kann unter Anderem bei urheberrechtlich geschützten Werke auch ein sehr ähnliches Werk herausgefiltert werden, wohingegen die leichte Veränderung eines illegalen Inhaltes eine von Grund auf neue Bewertung nötig machen kann.

Hieraus ergibt sich sofort die Notwendigkeit von zwei verschiedenen Technologien zur Bewertung der Uploads. Geschützte Werke können mit intelligenten Algorithmen erkannt und somit auch resistent gegen leichte Veränderungen sein, während illegale Inhalte nur gegen bereits bekannte Vergleichsinhalte im 1:1-Vergleich geprüften werden können.

Jedoch nicht nur die notwendigen Technologien mit ihren Vor- und Nachteilen, sondern auch die gesamte Infrastruktur rund um den/die Upload-Filter ist nicht einfach. So sind weitere wesentliche Fragen:

- Wer betreibt den Filter?
- Wo wird der Filter betrieben?
- Wie und in welcher Form gelangen die Daten zum Filter?

Die Frage der Infrastruktur um die Filter herum lässt sowohl aus der Diversität der Daten, als auch aus den Landesgrenzen ableiten. Daher ist abzusehen, dass urheberrechtlich geschützte Werke und illegale Daten in zwei getrennten Systemen geprüft und bewertet werden müssen. Jedoch auch die Landesgrenzen können hier ein ernstzunehmendes Problem werden. Hier sollte mindestens auf multinationaler am besten auf internationaler Ebene versucht werden, eine einheitliche Lösung zu finden.

1.2 Rechtliche Grundlage

Die rechtliche Grundlage für Upload-Filter hat die EU in verschiedenen Rechtsakten geschaffen. Direkter Auslöser für diese Diskussion ist die Richtlinie 2019/790/EU DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG, sowie indirekt die EMPFEHLUNG 2018/334/EU DER KOMMISSION vom 1. März 2018 für wirksame Maßnahmen im Umgang mit illegalen Online-Inhalten.

Die Richtlinie enthält den umstrittenen Artikel 17 (vorher Artikel 13), der die "Diensteanbieter für das Teilen von Online-Inhalten"in die Pflicht nimmt darauf zu achten, dass urheberrechtlich geschützte Werke ohne Zustimmung des Rechteinhabers nicht hochgeladen werden dürfen. So muss der Diensteanbieter gemäß Art. 17 Abs 4 b.) nachweisen, dass er "nach Maßgabe hoher branchenüblicher Standards [...] alle Anstrengungen unternommen hat, um sicherzustellen, dass bestimmte und Werke und sonstige Schutzgegenstände [...] nicht verfügbar sind". Des Weiteren muss nach einem Hinweis und entsprechender Bewertung durch den Diensteanbieter der Zugriff zu diesem Inhalt gesperrt und ein erneutes Hochladen vermieden werden.

Eben diese Anforderung des Vermeiden eines erneuten Hochladens begründet die Befürchtung, dass hierfür Upload-Filter zum Einsatz kommen würden. Doch Art. 17 Abs. 7 nennt Ausnahmen, wonach "Zitate, Kritik und Rezensionen"; sowie die "Nutzung zum Zweck von Karikaturen, Parodien und Pastiches". Somit muss die gewählte Maßnahme zur Verhinderung des erneuten Uploads zwischen unerlaubter Nutzung und Ausnahme unterscheiden können.

Zusätzlich zur Richtlinie hält auch die Handlungsempfehlung der EU ein vorgehen der Diensteanbieter gegen illegale Inhalte für angebracht. Hierin werden auch proaktive Maßnahmen empfohlen. Diese können laut Punkt 18 "den Einsatz von Systemen zur automatischen Erkennung illegaler Inhalte umfassen". Die folgenden Punkten formulieren Sicherheitsvorkehrungen im Zusammenhang mit solchen Maßnahmen. Hostingdiensteanbieter werden aufgerufen umsichtig bei der Bearbeitung von Hinweisen auf illegale Inhalte und

den Gegendarstellung der jeweiligen Inhalteanbieter vorzugehen. Des Weiteren "sollten wirksame und geeignete Sicherheitsvorkehrungen vorhanden sein, um sicherzustellen, dass [...] insbesondere Entscheidungen zur Entfernung oder Sperrung von als illegal erachteten Inhalten, zutreffend und fundiert sind". Auch die Empfehlung für eine menschliche Kontrolle und Aufsicht solcher Systeme und deren Entscheidungen wird hervorgehoben.

Somit müssen nicht nur zwei verschiedene oder eine kombinierte Maßnahme her, um die Richtlinie und die Handlungsempfehlung umzusetzen, sondern die aufgeführten Ausnahmen und Sicherheitsvorkehrungen adäquat umgesetzt werden.

2 Notwendigkeit

Über die Notwendigkeit von Upload-Filtern lässt sich genauso streiten, wie über deren Umsetzung. Hierzu wurden eine Reihe von Studien, Papern und andere Arten von Schriftstücken angefertigt. In diesem Kapitel sollen die wichtigsten im Hinblick auf Ergebnisse aber auch auf deren Verfasser bzw Auftraggeber beleuchtet und eingeordnet werden.

2.1 EU-Studie - Schätzung Verdrängungseffekte

Eine durch die EU-Kommision in Auftrag gegebene Studie zeigt zwar die Verdrängung von legalen Einnahmen durch illegale Downloads und/oder Streams von medialen Inhalten, relativiert diese Ergebnisse aber im gleichen Zuge wieder. In dieser Studie wurden 30.000 Menschen aus 6 EU-Ländern befragt. Die Auswahl der Mitgliedsstaaten und der jeweils dort lebenden Probanden erfolgte unter repräsentativen Gesichtspunkten. Die Studie kann somit als repräsentativ für die gesamte EU betrachtet werden. Untersucht wurde das Verhalten dieser Probanden im Zusammenhang mit dem Konsum von Musik, Filmen, E-Book, sowie Videospielen. Um die Ergebnisse vergleichbar darstellen zu können berechnet die Studie eine sogenannte Verdrängungsrate.

Von den untersuchten kreativen Inhalten – so wird es wörtlich Übersetzt in der Studie genannt – kann lediglich bei Musiktiteln kein Verdrängungseffekt erkannt werden. Die Einnahmen mit Musik seien stabil. Die Raubkopien von damals noch physischen Tonträgern werden heute durch illegale Aufnahmen und Streams von live-Konzerten kompensiert.
Bei Filmen wird zwischen Blockbustern und nicht-Blockbustern unterschieden. Blockbuster verzeichnen eine positive Verdrängungsrate von ca 40%. Das bedeutet, dass pro 10 illegal geschauten Blockbustern, 4 weitere Male für den gleichen Film bezahlt wird. Andere, weniger beliebte Filme, hingegen verzeichnen eine negative Rate, also pro illegal geschautem Film sind Käufe ausgeblieben. Gerechnet auf das Verhältnis von Blockbustern zu nicht-Blockbustern wurde für das Medium Film eine Verdrängungsrate von durchschnittlich -27% ermittelt.

Auch E-Books sind von einer negativen Rate betroffen. Diese beträgt zwar deutlich höhere -38%, jedoch erklärt die Studie auch, dass auf Grund der niedrigen Gesamtverkaufszahlen von E-Books diese Zahl insgesamt vernachlässigt werden könne.

Lediglich Videospiele in sämtlichen Formen verzeichnen eine durchweg positive Verdrängungsrate von 24%. Dies kann laut der Studie auf eine geschickte Taktik der Hersteller zurückgeführt werden. Zahlende Spieler werden z.B. mit Bonusmaterial oder mehr Levels belohnt. So entsteht der Gedanke, dass illegale Downloads von neuen Spielen einkalkuliert und sogar gewollt werden. Man könnte es als gewollte aber nicht publizierte Werbekampagne verstehen. Es ist unklar, war es genau ist, aber er wirkt sich positiv auf die Verkaufszahlen von Spielen aus.

Doch dieses Studie hat außerdem auch den Wille zu bezahlen abgefragt. Jedoch stand nur das zuletzt illegal genutzte Produkt im Vordergrund. Somit können diese Ergebnisse nur bedingt genutzt werden, sie zeigen aber einen Trend. Erschreckend und beunruhigend ist jedoch der Anteil der Personen, welche nicht bereit sind überhaupt für mediale Inhalte zu bezahlen. Spitzenreiter sind die Filme. Durchschnittlich 68% der EU-Bürger würden generell nicht für einen Film bezahlen wollen. Niedrigere Werte in der Studie haben lediglich Deutschland (59%) und das vereinigte Königreich (47%).

Die in der Studie genannten Ergebnisse sind zwar repräsentativ ermittelt worden, aber dennoch wenig aussagekräftig. Eine Frage nach dem eigenen illegalen Verhalten würde nicht immer wahrheitsgemäß beantwortet werden. Viele Probanden würden sozial akzeptable Antworten geben, wenn nach dem eigenen regelmäßigen Verhalten gefragt wird, stellt die Studie klar. van der Ende; Joost Poort; Robert Haffner; Patrick de Bas; Anastasia Yagafarova; Sophie Rohlfs; Harry van Til [2015]

Diese Studie ist von der EU nie offiziell veröffentlicht, sondern lediglich auf einen Antrag einer Abgeordneten des EU-Parlaments zugespielt worden. Ob es wegen der -laut der Studie- wenig belastbaren Zahlen, oder dem unpassenden Ergebnis ist, bleibt ebenfalls offen.

Schulzki-Haddouti [2017]

2.2 EU-Paper - Filmpiraterie und verdrängten Verkäufen in der EU

Dieses von der EU veröffentlichte Paper als Reaktion auf die Studie aus Kapitel 2.1 bezieht sich jedoch lediglich auf den illegalen Download und Stream von Filmen. Außerdem nennt das Paper verschiedene Gründe, warum es aktuell an belastbaren Zahlen zu diesem Thema mangelt – nicht repräsentativ, meist nicht mehrere Länder betrachtet, wenige Studien mit aktuellen Zahlen. Alle drei Mängel sollen in diesem Paper behoben werden. Da hier die Daten der zuvor genannten Studie genutzt wurden, steht fest, dass mehrere Länder betrachtet wurden und die Repräsentativität ebenfalls gegeben ist. Doch ein Blick in die Referenzen am Ende des Dokumentes zeigt, dass die jüngste sonstige Quelle aus dem Jahre 2012 stammt. Somit ist zumindest das Ziel der Aktualität deutlich verfehlt. Dieses Paper wertet die Daten der Studie lediglich neu aus und schafft somit keine neuen Informationen. Da sich hier zusätzlich nur auf die Betrachtung von Filmen beschränkt wird, nutzen die Verfasser das Paper um Gründe für eine gesetzliche Verschärfung des Urheberschutzes. Auch hier konnten keine eindeutigen Beweggründe für die Richtlinie erarbeitet werden.

Herz und Kiljanski [2016]

2.3 Max-Planck-Institut - Nutzung von geschützter Online-Inhalte

Die durch das Max-Planck-Institut für Innovation und Wettbewerb in Kooperation mit dem Munich Centre for Internet Research der Bayerischen Akademie der Wissenschaften herausgebrachte Studie betrachtet das Verhalten von gut 5500 Deutschen im Bezug auf die Nutzung von kreativen online Inhalten. Hierbei wurde besonders auf Minderjährige mit Internetanschluss Wert gelegt. Die Aufteilung nach Geschlecht beträgt

50:50. Die Studie stellt den Zeitraum vom 06.05.2017 bis 03.07.2017 dar und unterscheidet zwischen Musik, Filmen, TV-Programmen/Serien, E-Book, Videospielen und E-Papern.
Mit Ausnahme von E-Books und Videospielen haben die Mehrheit der Befragten in diesem Zeitraum mehr kostenfreie als kostenpflichtige Online-Angebote in Anspruch genommen. Bei allen Medien waren die Befragen mehrheitlich ebenfalls der Auffassung, sie würden das Angebot legal nutzen. Ein knappes Drittel sind nach eigener Einschätzung in der Unterscheiden, ob eine Angebot legal ist oder nicht, "relativ sicher", ein viertel sind sich jeweils "nicht sehr sicher"und "überhaupt nicht sicher", nur 11% sind sich darin "sehr sicher". Bestärken könnte hier die Tatsache, dass 93% noch keine Mahnung wegen illegalem Nutzen von geschützten Inhalten erhalten haben.

Die Gründe für das illegale Konsumieren sind vielfältig. Ganz oben stehen unter Anderem: "Es ist kostenfrei", "Es ist einfach/bequem", "Man kann etwas vor dem Kauf ausprobieren"; oder auch etwas primitiver: "Weil ich es kann".
Da ist die Frage nach den Anreizen für die Nutzung der Inhalte zu bezahlen nicht weit. Hierzu nennen die Befragten vorrangig folgende Gründe: Preis legaler Dienste, Inhalte legal nicht erhältlich, illegale Inhalte/Nutzung nicht gut genug gekennzeichnet; aber auch die Angst verklagt zu werden steht relativ weit oben.

Letztendlich zeigt diese Studie, dass eine schärfere gesetzliche Regelung gar nicht notwendig ist. Die Nutzer nennen hauptsächlich das Angebot, den Preis, die Kennzeichnung sowie das niedrige Risiko auf Sanktionen als Gründe für die illegale Nutzung. Es ist kein Hinweis auf mangelnde oder unzureichende gesetzliche Regelungen zu finden. Harhoff u. a. [2016]

2.4 Statistiken über illegale Inhalte

Facebook nimmt Meldungen über illegale Inhalte ernst und löscht auch fleißig entsprechend bestätigte Inhalte. Auf Facebook werden pro Tag (pro Quartal) ca 4 Mrd (364 Mrd) Textbeiträge, 350 Mio. (32 Mrd.) Bilder und 100 Mio. (9 Mrd) Std. Videos hochgeladen.Smith [2019b] Im Verhältnis dazu wurden im schlechtesten Quartal 9,4 Mrd Inhalte gelöscht. Das sind 1,1% aller geposteten Inhalte. Ob alle diese Inhalte durch einen automatisierten Upload-Filter entdeckt würden, ist nicht sicher.

YouTube stellt ebenfalls Statistiken über gemeldete und auch ggf anschließend gelöschte Inhalte zur Verfügung. Auf YouTube werden knapp 600 Mio. Std. Videos pro Tag hochgeladen.Smith [2019a] Statistisch gesehen sind die beliebtesten Videos auf YouTube zwischen 30 und 180 Sekunden lang.Spiller und Pohlmann [2014] Nimmt man die mittlere Länge von 105 Sekunden auch als durchschnittliche Länge eines YT-Videos, lassen sich 600 Mio Std. in ca 340 Mio. Videos pro Tag aufteilen. Hiervon wurden seit Inkrafttreten des Netzwerkdurchsetzungsgesetz am 01.10.2017 bis Juli 2018 gut 214.000 Inhalte gemeldet. Von denen entfernt Youtube ca 27% also knapp 58.000 Videos aus den verschiedensten Gründen.

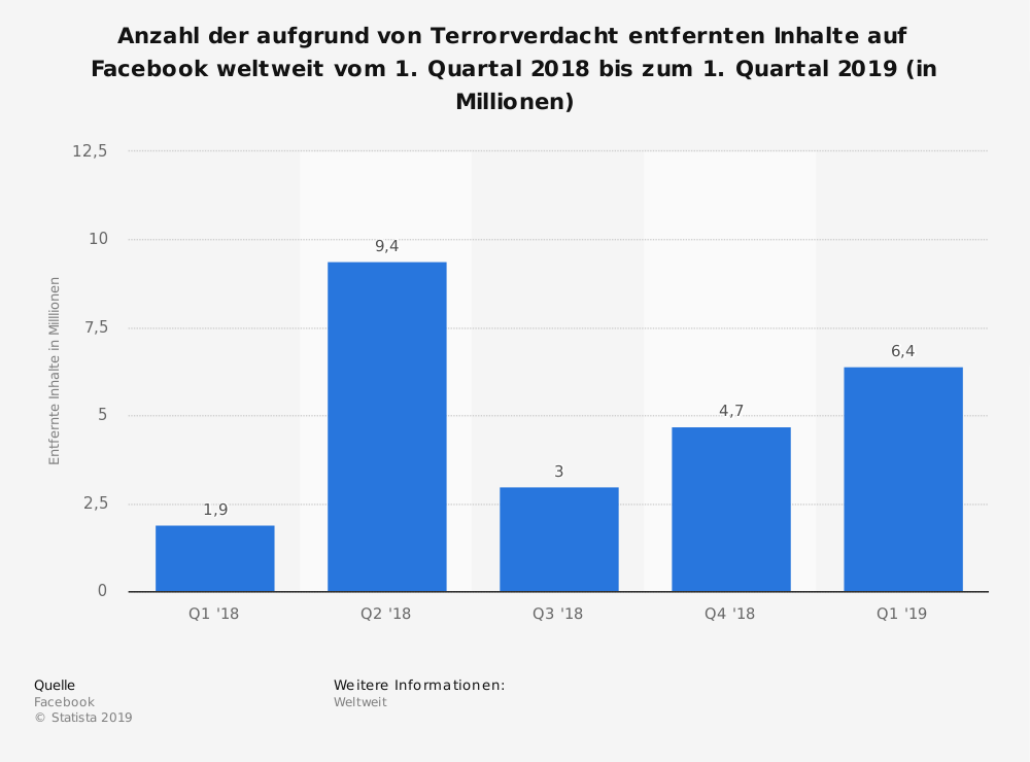

Abbildung 3: Löschung auf Grund von Terrorverdacht bei Facebook

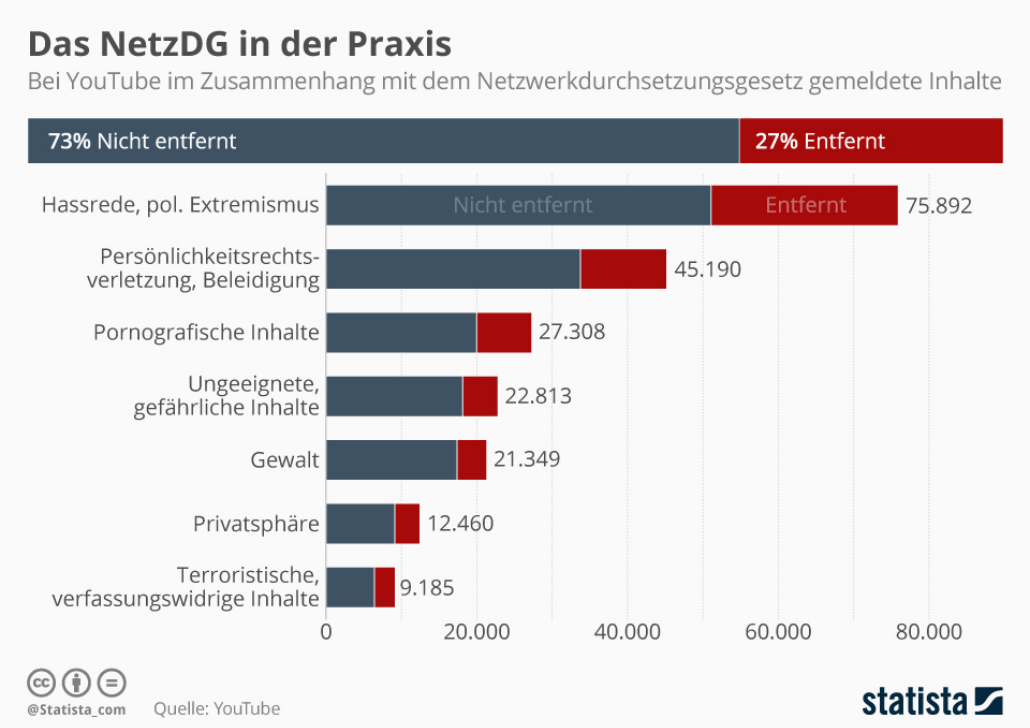

Abbildung 4: Löschung durch das NetzDG bei Youtube

Eine Statistik über den tatsächlichen Anteil von illegalen Inhalten im Internet ist aktuell kaum zu finden. Also kann man nur davon ausgehen, dass Nutzer wie Mitarbeiter von sozialen Netzwerken ihr bestes tun, um illegale Inhalte fern zu halten.

3 Aufgaben und Ziele

Dieses Kapitel beschäftigt sich mit dem Upload-Filter als Blackbox. Das heißt alle hier beleuchteten Aspekte sind unabhängig von der konkreten Technologie.

3.1 Aufgaben

Ein Upload-Filter ist ein Instrument zur Bewertung, Klassifizierung und Filterung aller Inhalte, welche auf eine bestimmte Plattform hochgeladen werden sollen. Er ist somit unumgänglich und muss passiert werden. Der Filter bewertet den Upload auf Basis von verschiedenen Technologien und nach unterschiedlichen Kriterien. In Abbildung 5 soll lediglich deutlich werden, dass der Filter fester Bestandteil des Uploadvorganges wird. Hier gibt es natürlich unterschiedliche Möglichkeit und Geschäftsmodelle. Jedoch die grundlegende Funktionsweise haben alle Filter gemeinsam. Sie sollen beurteilen, ob ein Upload zulässig ist, oder nicht. Ein zulässiger Upload wird unmittelbar an die entsprechende Plattform weitergeleitet und trägt den Vermerk, dass dieser freigegeben werden kann. Ein unzulässiger Upload, würde vom Filter an die zuständige Behörde weitergeleitet werden. In diesem Fall erhält die Plattform nur den Vermerkt, dass das Bild aussortiert wurde, um dies dem Nutzer mitteilen zu können.

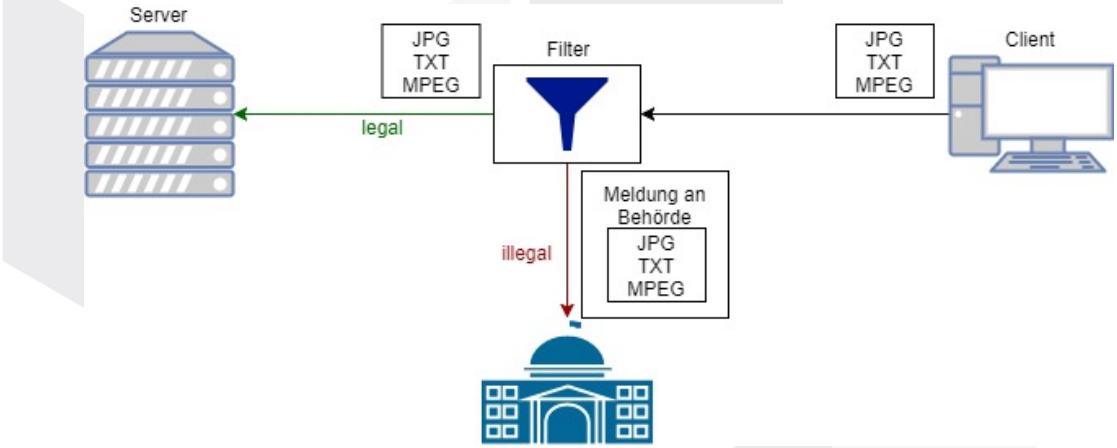

Abbildung 5: Filter wird vor den Server geschaltet.

3.2 Ziele

Transparenz

Ein Upload-Filter darf bei positiv bewerteten Inhalten keinerlei Auswirkungen auf dem Upload-Prozess haben. Viele Fotos bspw. werden gepostet, weil eine aktuelle Situation mit Freunden und anderen Leuten geteilt werden soll. Wenn dies ein Filter wesentlich verzögert, würde dieser zunehmend an Akzeptanz verlieren. Daher muss die Technologie auf die jeweilige Anzahl der zu erwartenden Uploads ausgelegt werden. So der Filter von Facebook beispielsweise ca 350 Mio Fotos pro Tag und 100 Mio. Std. Videos pro

Tag verarbeiten können.Smith [2019b] Das ergibt auf eine Sekunde heruntergebrochen eine Datenflut von ca 4000 Fotos und 1150 Std. Videos. Diese muss der Filter auch innerhalb von einer Sekunde bewältigen können. Anderenfalls bildet sich ein "Datenstau", der stetig wächst.

Zuverlässigkeit

Das Wort "Zuverlässigkeit"hat hier zwei Bedeutungen.
Hochverfügbarkeit: Der Filter muss zu jeder Zeit 24/7 volle Leistung bringen können, um einen oben erwähnten Datenstau nicht entstehen zu lassen. Ein vollständig oder teilweise ausfallender Filter kann die Funktionsfähigkeit des gesamten Systems beeinträchtigen.
Fehlerfreiheit: Das System muss die Masse von Daten nicht nur bewältigen können, sondern zu jedem Datensatz das richtige Ergebnis ausgeben. Aktuell kann dies noch durch kein System realisiert werden. Somit sind Fehler nicht nur absehbar, sondern vorprogrammiert. Auch wenn die Fehlerquote gegen 0 tendiert, ist die Anzahl der falsch eingeordneten Daten immens. Um das Beispiel von Facebook nochmals aufzugreifen: Eine Fehlerquoten von 1 % bedeutet, dass immer noch 40 Fotos pro Sekunde bzw. 3,5 Mio. Fotos pro Tag falsch eingeordnet werden. Allerdings müssen falsche Ergebnisse nochmals unterschieden werden. Ein fälschlicherweise zugelassenes Foto nennt man False-Positive (FP) und ein fälschlicherweise aussortiertes Foto nennt man False-Negative (FN). Nehmen wir ein Verhältnis FP:FN als 50:50. Da jedes negative Ergebnis händisch geprüft werden muss, können viele bis alle der FN nachträglich zugelassen werden. Ein positives Ergebnis kann jedoch die sofortige Freischaltung des Bildes zur Folge haben, ohne weitere menschliche Nachkontrolle. Das bedeutet 20 Fotos pro Sekunde würden auf Facebook freigeschaltet, obwohl sie hätten negativ bewertet werden müssen.

Neutralität

Der Filter trifft die Entscheidung, ob ein Upload zugelassen wird oder nicht. Jedoch in Zeiten von selbstlernenden Systemen verliert der Spruch *"Ein System ist nur so schlau wie der Mensch, der es programmiert hat."* zunehmend an allgemeiner Gültigkeit. Da drängt sich doch die Frage auf, wer dem System beibringt, was erlaubt ist und was nicht. Somit gilt es sicherzustellen, dass sich die Entscheidungen an allgemeinen objektiven gesetzlichen und ethischen Regelungen und nicht an subjektiven Ansichten von Personen oder Firmen orientieren.

4 Infrastruktur

Ein Upload-Filter muss in die bereits bestehende Infrastruktur des World Wide Web eingebunden werden. Somit werden entweder die bestehenden Endpunkte erweitert, oder es entstehen neue.

4.1 Dedizierte Filter

Ein dedizierter Filter ist genau einem Nutzer zugeordnet bzw ist sogar dessen Eigentum. Somit hat der Nutzer vollen Zugriff auf alle Ressourcen des Filters. Doch voller Zugriff heißt nicht nur volle Leistung und volle Kontrolle, sondern auch volle Kosten. Ein dedizierter Filter ist eine Instanz innerhalb des privaten Netzwerks der Plattform bzw. des Standortes der Plattform und ist somit für einen Upload nicht direkt aus dem Internet erreichbar. Eine Internetverbindung wird dennoch benötigt, damit die Daten zum Vergleich von einer oder mehreren zentralen Stellen aus dem Internet geladen werden können. Diese werden im Filter lokal gespeichert. Somit ist der Zugriff leichter und schneller, erzeugt aber auch Redundanzen. Hieraus können einerseits Inkonsistenzen entstehen, aber auch die Entstehung von Bottelnecks und Single Points of Failure verhindert werden. Die hierfür entstehenden Kosten verursacht nicht nur die zusätzliche Instanz mit ihrer Hard- und Software, sondern auch die Anpassung und ggf Erweiterung des bereits vorhanden internen Netzwerks in Form von Konfiguration und Hardware. Der wohl größte Punkt dürfte hierbei die Software des Filters sein, vor Allem sobald ein gewisses Niveau von Intelligenz in der Prüfung erreicht werden muss.

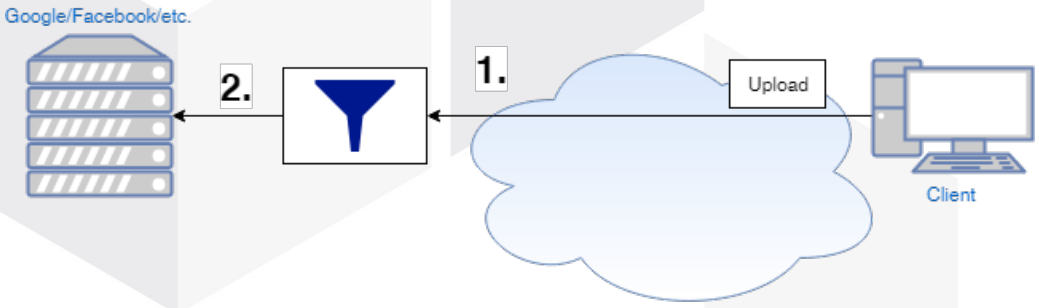

Abbildung 6: Dedizierter Filter

4.2 Generische Filter

Ein generischer Filter ist keinem Nutzer alleine zugeordnet. Hierbei handelt es sich entweder um einen externen Anbieter, dessen Geschäftsmodell auf der Erbringung von Filter-Dienstleistungen beruht, oder um eine Plattform mit eigenem Filter, der auch durch externe Plattformen, in der Regel entgeltlich, genutzt werden kann. Diese Infrastruktur würde offensichtlich zu einer Reduzierung von Filter-Instanzen führen und somit auch zu einer geringeren Anforderungen an Ressourcen. Die Bündelung der Ressourcen bedeutet damit auch die Bündelung der Kosten, welche auf jeden Nutzer heruntergebrochen geringer werden. Da sich nun die Filter-Instanzen verteilt im ganzen Internet befinden, muss der Upload nach der Übertragung zum Anbieter zum Vergleich ein erneutes Mal durch das Internet zum Filter transportiert werden. Und die

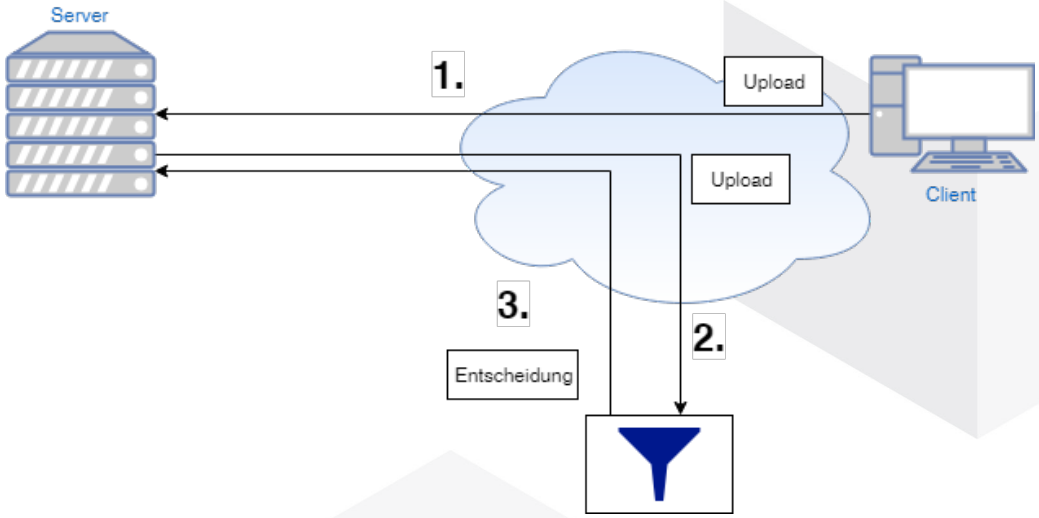

Abbildung 7: Generischer Filter

Antwort des Filters muss ebenfalls durch das Internet zurück übertragen werden. Eine weitere Konsequenz der Teilung und Verteilung der Filter ist der damit verbundene Verlust an Kontrolle über den Filter. Der Nutzer ist der Technologie und dem Verhalten vollkommen ausgeliefert.

5 Daten

Ein essentieller Bestandteil von Upload-Filtern sind die Daten, auf dessen Basis die Vergleiche und Bewertungen der Uploads durchgeführt wird. Die Daten lassen sich grob in 2 verschiedene Arten einteilen. Diese Einteilung lässt auf die unterschiedliche Herkunft und die Anforderungen schließen, um diese angemessen Bewerten zu können. Im Folgenden sind 3 Aspekte von Bedeutung – Herkunft und Pflege, Speicherung und Verarbeitung der Daten.

5.1 Woher kommen die Daten?

Die Quelle als Herkunft der Daten spielt die wichtigste Rolle in der Verarbeitung von Informationen. Auf der Qualität und Belastbarkeit der gelieferten Daten beruht die Qualität der Verarbeitung und damit die Aussagekraft des Ergebnisses. Eine gute und seriöse Quelle muss daher mehrere Anforderungen erfüllen, damit sie ihrer Aufgabe der Bereitstellung und Pflege der Vergleichsdaten in vollem Umfang gerecht werden kann.

Um die Quelle(n) der Daten genauer beleuchten zu können, ist es notwendig sich zuvor mit der Art der Daten auseinanderzusetzen. Es soll in der Regel zwischen strafbaren Inhalten und urheberrechtlich geschützten Werken unterschieden werden. Durch diese Einteilung ergibt sich direkt die Notwendigkeit von verschiedenen Quellen. Strafbare illegale Inhalte müssen durch die zuständigen Strafverfolgungsbehörden zur Verfügung gestellt werden. Denn diese sind für das Aufspüren und ahnden zuständig. Selbstverständlich können und sollen auch Privatpersonen vermeintlich strafbare Inhalte melden. Doch die Entscheidung über deren Strafbarkeit muss schlussendlich von den zuständigen Behörden und/oder Gerichten getroffen werden. Somit obliegt diesen auch die Aufgabe die Integrität und Aktualität der Daten sicherzustellen.

Urheberrechtlich geschützte Werke werden durch die jeweiligen Urheber oder deren Vermarktungsagenturen verwaltet. Somit gibt es weltweit eine nur schwerlich abschätzbare Anzahl von Rechteinhabern und eine noch größere Zahl an entsprechend geschützten Werken. Des Weiteren muss sichergestellt werden, welches Werk bzw welche Version eines Werkes von welchem Urheber zu erst veröffentlicht wurde. So kann der eigentliche Rechteinhaber ermittelt werden.

5.2 Wo werden die Daten gespeichert?

Für die Vorhaltung von Vergleichsdaten gibt es auch Filtersicht (Nutzer) 2 verschiedene Modelle, analog zur Infrastruktur. Ein Filter kann eine dezidierte Datenvorhaltung haben, wobei der Filter und die Daten im gleichen Netzwerk angesiedelt sind und eine schnelle, zuverlässige und sicherer Kommunikation gewährleistet werden kann. Hat der Filter diese jedoch nicht, ist er auf generische Datenbank, also eine geteilte Ressource angewiesen. Die Vor- und Nachteile verhalten sich ebenfalls analog zum Kapitel 4. So hat eine dezidierte Datenbank die Vorteile einer zuverlässigen und sicheren Anbindung an den Filter sowie voller Kontrolle über das System, die Nachteile der vollen Kosten und vollem Aufwand zur Verwaltung und

Aktualisierung der Daten. Im Gegensatz dazu hat eine geteilte Ressource die Vorteile von wenig Verwaltungsaufwand und geringeren Kosten für den Nutzer, die Nachteile von fehlender Kontrolle über die Daten und einer unsicheren und ggf unzuverlässigeren Anbindung. Hier sind diese jeweiligen Vor- und Nachteile für die Betreiber der Filter sorgfälltig abzuwägen.

Aus Sicht des Datenbankbetreibers (Anbieter) ist der organisatorische Aufwand deutlich höher. Um die Datenvorhaltung möglichst effizient zu betreiben, sollten die Daten möglichst zentral vorgehalten werden. Das heißt es sollte nur weniger – im Idealfall nur – einen Anbieter geben. Somit wird eine Redundanz und die damit verbundene Gefahr von Inkonsistenzen möglichst gering gehalten. Sollte der Anbieter aus dem öffentlich-rechtlichen Bereich stammen, ein "Monopol"durch eine öffentliche Einrichtung vergleichsweise einfach zu realisieren. Sollten die Anbieter aus dem privatrechtlichen Bereich stammen, wäre eine solche Regulation schwer durchzusetzen. Hier könnte eine entsprechende Behörde mit einer Lizenz-Lösung arbeiten, um die Anzahl der Konkurrenten möglichst gering zu halten. Jedoch würden sich beide Möglichkeiten nur auf den Zuständigkeitsbereich dieser Behörde beschränken. Somit wäre für Deutschland maximal eine EU-einheitliche Lösung möglich. Es sei denn es gelingt entsprechende Abkommen mit anderen Nicht-EU-Ländern abzuschließen. Dies ist nicht unmöglich, soll aber zeigen, dass der Verwaltungsaufwand nur schwer abzusehen ist. Jedoch ist es nicht unwahrscheinlich, dass die Privatwirtschaft schneller ist, als die Gesetzgebung. Also sollte vor der offiziellen Einführung eine umfassende Regelung getroffen werden, welche die Struktur von Geschäftsmodellen in der Privatwirtschaft eingrenzt, damit der Nutzen und nicht das finanzielle Interesse im Vordergrund steht.
Neben der Zentralität steht auch die hohe Verfügbarkeit im Vordergrund. Vor Allem wenn die Speicherung räumlich getrennt vom Filter erfolgt, muss nicht nur die physikalische Anbindung, sondern auch die Verfügbarkeit des System theoretisch bei 100 % liegen. Dies ist zwar kein neues Problem, sollte aber mit hoher Priorität beachtet werden.

Als wären die bisher genannten Punkte nicht schon aufwendig genug umzusetzen, kommt jetzt noch der Aspekt hinzu, dass hiervon sowohl urheberrechtlich geschützte Werke als auch illegale Inhalte gespeichert werden müssen. Hier entsteht schnell ein Interessenskonflikt. Urheberrechtsverletzungen sind in der Regel zivilrechtliche Verfahren. Jedoch das Hochladen und/oder Verbreiten von illegalen Inhalten eine Straftat darstellen und somit nach der Strafprozessordnung verfahren werden würde. Das bedeutet die Strafverfolgungsbehörden haben gar kein Interesse urheberrechtlich geschützte Werke als Vergleichsdaten vorzuhalten. Des Weiteren würden die Behörden genauso wenig illegale Daten an private Anbieter weitergeben. Eine Möglichkeit würde evtl. darin bestehen, dass lediglich die Hash-Codes von bekannten illegalen Inhalten weitergegeben werden. Doch auch dies würde einen erheblichen verwaltungstechnischen Aufwand bedeuten. Somit ist es am wahrscheinlichsten, dass 2 getrennte System zur Datenvorhaltung entstehen würden.

5.3 Wie werden die Daten verarbeitet?

Die vorgehaltenen Daten dienen als Basis, auf Grund dessen die Uploads bewertet und entsprechend freigeschaltet oder gemeldet werden. Je nach eingesetzter Technologie werden die Uploads mit den Daten verglichen, oder die Daten dienen als Trainingsdaten.

Werden die Uploads mit den vorgehaltenen Daten verglichen, stellt dies ein vergleichsweise einfaches Verfahren dar, welches jedoch auch nur eine begrenzte Möglichkeit bietet. Dieses Verfahren ist schnell, leicht zu implementieren und ressourcensparend. Dafür kann es lediglich bereits bekannte Inhalte finden. Diese müssen entweder völlig identisch oder dürfen nur leichte Abwandlungen enthalten. Für, aus Sicht des Filters, völlig unbekannt Inhalte besteht keine Möglichkeit diese zu erkennen und zu bewerten.

Im anderen Fall kommen intelligente Filter zu Einsatz. Diese arbeiten in der Regel auf einem neuronalen Netz. Hier werden die bekannten Daten als Trainingsdaten verwendet. Das heißt das Netz bekommt die Daten mit den jeweils gewünschten Ergebnissen. Somit lernt das Netz welche Art von Inhalten wie bewertet werden sollen. Nach der Trainingsphase können hier zwar auch bereits gesehene Inhalte erkannt werden, aber vor Allem auch Inhalte, die noch nicht gesehen wurden. Diese erweiterten Möglichkeiten benötigen jedoch eine etwas höhere Bearbeitungszeit und vor Allem auch mehr Ressourcen.

6 Technologien

Die technische Umsetzung kann grob in zwei verschiedene Ansätze aufgeteilt werden – einfache Filter und intelligente Filter. Im Folgenden wird sich herausstellen, die Vorteile des Einen sind die Nachteile des anderen und umgekehrt. Es gibt zwar einzelne Ansätze um diese harte Grenze etwas aufzuweichen, aber im Großen und Ganzen ändert sich daran nicht viel.

6.1 Einfache Filter

Unter einfachen Filtern versteht man Filter-Techniken, welche nach einem "harten"Algorithmus die Eigenschaften des Inhalts festlegt und nur diese bewerten. Diese Eigenschaften können sein u. A. die Herkunft, auffällige Metadaten, und vor Allem der Hash-Wert. Diese erhobenen Daten werden gegen eine Datenbank abgeglichen, welche entsprechende Eigenschaften bereits auffällig gewordener und als negativ bewerteter Inhalte enthält.

Jede Standard-Hashfunktion ist selbstverständlich gar nicht resistent gegen leichte Veränderung des Inhaltes. Allerdings haben große Unternehmen wie u. A. YouTube und Microsoft bereit eigene Verfahren entwickelt.

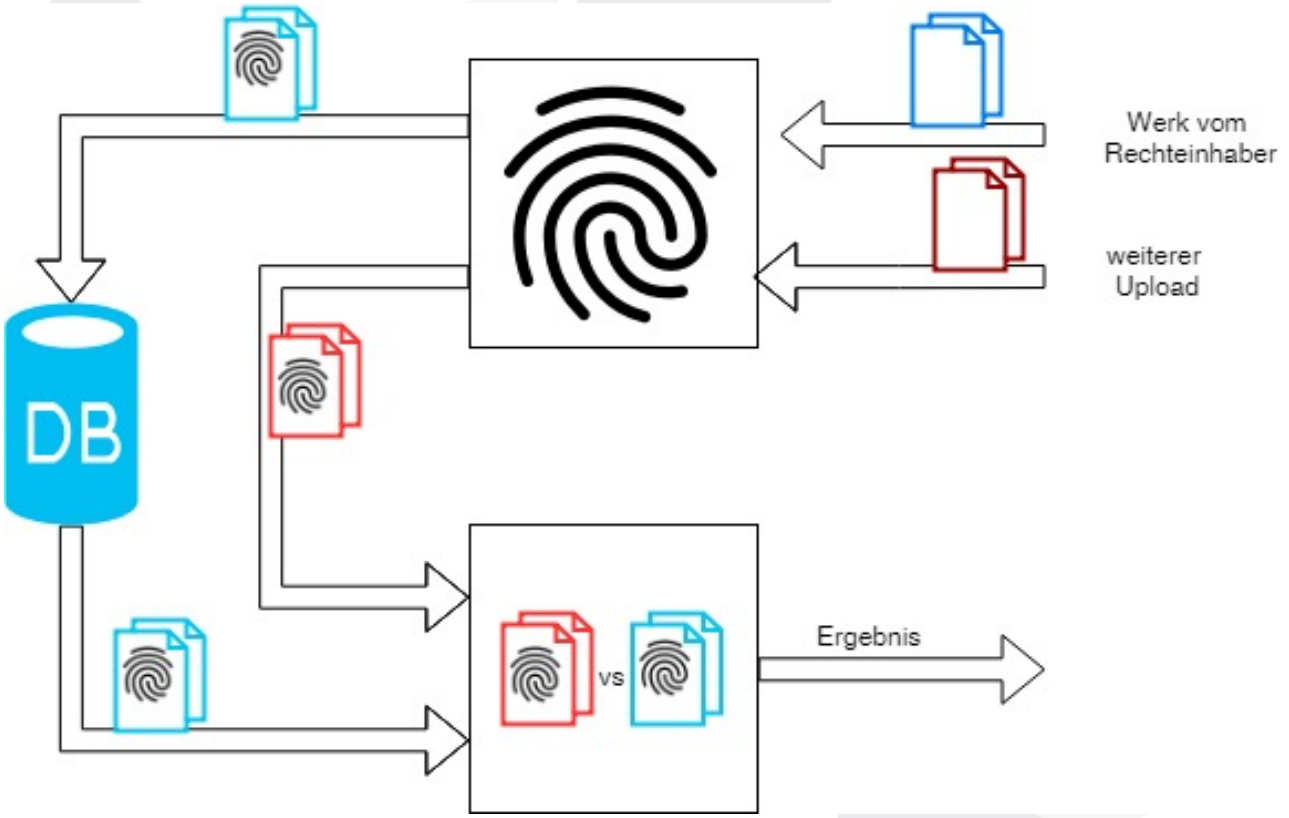

Abbildung 8: Content-ID von YouTube

Dieses System ist zum Finden von Urheberrechtsverletzungen entwickelt worden. Hierzu unterhält Youtube eine eigene Datenbank, in der Fingerabdrücke von urheberrechtlich geschützten Werken vorgehalten werden.

Wird nun ein neues Video hochgeladen, wird hiervon ebenfalls ein solcher Fingerabdruck erstellt. Dieser wird anschließend gegen die Datenbank abgeglichen. Das Verfahren zur Berechnung des Fingerabdrucks ist in der Lage ähnliche Inhalten mit ähnlichen Fingerabdrücken zu versehen. Somit können auch leicht abgewandelte Inhalte identifiziert werden. Ist der Upload teilweise oder vollständig geschützt und besitzt der Uploader keine Recht daran, wird der eigentliche Rechteinhaber informiert und kann über das weitere Verfahren entscheiden. Youtube

Ein anderes, ebenfalls etwas robusteres, Verfahren wurde von Microsoft in Kooperation mit der Universität Dartmouth entwickelt. Der Algorithmus PhotoDNA wandelt hierzu das Bild in wenigen Schritten so um, dass auch ein leicht abgewandeltes Bild hier kaum noch auffallen würde. Im ersten Schritt wird das Bild von bunt in schwarz-weiß umgewandelt, um leichte Farbveränderungen unwirksam zu machen. Anschließend wird das Bild in Raster eingeteilt. Für jedes Raster wird nun separat der Hash-Wert berechnet. Die Kombination der einzelnen Hash-Werte ergibt nun die DNA des Bildes, welche in einer Datenbank abgespeichert und für Vergleiche mit späteren Bildern verwendet werden kann. Kleinhans [2013]

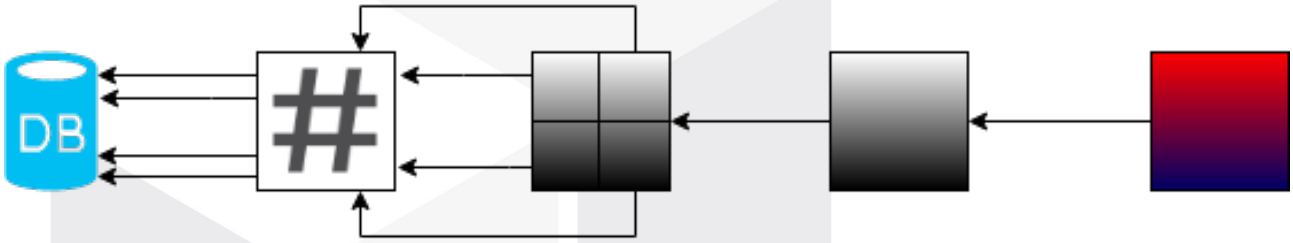

Abbildung 9: PhotoDNA von Microsoft

6.2 Intelligente Filter

Die andere Möglichkeit zur Umsetzung automatisierter Upload-Filter basiert auf künstlicher Intelligenz. Hier wird auf Basis von selbstlernenden Systemen ein Upload bewertet. Anders als bei einfachen Filtern steht hier nicht direkt eine Datenbank im Hintergrund, sondern es werden eine große Anzahl von Datensätze bekannter unzulässiger Inhalte zum Training verwendet. Das System lernt wie diese Inhalte aufgebaut sind und wie die erkannten Eigenschaften zu gewichten sind.

Intelligente Filter bieten einen sehr wesentlichen Unterschied zu einfachen Filtern. Während ein einfacher Filter lediglich bekannte – mit den oben genannten Variationen auch leicht veränderte – Inhalte wiedererkennen kann, ist der intelligente Filter in der Lage auch noch nie gesehene Inhalte bewerten zu können.

Bei den einfachen Filtern war die Antwort recht einfach. Wenn die Inhalte 1:1 hochgeladen werden, liegt die Trefferquote bei 100%, da der Algorithmus sich nicht ändert. Bei leicht veränderten Inhalten kommt es auf die Robustheit des Algorithmus an. Zwar ist die Trefferquote bei neuronalen Netzen nur annähernd bei 100%, allerdings gibt es einen anderen Vorteil. Ein neuronales Netz kann auch noch unbekannte Inhalte einordnen und bewerten. Dies liegt an dem “weicheren“Algorithmus. Dieser bewertet weniger die Metadaten und Hashes, sondern den Aufbau des Inhaltes wie ein künstliches Gehirn.

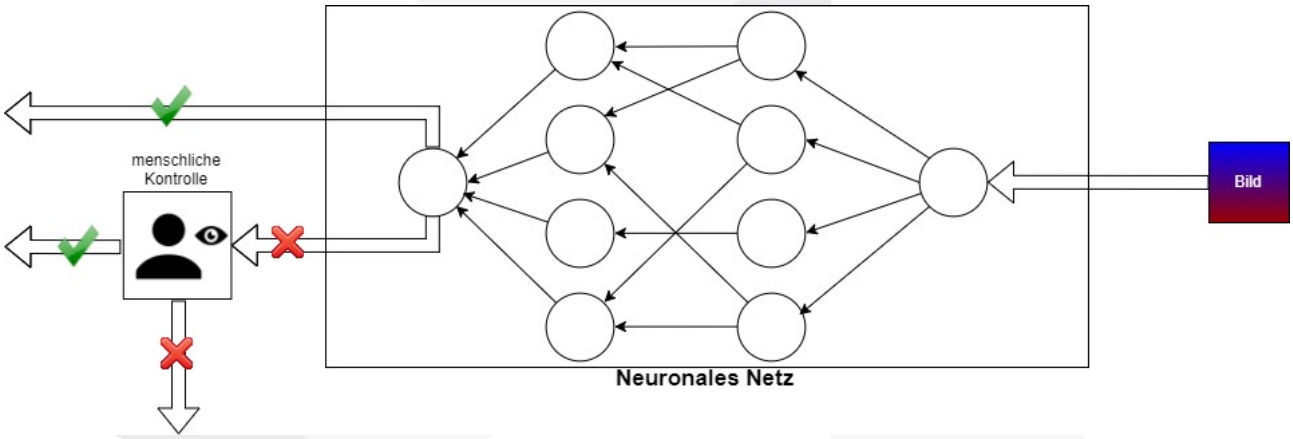

Abbildung 10: neuronales Netz

7 Fazit und Ausblick

Auch wenn durch die EU eine Handlungsempfehlung für den Umgang mit terroristischen Online-Inhalten und eine Richtlinie zur Verbesserung des Urheberschutzes herausgebracht wurde, welche beide wohle Upload-Filter nach sich ziehen, ist diese Notwendigkeit in keinster Weise erwiesen. Im Gegenteil, es gibt sogar Studien, welche Upload-Filtern keinen Mehrwert beimessen oder diese sogar als schädlich darstellen. So zb. wenn es um illegales Konsumieren von kreativen Online-Inhalten geht. Dies ist in gewissem Maße sogar förderlich für den Verkauf. Auch die urheberrechtswidrige Verbreitung von geschützten Werken wird wahrscheinlich nicht unbedingt eingedämmt. Es hat sich gezeigt, dass die Wirkung von Upload-Filtern von der Zusammenarbeit aller beteiligten Parteien abhängt, und das auf internationaler Ebene. Diese Zusammenarbeit von erstmal zustande kommen und dann aufrecht gehalten werden. Es bleibt fraglich, ob dieser Aufwand und die damit verbunden Kosten im Verhältnis stehen zu den Mehreinnahmen, die durch die gemeldeten unberechtigten Verbreitungen geschützter Inhalte und der dadurch folgenden Mahnverfahren entstehen.

Doch auch von der technischen Seite her sind Upload-Filter sehr zwiespältig. Sie müssten in eine bestehende Internet-Infrastruktur eingebunden werden. Somit nutzen sie die gleiche Internetleitungen, wie alle anderen Dienste es jetzt schon tun. Das bedeutet je nach Auslastung und Verhältnis von dezidierten und generischen Filtern steigt die Auslastung des Internets deutlich. Somit wäre ein massiver Ausbau der Infrastruktur höchst wahrscheinlich unumgänglich. Doch verlässliche Zahlen sind schwer zu beschaffen, da diese Technologie noch kaum bis gar nicht flächendeckend besteht, kann hier nur vermutet werden. Eine hauptsächliche Nutzung von dezidierten Filtern würde zwar weniger Datentransfer bedeuten, da nur die Vergleichsdaten und nicht alles Uploads bzw deren Hash-Codes übertragen werden müssen; jedoch ist hier der koordinative Aufwand deutlich höher. Da alle Knoten immer auf dem aktuellsten Stand gehalten werden müssen. Allerdings gibt es hier für bereits Lösungen für verteilte Datenhaltung. Wird jedoch hauptsächlich auf generische also geteilte Filter gesetzt, entfällt zwar die Koordination der einzelnen Datenbanken, jedoch muss jedes Upload bzw der Hash-Code über das Internet versendet werden. Das selbe Problem besteht bei der Frage, wo der Speicher der Daten ist. Befindet er sich in räumlicher und organisatorischer Näher zum Filter, oder nicht. Sollte er dies nicht tun, ergeben sich auch hier, analog zum Standort des Filters, die gleichen Vor- und Nachteile. Im schlimmsten Fall existiert ein Unternehmen, welches das Filtern als Dienstleistung anbietet, die Datenspeicherung jedoch outgesourct oder direkt durch ein weiteres externe Unternehmen durchführen lässt. Dann fungiert der Filter als Mittelpunkt einer Sternverkehrskommunikation. Dort laufen alle Daten und Informationen zusammen, welche zuvor über das Internet dorthin transportiert werden mussten. Von dem jetzt schon stattfindenden Transport des Uploads vom Nutzer zur Plattform ganz zu schweigen.

Unabhängig von der Infrastruktur sind auch die verwendeten Technologien nicht überzeugend. Ein direkter Vergleich von Daten bzw deren Hash-Codes beschränkt sich auf bereits bekannte Inhalte oder minimale Veränderungen von diesen. Sollen auch völlig unbekannte Uploads erkannt werden, müssen hier intelligente Filter zum Einsatz kommen. Dies basieren in der Regel auf neuronalen Netzen. Sie werden einmal ausreichend trainiert und können dann selbstständig Eingaben bewerten. Diesen haben nicht nur einen deutlich höheren Verbrauch an Ressourcen, sondern auch eine Fehlerrate von ca 1%. Das wären alleine 3,5 Mio. Bilder, die für Facebook falsch bewertet werden würden. Das heißt, ein Verhältnis von 50:50 angenommen,

werden 1,75 Mio. Bilder pro Tag fälschlicherweise freigeschaltet und 1,75 Mio. Bilder pro Tag fälschlicherweise nicht freigeschaltet. Alle nicht freigeschalteten Bilder können und müssen im Nachhinein händisch von einem Menschen kontrolliert und die Bewertung ggf geändert werden. Doch alles was einmal freigeschaltet wurde, ist aus dem Einzugsbereich des Filters raus. In diesem Fall greift nur noch das Prinzip, dass Nutzer auffällige Inhalte melden und diese darauf hin neu bewertet werden. Doch dieses Vorgehen wird bereits seit Jahren praktiziert ohne die Anwesenheit von Upload-Filtern.

Alles in Allem lässt sich festhalten: Upload-Filter sind eine sicherlich gut gemeinte, aber wahrscheinlich wirkungslose Maßnahme gegen kriminelle Aktivitäten im Internet.

Literatur

[Harhoff u. a. 2016] Harhoff, Dietmar ; Hilty, Reto M. ; Stürz, Roland A. ; Suyer, Alexander: *Movie Piracy and Displaced Sales in Europe: Evidence from Six Countries*. 09 2016

[Herz und Kiljanski 2016] Herz, Benedikt ; Kiljanski, Kamil: *Movie Piracy and Displaced Sales in Europe: Evidence from Six Countries*. 09 2016

[Kleinhans 2013] Kleinhans, Jan-Peter: *DNA und Tagesdecken im Kampf gegen Kindesmissbrauchs-Dokumentation Online*. 2013

[Schulzki-Haddouti 2017] Schulzki-Haddouti, Christiane: *Auswirkungen von Raubkopien: EU-Kommission unterdrückt Piraterie-Studie*. https://www.heise.de/newsticker/meldung/Auswirkungen-von-Raubkopien-EU-Kommission-unterdrueckt-Piraterie-Studie-3837330.html, 09 2017. – Zugegriffen am 01.06.2019

[Smith 2019a] Smith, Kit: *46 interessante Zahlen und Statistiken rund um YouTube*. https://www.brandwatch.com/de/blog/statistiken-youtube/, 01 2019. – Zugegriffen am 22.05.2019

[Smith 2019b] Smith, Kit: *Facebook in Zahlen: 53 interessante Statistiken*. https://www.brandwatch.com/de/blog/facebook-statistiken/, 02 2019. – Zugegriffen am 02.04.2019

[Spiller und Pohlmann 2014] Spiller, Ralf ; Pohlmann, Jens: *Länge der erfolgreichsten viralen Videos auf Youtube im Zeitraum von Januar 2011 bis Mai 2013*. https://de.statista.com/statistik/daten/studie/370590/umfrage/laenge-der-erfolgreichsten-viralen-videos-bei-youtube/, 11 2014. – Herkunftsnachweis: Horizont Nr. 48, 27.11.2014, Seite 26

[van der Ende; Joost Poort; Robert Haffner; Patrick de Bas; Anastasia Yagafarova; Sophie Rohlfs; Harry van Til 2015] Til, Martin van der Ende; Joost Poort; Robert Haffner; Patrick de Bas; Anastasia Yagafarova; Sophie Rohlfs; Harry v.: *Estimating displacement rates of copyrighted content in the EU*. 05 2015

[Youtube] Youtube: *So funktioniert Content ID*. https://support.google.com/youtube/answer/2797370?hl=de, . – Zugegriffen am 02.04.2019