Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

GUTACHTEN

ZUR ZIVILRECHTLICHEN VERANTWORTLICHKEIT

VON INTERNET-SERVICE PROVIDERN

IN DEUTSCHLAND, FRANKREICH, DÄNEMARK, DEM VEREINIGTEN KÖNIGREICH UND DEN VEREINIGTEN STAATEN VON AMERIKA

ENDVERSION

Avis 14-106

Lausanne, den 29. September 2015, Stand der Länderberichte 30.06.2015

Dorigny – CH – 1015 Lausanne - Tel : +41 (0)21 692 49 11 - Fax : +41 (0)21 692 4949 –
www.isdc.ch – info@isdc.ch

ZUSAMMENFASSUNG – EXECUTIVE SUMMARY

Die vorliegende Studie untersucht im Auftrag des Bundesamtes für Justiz die zivilrechtliche Verantwortlichkeit im weiteren Sinne (d.h. neben reparatorischen Ansprüchen wie Schadenersatz oder auch Publikation von Urteilen auch negatorische Ansprüche [Unterlassung] und Informationsansprüche der betroffenen Personen) von Plattformbetreibern und Internet-Providern. Die Studie soll zu Handen der interdepartementalen Arbeitsgruppe „Providerhaftung“ die Beurteilung der bestehenden Schweizer Regelungen im Hinblick auf eine allfällige Revision erleichtern. Dabei behandelt die Studie das europäische Recht sowie das deutsche, französische, englische, dänische und US-amerikanische Recht.

Im **Recht der Europäischen Union** sehen insbesondere die E-Commerce Richtlinie[1], die Durchsetzungsrichtlinie[2], die Urheberrechts- oder Informationsrichtlinie[3] sowie die Datenschutzrichtlinie[4] Bestimmungen vor, welche die zivilrechtliche Verantwortlichkeit von Internetdienstleistern betreffen. Bevor auf diese geltenden Bestimmungen eingegangen wird, ist jedoch darauf hinzuweisen, dass diese rechtliche Regelung aktuell auf europäischer Ebene **grundlegend überarbeitet** wird. In Evaluationen aller erwähnten Richtlinien wurde festgestellt, dass das geltende Instrumentarium u.a. angesichts der Herausforderungen im Online-Bereich nicht genügt. Die im Mai 2015 verabschiedete Strategie für einen digitalen Binnenmarkt in Europa[5] stellt nun eine umfassende Analyse der Haftung der Internetvermittler (Online-intermediaries) in Aussicht, wobei insbesondere eine Regelung des Melde- und Abhilfeverfahrens (*Notice und Take -Down -Procedure*) sowie die Einführung von Sorgfaltspflichten für Internetdienstleister geprüft werden. Auch das aktuell am weitesten fortgeschrittene Revisionsprojekt, die auf Ende 2015 geplante Datenschutz-Grundverordnung, wird in der Strategie als wichtiges Element zur Stärkung des Vertrauens in den Online-Bereich erwähnt. Hier könnten neue Ansprüche gegenüber Internetdienstleistern – mindestens soweit diese für die Datenverarbeitung verantwortlich sind – eingeführt werden, wobei sich die Positionen zwischen dem Europäischen Parlament und dem Rat gerade diesbezüglich noch unterscheiden.

Nach **aktuell geltendem Recht** sieht die E-Commerce Richtlinie im Abschnitt 4 (Verantwortlichkeit der Vermittler) ganz allgemein keine Verantwortlichkeit der Internetprovider vor, sondern führt **Haftungserleichterungen** für die Provider bei reiner Übermittlung, kurzer Zwischenspeicherung sowie unter gewissen Umständen auch bei der Beherbergung ein. Sie stellt ebenfalls fest, dass diese keine allgemeine Überwachungspflicht haben. Im Bereich des Urheberrechts schreibt Art. 8 Abs. 3 der

---

1 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr").

2 Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums (ABl. L 157 vom 30.4.2004).

3 Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (ABl. L 167 vom 22.06.2001).

4 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995).

5 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtscahfts- und Sozialausschuss und den Ausschuss der Regionen. Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192, vom 6.5.2015. Der vernetzte digitale Binnenmarkt ist in der Tat eine der Prioritäten im Rahmen der politischen Leitlinien für die Europäische Kommission 2014 – 2019, die diesbezüglich die digitale Agenda für Europa im Rahmen der Strategie Europa 2020 von 2010 (Mitteilung der Kommission vom 03.03.2020, EUROPA 2020, Eine Strategie für ein intelligentes, nachhaltiges und integratives Wachstum, COM(2010) 2020 endgültig, S. 16 f.) aufnimmt. Der digitale Binnenmarkt ist heute die 1. Säule der Agenda 2020, s. https://ec.europa.eu/digital-agenda/en/digital-agenda-europe-2020-strategy (10.07.2015) .

Urheberrechtsrichtlinie ausdrücklich vor, dass Inhaber von Schutzrechten gerichtliche Anordnungen gegen Vermittler (und damit auch Internet-Provider) beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden. Zudem sind Internetdienstleister von Art. 8 der Durchsetzungsrichtlinie betroffen, die einen Auskunftsanspruch gegenüber jeder Person vorsieht, die „nachweislich für rechtsverletzende Tätigkeiten genutzte Dienstleistungen in kommerziellem Ausmass" erbracht hat, und Art. 11 derselben Richtlinie schreibt vor, dass gerichtliche Anordnungen auch gegenüber dem Vermittler möglich sein müssen. Das Datenschutzrecht sieht schliesslich keine für Internetdienstleister spezifischen Ansprüche vor, aber die allgemeinen Ansprüche auf Auskunft, Berichtigung, Löschung und Sperrung sind grundsätzlich auch auf Internetdienstleister anwendbar, sofern diese entsprechende Daten verarbeiten.

Die europarechtlichen Ansprüche sowie das Haftungsprivileg von Internetdienstleistern waren Gegenstand verschiedener **Urteile des Europäischen Gerichtshofs**. In einem ersten Urteil[6] wurde festgestellt, dass zivilrechtliche Auskunftsansprüche (auf Information über Nutzer, welche Urheberrechte verletzen) nicht europarechtlich vorgeschrieben sind, dass diese aber unter gewissen Bedingungen (Verhältnismässigkeit) im nationalen Recht vorgesehen sein können. Eine Reihe von Urteilen im Immaterialgüterrecht erging zu Unterlassungsansprüchen (Ansprüchen auf Blockierung bzw. Filterung) gegenüber Internetdienstleistern. Demnach ist ein allgemeiner Anspruch auf Filterung europarechtlich weder für Access- noch für Content-Provider zulässig,[7] eine Anordnung auf Blockierung kann dies jedoch durchaus sein, sofern der (Access-)Provider die technische Massnahme selbst bestimmen kann und die Betroffenen angehört werden.[8] Die Möglichkeit von Unterlassungsansprüchen wurde auch gegenüber Online-Marktplätzen bestätigt, wobei neben deren Wissen oder Kontrollmöglichkeit des Inhalts insbesondere deren aktive Unterstützung für den Verkauf massgeblich war, dass keine Haftungsfreistellung angenommen wurde.[9] Eine ganze Reihe von Urteilen erging schliesslich zu Hyperlinks, deren Zulässigkeit in verschiedenen Formen (auch durch *Framing*) grundsätzlich bejaht wurde, sofern der verlinkte Inhalt frei zugänglich ist, d.h. sofern damit nicht Zugangsbegrenzungen der verlinkten Website zum Schutz des Werkes umgangen werden.[10] Das wohl bekannteste Urteil erging im Bereich des Datenschutzes, wo der datenschutzrechtliche Unterlassungsanspruch gegenüber Suchmaschinen bejaht wurde, da und soweit die ursprünglich zulässige Datenbearbeitung widerrechtlich geworden war, so dass insbesondere Links zu von Dritten veröffentlichten Internetseiten entfernt werden mussten.[11]

In den **nationalen Rechtsordnungen** wurden die europäischen Vorgaben auf unterschiedliche Art umgesetzt. In Frankreich wurde im Rahmen der Umsetzung der E-Commerce-Richtlinie eine relativ ausführliche Regelung erlassen, das deutsche und dänische Recht begnügen sich demgegenüber mit einer relativ wortgetreuen Umsetzung der europäischen Vorgaben (wobei in Deutschland angesichts des Konzepts der Störerhaftung eine Umsetzung von Art. 8 Abs. 1 der Richtlinie 2001/29/EG als hinfällig erschien), so dass sich insbesondere die Grundlage allfälliger Ansprüche weitgehend nach vorbestehendem nationalem Recht richtet. Im Vereinigten Königreich finden sich hingegen einige neuere Gesetze (Digital Economy Act 2010, Defamation Act 2013). So sieht der Digital Economy Act 2010 vor, dass gewisse Provider zur Prävention von Urheberrechtsverletzungen zum Treffen von „technischen Massnahmen" (Beschränkungen im Zugang zu den Dienstleistungen oder zu gewissem Material) gegenüber Kunden verpflichtet werden können, ihre Kunden über Rechtsverletzungen und die Rechteinhaber über rechtsverletzende Kunden informieren müssen, wobei soweit ersichtlich angesichts eines Memorandum of Understanding zwischen grossen Internetdienstleistern und der

---

6 C-275/06 (Promusicae).

7 C-360/10 und C-70/10 (SABAM).

8 C-314/12 (UPC Telekabel Wien).

9 C-324/09 (Oréal v. Ebay).

10 C-466/12 (Svensson), C-348/13 (Bestwater) sowie C-279/13 (C-More Entertainment).

11 C-131/12 (Google Spain).

„kreativen Industrie“ insbesondere im Unterhaltungsbereich (Musik, Film) auf die Umsetzung und Konkretisierung dieser Bestimmung verzichtet wird. Der Defamation Act 2013 sieht eine Anordnung zur Entfernung gewisser Inhalte (*Order to remove or cease distribution*) vor. Aus diesen Bestimmungen ergibt sich, dass die Privilegierungstatbestände der E-Commerce-Richtlinie nicht auf Auskunfts- und Unterlassungsansprüche angewendet werden. Dies scheint auch in den übrigen Rechtsordnungen der Fall zu sein.

Im **Bundesrecht der USA** sind zwei rechtliche Grundlagen zur Verantwortlichkeit von Internetdienstleistern relevant. Die eine sieht eine gewisse Haftungsbefreiung für Internetdienstleister im Bereich von ehrverletzenden und diffamierenden Äusserungen vor, die andere begrenzt die Verantwortlichkeit bei Urheberrechtsverletzungen (*copyright*) je nach Art des Internetdienstleisters. Im Markenrecht besteht keine spezifische gesetzliche Regelung, doch die Rechtsprechung hat sich mit der Verantwortlichkeit von Internetdienstleistern, insbesondere von Auktionsplattformen und Suchmaschinen, auseinandergesetzt. Dabei dreht sich die Rechtsprechung u.a. darum, wann und wie genau ein Internetdienstleisters von einer Rechtsverletzung haftungsbegründende Kenntnis hat, so dass die Rechtsprechung im Ergebnis zur Errichtung von **„Notice and Takedown“**-Verfahren geführt hat.

Vor allem in den USA, aber teilweise auch in der EU und in einigen Mitgliedstaaten (z.B. im Vereinigten Königreich) besteht zudem ein Trend, die Verantwortlichkeit von Internetdienstleistern nicht durch gesetzliche Vorschriften, sondern durch **Vereinbarungen (Memoranda of Understanding) zwischen den grösseren Dienstleistern und den grösseren Rechteinhabern** zu regulieren. Diese sehen in der Regel u.a. einen Informationsaustausch und eine Benachrichtigungspflicht der Dienstleister vor. Der Gesetzgeber bzw. die Aufsichtsbehörde über die Telekommunikation ist dabei oft mindestens beobachtend beteiligt und erleichtert teilweise sogar durch Inaussichtstellen einer verbindlichen Norm im Falle der Nichteinigung den Abschluss entsprechender Vereinbarungen. Dieser Ansatz bedingt allerdings das Vorhandensein grösserer Rechteinhaber als Verhandlungspartner und scheitert wohl deshalb insbesondere im Bereich des Datenschutzes und des Schutzes der Privatsphäre.

INHALTSVERZEICHNIS

I. SACHVERHALT

Anlässlich der Verabschiedung des Berichts "Rechtliche Basis für Social Media" hat der Bundesrat am 9. Oktober 2013 das EJPD beauftragt, "die zivilrechtliche Verantwortlichkeit von Plattformbetreibern und Providern zu prüfen und bis Ende 2015 bei allfälligem gesetzgeberischen Handlungsbedarf eine Vernehmlassungsvorlage zu erarbeiten."

Um die Beurteilung allfälliger Lücken und Mängel der bestehenden Schweizer Regelungen zu ermöglichen, soll eine rechtsvergleichende Studie im Ausland bestehende Regelungen sowie deren konkrete Umsetzung untersuchen.

Das Schweizerische Institut für Rechtsvergleichung (SIR) wurde beauftragt, ein rechtsvergleichendes Gutachten vorzulegen, das als Grundlage für die weiteren Arbeiten dienen soll. Das Gutachten sollte als Textbaustein zu einem allfälligen späteren Begleitbericht zum Vorentwurf oder aber zu einem Bericht, der die Gründe für den Verzicht auf gesetzgeberische Arbeiten darlegen würde, verwendbar sein. Auch ist vorgesehen, das Gutachten öffentlich zugänglich zu machen.

Dem Schweizerischen Institut für Rechtsvergleichung wurde eine vorläufige Fassung des Berichts der interdepartementalen Arbeitsgruppe Providerhaftung („IDA Providerhaftung“) vom 10. November 2014 zur Verfügung gestellt.

II. FRAGESTELLUNG

Das Gutachten soll die zivilrechtliche Verantwortlichkeit von Providern in Europa und in den USA zum Gegenstand haben. Die Arbeitsgruppe geht dabei von einem weiten Verständnis der "zivilrechtlichen Verantwortlichkeit" aus. Umfasst werden sowohl negatorische Ansprüche (Beseitigungs-, Unterlassungs- und Feststellungsbegehren etc.) als auch reparatorische Ansprüche (Schadenersatz, Genugtuung, Gewinnherausgabe, Publikation von Urteilen etc.) sowie Auskunftsansprüche. Auch der Provider-Begriff wird weit verstanden: Das Gutachten sollte neben den Ansprüchen gegen die klassischen Providertypen auch die zivilrechtliche Verantwortlichkeit von Plattform- und Suchmaschinenbetreibern behandeln.

Von der Arbeitsgruppe nicht vertieft behandelt werden vertragliche Ansprüche, da diese – soweit ersichtlich – keine besonderen Probleme aufwerfen. Weiter wird in Einklang mit dem Auftrag des Bundesrates die allfällige strafrechtliche Verantwortlichkeit von Providern nicht thematisiert. Diese beiden Aspekte können deshalb bei der Verfassung des Gutachtens weitgehend ausgeklammert werden bzw. sind nur soweit zu berücksichtigen, wie es für das Verständnis der Ausführungen erforderlich ist.

Nachfolgend werden die Aspekte aufgeführt, welche durch das Gutachten vertieft werden sollen. Die Liste der aufgeführten Aspekte und Fragestellungen ist nicht abschliessend oder unveränderlich; die Arbeitsgruppe ist offen für Vorschläge.

1. Wie werden die auf Provider anwendbaren speziellen zivilrechtlichen Verantwortlichkeitsbestimmungen (Handlungs- und Auskunftspflichten, Haftungsfreistellungen etc.) vom EuGH ausgelegt und angewendet? Hat der EuGH in seinen Urteilen und allfälligen sonstigen Stellungnahmen, Gutachten etc. Hinweise an den Gesetzgeber gemacht (wenn ja, welche)? Zu berücksichtigen sind unseres Erachtens insbesondere die Richtlinien 2000/31/EG (E-Commerce, namentlich Art. 12 ff.), 2004/48/EG (Durchsetzung, namentlich Art. 8),

2001/29/EG (Urheberrechts- oder Informationsrichtlinie, namentlich Art. 8 Abs. 3) sowie ferner die RL 95/46/EG (Datenschutz).

2. Gibt es Evaluationen der massgebenden EU-Richtlinien oder Pläne zu deren Revision (wenn ja, welche und mit welchen Ergebnissen)?

3. Wie wurden die massgebenden EU-Richtlinien in ausgewählten EU-Mitgliedstaaten umgesetzt (insbesondere Deutschland und Frankreich)? Wie ist die Rechtsprechung dazu (leading cases)? Welche Erfahrungen wurden mit diesen Regelungen gemacht, wo wurden in Rechtsprechung und Literatur allenfalls Mängel oder Lücken festgestellt?

4. Gelten in den ausgewählten EU-Mitgliedstaaten über die Vorgaben der erwähnten EU-Richtlinien hinaus für Provider spezielle zivilrechtliche Verantwortlichkeitsbestimmungen (wenn ja, welche)? Welche konkreten Erfahrungen bestehen in den ausgewählten EU-Mitgliedstaaten mit der Anwendung der allgemeinen zivilrechtlichen Verantwortlichkeitsbestimmungen auf Provider? Wie wird das Verhältnis zwischen diesen allgemeinen Ansprüchen und den untersuchten speziellen gemeinschafts- oder nationalrechtlichen Verantwortlichkeitsbestimmungen ausgestaltet?

5. Welche speziellen zivilrechtlichen Verantwortlichkeitsbestimmungen bestehen in den USA gegenüber Providern (Beispiel: Sec. 202(a) DMCA/17 U.S.C. § 512)? Welche Erfahrungen wurden damit gemacht? Welche Erfahrungen bestehen mit der Anwendung der allgemeinen zivilrechtlichen Verantwortlichkeitsbestimmungen auf Provider? In welchem Verhältnis stehen diese allgemeinen Regelungen zu den untersuchten speziellen Verantwortlichkeitsbestimmungen?

6. Bestehen in der EU oder den ausgewählten EU-Mitgliedstaaten besondere Regelungen zur Rechtsdurchsetzung gegenüber Providern:

   a) national (z.B. beschleunigte Zivilverfahren);
   b) bei grenzüberschreitenden Sachverhalten (z.B. spezielle IPR-Regelungen, allenfalls andere besondere Verfahren)? Wenn ja, wie sind diese ausgestaltet?

7. Bestehen in der EU oder den ausgewählten EU-Mitgliedstaaten Bestrebungen, Regelungen zur rascheren oder besseren Rechtsdurchsetzung gegenüber Providern zu schaffen (z.B. einerseits innerhalb der EU oder andererseits im Verhältnis zu Drittstaaten durch Abschluss bi- oder multilateraler Abkommen oder durch Gemeinschaftsrecht)?

8. Bestehen in den USA besondere Regelungen zur Rechtsdurchsetzung gegenüber Providern:

   a) national (z.B. „beschleunigte“ Zivilverfahren);
   b) bei grenzüberschreitenden Sachverhalten (z.B. spezielle IPR-Regelungen, allenfalls andere besondere Verfahren)?

   Wenn ja, wie sind diese ausgestaltet? Bestehen Bestrebungen solche Regelungen (z.B. durch Abschluss bi- oder multilateraler Abkommen) zu schaffen?

Entsprechend verschiedener Korrespondenz sowie angesichts der Kapazitäten und des Zeitrahmens werden im Gutachten das deutsche, französische und englische sowie als Vertreter der skandinavischen Rechtsordnungen das dänische Recht behandelt. Ebenfalls untersucht wird das US-amerikanische Bundesrecht.

Die Studie ist nach den verschiedenen untersuchten Rechtsordnungen gegliedert. Dabei werden Fragen 1, 2, 6 und 7 im ersten Teil (zur Europäischen Union) behandelt. Die übrigen Fragen (3, 4, 5, 6, 7 und 8) werden jeweils in zu jedem untersuchten Staat erstellten Länderberichten analysiert.

III. ANALYSE

A. RECHT DER EUROPÄISCHEN UNION

1. Evaluationen und Revisionspläne in der Europäischen Union

1.1. Die Strategie für einen digitalen Binnenmarkt in Europa

Am 6. Mai 2015 verabschiedete die Europäische Kommission die Strategie für einen digitalen Binnenmarkt für Europa.[12] Diese beruht auf den drei Säulen „Besserer Zugang für Verbraucher und Unternehmen zu digitalen Waren und Dienstleistungen in ganz Europa", „Schaffung der richtigen Bedingungen für florierende digitale Netze und Dienste" sowie „Bestmögliche Ausschöpfung des Wachstumspotenzials der europäischen digitalen Wirtschaft"[13] und stellt unter jeder Säule verschiedene Massnahmen in Aussicht.

Das Regulierungsumfeld für Internetplattformen und Mittler wird als ein wesentlicher Teil der **zweiten Säule** angesehen.[14] In diesem Rahmen soll noch vor Ende 2015 eine umfassende Untersuchung u.a. über die Beziehungen zwischen Plattformen und Anbietern sowie die Bekämpfung illegaler Inhalte im Internet in die Wege geleitet werden.[15] In den weitergehenden Unterlagen[16] wird die Haftung der Internet-Vermittler (*Liability of Online Intermediaries*) spezifisch angesprochen und auf die (Schwierigkeiten mit den) rechtlichen Rahmenbedingungen, insbesondere mit der E-Commerce Richtlinie (s. unten 1.2.) und der Durchsetzungsrichtlinie (s. unten 1.3.) eingegangen.[17]

Die Haftung von Internetprovidern und Plattformbetreibern wird aber auch von anderen Massnahmen betroffen. So ist die „Stärkung des Vertrauens (…) beim Umgang mit personenbezogenen Daten" eine weitere Stossrichtung der Massnamen im Rahmen der zweiten Säule.[18] Dabei wird davon ausgegangen, dass die Revisionen im Bereich des **Datenschutzrechts** (s. dazu unten, 1.4.) „das Vertrauen in die digitalen Dienste" verbessern wird.[19]

Schliesslich wird „ein modernes europäisches Urheberrecht" mit „ein[em] wirksame[n], ausgewogene[n] zivilrechtliche[n] Schutz gegen gewerbsmässige Urheberrechtsverletzungen" als entscheidender Faktor im Rahmen der **ersten Säule** angesehen.[20] Entsprechend werden **Rechtssetzungsvorschläge**

---

12 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtscahfts- und Sozialausschuss und den Ausschuss der Regionen. Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192, vom 6.5.2015. Der vernetzte digitale Binnenmarkt ist in der Tat eine der Prioritäten im Rahmen der politischen Leitlinien für die Europäische Kommission 2014 – 2019, die diesbezüglich die digitale Agenda für Europa im Rahmen der Strategie Europa 2020 von 2010 (Mitteilung der Kommission vom 03.03.2020, EUROPA 2020, Eine Strategie für ein intelligentes, nachhaltiges und integratives Wachstum, COM(2010) 2020 endgültig, S. 16 f.) aufnimmt. Der digitale Binnenmarkt ist heute die 1. Säule der Agenda 2020, s. https://ec.europa.eu/digital-agenda/en/digital-agenda-europe-2020-strategy (10.07.2015) .

13 COM(2015)192, S. 4.

14 COM(2015)192, S. 12 ff., Punkt 3.3.

15 COM(2015)192, S. 14.

16 Commission Staff Working Document. A Digital Single Market Strategy for Europe – Analysis and Evidence. Accompanying the document A Digital Single Market Strategy for Europe, SWD(2015) 100 final.

17 SWD(2015)100 final, S. 55 ff., 4.6.

18 COM(2015)192, S. 14 f., 3.4.

19 COM(2015)192, S. 15.

20 COM(2015)192, S. 7 f.

im Rahmen des Immaterialgüterrechts in Aussicht gestellt, dies mit dem Ziel einer „klareren Regelung der Tätigkeiten von Mittlern in Bezug auf urheberrechtlich geschützte Inhalte“[21] sowie einer „Modernisierung des Immaterialgüterrechtsschutzes“ (s. dazu unten, 1.3.).

Die Strategie für einen digitalen Binnenmarkt zeigt somit, dass die EU die **Kernbereiche der Vorschriften zur Haftung von Internetprovidern und –vermittlern überdenkt**, und dass auch weitere Regelungen diesbezüglich revidiert werden. Die entsprechenden Vorschriften zur Haftung von ISP könnten sich also in näherer Zeit wesentlich ändern.

1.2. Die E-Commerce Richtlinie

Wie erwähnt (1.1.) ist die Revision des Regulierungsumfelds für Plattformen und Mittler und damit die e-Commerce-Richtlinie[22] ein wesentlicher Bestandteil der Strategie für einen digitalen Binnenmarkt. Dabei hebt die Strategie die positive Wirkung des in der e-Commerce-Richtlinie verankerten Haftungsprivilegs hervor, weist aber auf **Probleme beim Umgang mit illegalen Inhalten** hin.[23] Die verschiedenen Kritikpunkte, welche im Folgenden ausgeführt werden, basieren im Wesentlichen auf Evaluationen und Vorarbeiten, insbesondere zwischen 2010 und 2013.[24]

Hauptpunkt der Kritik der Strategie und früherer Analysen und entsprechend auch Gegenstand der Vorarbeiten und Vorschläge waren und sind die **Verfahren zur Entfernung illegaler Inhalte** durch Betreiber von Hosting-Diensten.[25] Die E-Commerce-Richtlinie gewährt nach Art. 14 das Haftungsprivileg für Hosting-Provider nur, wenn diese unverzüglich nach Kenntnisnahme der Rechtswidrigkeit

---

21 COM(2015)192, S. 9.

22 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr").

23 COM(2015)192, S. 13.

24 Gemäss Art. 21 der Richtlinie 2000/31/EG muss ein entsprechender Bericht zusammen mit allfälligen Vorschlägen zur Änderung grundsätzlich zweijährlich vorgelegt werden; ein erster Bericht wurde 2003 vorgelegt (KOM(2003) 702 endg. vom 21.11.2003), es folgte 2007 insbesondere eine Studie im Auftrag der Kommission über die Haftung von Internetmittlern: T. Verbiest / G. Spindler / G.M. Riccio / A. van der Perré, Study on the Liability of Internet Intermediaries, 12.11.2007, verfügbar unter http://ec.europa.eu/internal_market/e-commerce/directive/index_de.htm (30.01.2015); nach Verabschiedung der digitalen Agenda 2010 (http://ec.europa.eu/digital-agenda/, 31.01.2015) erfolgte die Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Ein kohärenter Rahmen zur Stärkung des Vertrauens in den digitalen Binnenmarkt für elektronischen Handel und Online-Dienste. KOM(2011)942 endgültig (11.01.2012) mit einem Aktionsplan sowie einem Arbeitspapier zum Stand der Umsetzung und Anwendung der Richtlinie (Commission Staff Working Document SEC(2011) 1641 final, 11.01.2012, Online services, including e-commerce, in the Single Market, verfügbar unter http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf (31.01.2015)); am 23. April 2013, nach weiteren Konsultationen (insbesondere zu den Melde- und Abhilfeverfahren: A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries, http://ec.europa.eu/internal_market/consultations/2012/clean-and-open-internet_en.htm; insbesondere relevant ist die dazu veröffentlichte “Roadmap”, verfügbar unter http://ec.europa.eu/smartregulation/impact/planned_ia/docs/2012_markt_007_notice_and_takedown_procedures_en.pdf (31.01.2015) sowie nach Expertentreffen verabschiedete die Kommission einen Bericht über die Umsetzung des Aktionsplans „elektronischer Handel“ (Commission Staff Working Document, E-commerce Action Plan 2012-2015, State of play 2013, SWD(2013) 153 final).

25 COM(2015)192, S. 13; ausführlich bereits SWD(2013)153 final, S. 17: “In response to the 2010 public consultation on e-commerce, the vast majority and a wide variety of stakeholders indicated, in their contributions to the consultation, that changing the E-commerce Directive (ECD) would be undesirable.

einer Tatsache oder Information tätig werden, um die Information zu entfernen oder den Zugang zu sperren. Für die übrigen Arten von Providern ist die Abhilfe, d.h. das Unterbinden des Zugangs zu den Informationen, nicht in der Richtlinie geregelt. So bestehen in der Anwendung und Umsetzung laut der Kommission aus folgenden Gründen Schwierigkeiten und Rechtsunsicherheit:

1) Es besteht eine grosse **Fragmentierung** der Regeln zu den Melde- und Abhilfeverfahren. Einige Mitgliedstaaten haben gewisse Mitteilungs- und Abhilfeverfahren (mehrheitlich im Anwendungsbereich von Art. 12 und 13 der Richtlinie) geregelt, andere nicht.[26] Zudem haben verschiedene Akteure Melde- und Abhilfeverfahren durch Selbstregulierung eingerichtet[27] – ein Ansatz, der durch die Richtlinie explizit gefördert wird. Die grosse Zahl verschiedener Regelungen führt aber zu Unsicherheiten darüber, welches Verfahren massgeblich ist und ob gewisse Minimalanforderungen bestehen, insbesondere hinsichtlich der Anforderungen an eine Meldung, die zeitliche Dimension sowie die Möglichkeit der Stellungnahme des Betroffenen.[28] Soweit Art. 14 der Richtlinie betroffen ist, handelt es sich hier um eine Frage der Auslegung der Richtlinie (s. Punkt 2, unten). Die Möglichkeit der Stellungnahme ist insbesondere aufgrund von Verfahrensgarantien und der Meinungsäusserungsfreiheit relevant, wie auch die Kommission erwähnt.[29]
2) Die Voraussetzungen der Haftungsfreistellung, insbesondere zum Kriterium des „Wissens um die Illegalität eines Inhalts“ oder das „unverzügliche Tätigwerden“ i.S. von Art. 14 werden in der **Rechtsprechung verschiedener Mitgliedstaaten unterschiedlich ausgelegt**.[30]
3) Die Verfahren sind teilweise **langsam,** und bei verschiedenen Anbietern ist das Vorgehen diesbezüglich **intransparent**.[31]

Schon 2007 wurde die **Regelung von sogenannten Notice und Take-Down-Verfahren** vorgeschlagen.[32] Eine entsprechende Richtlinie scheint in Vorbereitung gewesen zu sein,[33] nachdem der Aktionsplan von 2011 „eine horizontale Initiative zu den Melde- und Abhilfeverfahren“[34] vorgesehen hatte und die

---

However, they also indicated that the functioning of notice-and-action procedures, in the context of Article 14 ECD, should be improved. In particular they considered that there is too much regulatory fragmentation and legal uncertainty, growing costs due to inefficiencies, too many instances of too slow action against illegal content and instances of action against legal content.” (Fussnote mit Hinweisen auf Art. 14 der Richtlinie weggelassen); die öffentliche Konsultation Public consultation on e-commerce of 2010, verfügbar unter: http://ec.europa.eu/internal_market/consultations/docs/2010/ecommerce/summary_report_en.pdf.

26 SWD(2011)1641 final, S. 42 f. erwähnt gesetzliche Massnahmen in Deutschland, Finnland, Frankreich, Litauen, Schweden, Spanien, Ungarn und dem Vereinigten Königreich; in Finnland scheint das Verfahren im Rahmen von Art. 14 zu gelten, wobei es auf das Urheberrecht beschränkt ist (Erster Bericht KOM(2003) 702, S. 16; s. auch Verbiest et al. (zit.), S. 12, wonach hauptsächlich die von der Richtlinie nicht geregelten Inforamtionsansprüche und die Blockierung Gegenstand der Rechtsprechung ist).

27 S. dazu auch die Länderberichte, z.B. zum Vereinigten Königreich.

28 Eine Verteidigungsmöglichkeit scheint in Finnland, Litauen, Spanien und dem Vereinigten Königreich vorgesehen, s. Erster Bericht KOM(2003) 702; s. auch SEC(2011)1641 final, S. 25 und 40 ff.

29 COM(2015)192, S. 14; s. auch SEC(2011) 1641, S. 45.

30 Verbiest et al. (zit.), S. 14 ff.; ausführlich SEC(2011)1641 final, S. 32 ff.

31 SWD(2015)100, S. 55 f.

32 Verbiest et al. (zit.).

33 A. Kuczerawy & J. Ausloss, NoC Online Intermediaries Case Studies Series: European Union and Google Spain, verfügbar unter https://lirias.kuleuven.be/bitstream/123456789/487619/1/NoC_EU+Google+Spain+case+study_AKJA.pdf (16.08.2015), S. 14.

34 KOM(2011)942 endgültig, zit., S. 17, Punkt 12 der Hauptmassnahmen des Aktionsplans.

Initiative auch im Bereich der Immaterialgüterrechte als Revisionsprojekt erwähnt worden war, wobei in jüngerer Zeit das Schicksal der entsprechenden Initiative unklar war.[35]

Ein zweiter Punkt, der vor allem in verschiedenen vorherigen Evaluationen erwähnt wird, sind Unklarheiten zum **Anwendungsbereich** der Richtlinie und insbesondere der Haftungsfreistellung angesichts des technischen Fortschritts, d.h. der laufenden Entwicklung von neuen Dienstleistungen und der wachsenden Menge digitaler Inhalte.[36] Es handelt sich dabei z.B. um die Anwendung der Richtlinie auf Hyperlinks, Suchmaschinen, Video-Sharing Seiten, Verkaufsplattformen, Blogs, soziale Netzwerke[37], wobei die Rechtsprechung sich mit verschiedenen Aspekten mittlerweile befasst hat (s. unten, 3.). Die Frage bleibt insofern aktuell, als dass die Strategie daran anknüpft und einräumt, dass es schwierig zu bestimmen ist, „was Mittler mit den von ihnen übermittelten, gespeicherten oder bereitgestellten Inhalten eigentlich tun dürfen“ [38], um von den Haftungsprivilegien profitieren zu können.[39] Aus dieser Formulierung lässt sich der Wille ableiten, den Anwendungsbereich von Art. 14 neu zu definieren, insbesondere aufgrund der Problematik der Big Data.

Der dritte Kritikpunkt, der in der Strategie und in verschiedenen vorherigen Evaluationen angesprochen wird, ist die Frage von **Sorgfaltspflichten der Internetdienstleister**. Die Richtlinie selbst verbietet den Mitgliedstaaten zwar in Art. 15 das Einführen einer allgemeinen Überwachungspflicht, nach Ziff. 47 Präambel können die Mitgliedstaaten aber in spezifischen Fällen durchaus entsprechende Überwachungspflichten vorsehen oder anordnen, und nach Präambel Ziff. 48 können Mitgliedstaaten Vermittlern, welche Informationen speichern, durchaus Sorgfaltspflichten zur Aufdeckung und Verhinderung bestimmter Arten rechtswidriger Tätigkeiten auferlegen. Es ist aber unklar, wo die Abgrenzung zwischen allgemeiner und spezifischer Überwachung bzw. bestimmten Arten von Tätigkeiten zu ziehen ist.[40] Insbesondere die gerichtlichen Anordnungen (*injunctions*) und Filterung werden in den verschiedenen Mitgliedstaaten oft unterschiedlich geregelt,[41] und es besteht auch auf europäischer Ebene Rechtsprechung dazu (s. dazu unten, 3.2.1. und 3.3.). Die entsprechenden Ansprüche gegenüber Hosting- und Caching-Provider sind ebenfalls nicht geregelt, doch diese Ansprüche (**Informationsansprüche und die Blockierung**) stehen im Vordergrund der nationalen Rechtsprechung.[42]

Ein letzter Kritikpunkt ist die **Koordination** der Richtlinie mit verschiedenen anderen **gemeinschaftsrechtlichen Rechtsakten** (Urheberrecht, Telekommunikation), welche eigentliche Anspruchsgrundlagen bilden, sowie teilweise auch Differenzen in der Umsetzung der entsprechenden Rechtsakte (s. dazu unten, 1.3.).[43]

Nachdem vor dem Strategiepapier von einer grundsätzlichen Überarbeitung der E-Commerce-Richtlinie (mit Ausnahme der oben erwähnten Initiative zu Melde- und Abhilfeverfahren) noch Abstand

---

35 S. z.B. Monica Horten, 2014, Notice of Action! Barnier to resurrect take-down directive, in Iptegrity.com 6 February 2014, verfügbar unter http://www.iptegrity.com/index.php/ipred/875 (31.01.2015).

36 COM(2015) 192, S. 14 ; SEC(2011)1641 final, S. 25.

37 SEC(2011)1641 final, S. 25 ; nach Verbiest et al. (zit.), S. 17 – 23 waren Hyperlinks und Suchmaschinen ein Bereich, der am meisten Probleme in der Rechtsprechung gab, wobei diese nach Auffassung der Autoren nicht geregelt waren.

38 COM(2015)192, S. 14

39 Die Formulierung könnte auf ein Anliegen der Stakeholder, erwähnt in SEC (2011) 1641 final, S. 43, zurückgehen.

40 SEC(2011)1641 final, S. 25 f. und S. 47 ff.

41 SEC(2011)1641 final, S. 47 ff.

42 Verbiest et al. (zit.), S. 12

43 SWD(2015) 100, S. 56 ; so bereits Verbiest et al., zit., S. 14 ff.

genommen worden war,[44] stellt die Kommission aufgrund der erwähnten Schwierigkeiten (sowie deren absehbarer Zunahme in Anbetracht der wachsenden Datenmenge) in der Strategie für einen digitalen Binnenmarkt eine umfassende Untersuchung der Rolle von Internetplattformen in Aussicht, die insbesondere analysiert, ob **neue Massnahmen zur Bekämpfung illegaler Inhalte** unter Berücksichtigung der Meinungsäusserungs- und Informationsfreiheit erforderlich sind. Im Zentrum stehen dabei die **Regulierung von *Notice und Take-Down*-Verfahren** und die Frage **allfälliger Sorgfaltspflichten** (inkl. möglicher Transparenzpflichten) der Internetdienstleister („Mittler") über die Art, wie die Netzwerke und Systeme verwaltet werden.[45] Die Frage der Haftungsfreistellung, die Melde- und Abhilfeverfahren sowie die Frage allfälliger Sorgfaltspflichten in Bezug auf die Überwachung und Betreibung der Internetdienstleistungen könnte also in mittlerer Zukunft durchaus einer fundamentalen Neuregulierung unterworfen werden.

1.3. Die Richtlinien im Immaterialgüterrecht

Wie bereits erwähnt (1.1.) stellt die Strategie für einen digitalen Binnenmarkt fest, dass die Tätigkeit der Online-Mittler in Bezug auf urheberrechtlich geschützte Inhalte **klarer geregelt** werden muss. Entsprechende Rechtssetzungsvorschläge sollen noch im Jahr 2015 unterbreitet werden.[46] Im Zentrum sollen (gemäss dem Grundsatz „follow the money") grosse kommerzielle Urheberrechtsverletzungen stehen, und es ist zu erwarten, dass Vorschläge einer Regulierung der Melde- und Abhilfeverfahren sich ebenfalls (wenn nicht gar in erster Linie) auf Urheberrechtsverletzungen beziehen.[47] Genauere Angaben zur Urheberrechtsreform seitens der Kommission liegen soweit ersichtlich nicht vor. Einige Anzeichen lassen sich jedoch einer Entschliessung des Europäischen Parlaments vom 9. Juli 2015 entnehmen. So schlägt das Europäische Parlament vor, dass „die Bestimmungen über die Haftung von Dienstleistungserbringern und Vermittlern" zu überprüfen seien „um zu garantieren", dass diese angemessene Sorgfalt wahren und dass die Urheber und Rechtsinhaber „eine gerechte Vergütung" erhalten.[48] Daraus lässt sich – ähnlich wie im Rahmen der e-commerce- Richtlinie – ableiten, dass neue Regeln möglicherweise Sorgfaltspflichten von Internetvermittlern vorsehen könnten. Erfolgsaussichten dieser Reformvorschläge sind jedoch schwierig einzuschätzen. [49]

---

44 SWD(2013)153 final, S. 17: In response to the 2010 public consultation on e-commerce, the vast majority and a wide variety of stakeholders indicated, in their contributions to the consultation, that changing the E-commerce Directive (ECD) would be undesirable. However, they also indicated that the functioning of notice-and-action procedures, in the context of Article 14 ECD, should be improved. In particular they considered that there is too much regulatory fragmentation and legal uncertainty, growing costs due to inefficiencies, too many instances of too slow action against illegal content and instances of action against legal content." (Fussnote mit Hinweisen auf Art. 14 der Richtlinie weggelassen); die öffentliche Konsultation Public consultation on e-commerce of 2010, verfügbar unter: http://ec.europa.eu/internal_market/consultations/docs/2010/ecommerce/summary_report_en.pdf.

45 COM(2015)192, S. 14; SWD(2015) 100, S. 56 f.

46 COM(2015)192, S. 9

47 SWD(2015)1641, S. 51; gemäss dem Blog-Beitrag vom 07.05.2015 von M. Horten auf dem Media Policy Blog der London School of Economics lassen sich drei Ansätze erkennen: follow the money, commercial scale infringement, Notice and Action, http://blogs.lse.ac.uk/mediapolicyproject/2015/05/07/european-commission-announces-radical-copyright-overhaul-for-cross-border-content/, wobei die Autorin grosse Schwierigkeiten bei der Umsetzung dieser Vorschläge voraussieht.

48 Ziffer 45 der Entschliessung des Europäischen Parlaments vom 09.07.2015 zur Umsetzung der Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informations-gesellschaft.

49 Gemäss dem Blog-Beitrag vom 07.05.2015 von M. Horten auf dem Media Policy Blog der London School of Economics, http://blogs.lse.ac.uk/mediapolicyproject/2015/05/07/european-commission-announces-radical-copyright-overhaul-for-cross-border-content/, ist gerade die Regelung der Internetdienst-leister politisch sehr heikel.

Die erwähnten Vorschläge basieren auf zwei Feststellungen: die eine steht im Zentrum der diesbezüglichen Erwägungen des Parlaments, die andere geht aus den Stellungsnahmen der Europäischen Kommission hervor. Nach Ansicht des Europäischen Parlaments sind die **Urheberrechtsinhaber gegenüber den Internetdienstleistern** (sozialen Medien, Plattformen, Suchmaschinen) **benachteiligt**, da letztere den Grossteil des dank geschützten Werken geschöpften Werts bei sich behalten und erstere kaum oder nicht vergütet werden, und da zudem die Macht bestimmter Vermittler zunehme.[50] Diesbezüglich spricht die Kommission in der Strategie zwar das Verhältnis zwischen Internetdienstleistern und Rechtsinhabern nicht an, streicht aber immerhin die steigende Bedeutung der Internetdienstleister im Bereich der Urheberrechte und die Notwendigkeit einer Vergütung für die Rechtsinhaber hervor.[51]

Die Kommission nennt als Grund für eine Überarbeitung der Richtlinien im Bereich des Immaterialgüterrechts in erster Linie die **unterschiedliche Umsetzung** der Bestimmungen zu Internetmittlern in der Durchsetzungsrichtlinie[52] und der Urheberrechtsrichtlinie[53] in den verschiedenen Mitgliedstaaten, wobei die Unterschiede auch durch die verschiedenen Haftungs- und Wettbewerbsrechte in den Mitgliedstaaten bedingt seien.[54] Nach öffentlicher Wahrnehmung sei es insbesondere schwierig, bei Online Verletzungen im gewerblichen Ausmass gerichtliche Anordnungen gegenüber Plattformen zu erhalten.[55] Auch im Bereich des Urheberrechts wird also die **Fragmentierung der Verfahren**, insbesondere für Anordnungen (*injunctions*) hervorgehoben.[56] Diese Beobachtungen finden sich teilweise bereits in Evaluationen der Durchsetzungsrichtlinie (1.3.1.) und der Urheberrechtsrichtlinie (1.3.2.).

1.3.1. Durchsetzungsrichtlinie

Über die Anwendung der **Durchsetzungsrichtlinie**[57] erstellte die Kommission erstmals am 22.12.2010 Bericht.[58] Dabei wird ausgeführt, „dass die derzeit verfügbaren legislativen und nichtlegislativen Instrumente nicht ausreichen, um Online-Verletzungen von Rechten des geistigen Eigentums wirksam zu bekämpfen.“[59] Im Anschluss wurden 2011 eine Konsultation zum Bericht und eine öffentliche

---

50 Entschliessung vom 09.07.2015, zit., Ziff. O und R.

51 KOM(2015)100 final, S. 8; s. dazu auch die Ankündigung des Kommissars Oettinger vom 22.06.2015, wonach die Verwendung von urheberrechtlich geschützten Materialien von Internet-Mittlern in einer Studie geklärt werden soll, Speech at DW Global Media Forum: The role of traditional and new media in the digital age – the EU view, verfügbar unter http://ec.europa.eu/commission/2014-2019/oettinger/announcements/speech-dw-global-media-forum-role-traditional-and-new-media-digital-age-eu-view_en (14.08.2015).

52 Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums (ABl. L 157 vom 30.4.2004).

53 Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (ABl. L 167 vom 22.06.2001).

54 SWD(2015)100 final, S. 30 und 56.

55 SWD(2015)100 final, S. 56, mit Verweis auf eine öffentliche Anhörung zur Umsetzungsrichtlinie im Juli 2013..

56 SWD(2015)100 final, S. 30 und 50.

57 Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums (ABl. L 157 vom 30.4.2004).

58 Bericht der Kommission an den Rat, das Europäische Parlament, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Anwendung der Richtlinie 2004/48/EG (…) zur Durchsetzung der Rechte des geistigen Eigentums, KOM(2010) 779 endgültig.

59 KOM(2010) 779 endgültig, zit., S. 7; s. dazu insbesondere auch COMMISSION STAFF WORKING DOCUMENT. Analysis of the application of Directive 2004/48/EC of the European Parliament and the

Anhörung zu den Herausforderungen im digitalen Umfeld durchgeführt. 2012 folgte eine Konferenz sowie eine Konsultation zur Wirksamkeit der Verfahren und der Zugänglichkeit der Massnahmen.[60] Auf der Grundlage dieser Vorarbeiten erstellte die Kommission 2014 einen Aktionsplan für einen neuen Konsens über die Durchführung der Immaterialgüterrechte, [61] der am November 2014 vom Rat angenommen wurde.[62] Interessanterweise erwähnt dieser Aktionsplan die Rolle der Internetdienstleister nicht direkt, auch wenn gewisse Aktionen (z.B. Sorgfaltspflichten in der Lieferkette, Aktion Nr. 2, oder Aktion Nr. 3 zu den Schutzrechtsrevisionen im Online-Bereich) diese durchaus betreffen könnten. Der Rat erinnert in seiner Entscheidung denn auch ausdrücklich daran, dass die Rolle „zwischengeschalteter Stellen bei der Unterstützung der Bekämpfung" von Verletzungen von Immaterialgüterrechten wichtig sei und fordert die Kommission auf, diese Aspekte zu berücksichtigen.[63] Im Rahmen des Arbeitspapier der Strategie zum digitalen Binnenmarkt wird eben diese Forderung aufgenommen, ohne dass dabei auf die möglichen Folgerungen eingegangen wird.[64]

Von grundlegender Bedeutung für die Durchsetzungsrichtlinie ist das **Memorandum of Understanding (MoU) vom 4. Mai 2011 über den Verkauf gefälschter Artikel auf Internetplattformen**,[65] das von vielen Stakeholdern (inkl. Branchenverbänden) unterzeichnet wurde, und das u.a. eine Zusammenarbeit der Berechtigten mit den Internetplattformen vorsieht. Dabei ist insbesondere ein Melde- und Abhilfeverfahren von einzelnen Verkaufsangeboten vorgesehen, aber auch verkäuferbasierte Mitteilungen an die Rechtsinhaber. In einem Bericht vom 18. April 2013 würdigte die Kommission diese Initiative als positiv und verlängerte sie um weitere zwei Jahre.[66] Der neue Bericht der Kommission liegt soweit ersichtlich noch nicht vor. Es ist aber durchaus möglich, dass der Erfolg bzw. das Abwarten der Erfahrungen mit dem MoU ein Grund sind, dass die Internetplattformen nicht ausdrücklich im Aktionsplan aufgenommen wurden, sondern dass man diesbezüglich eher auf „weiche" Massnahmen setzt.

Council of 29 April 2004 on the enforcement of intellectual property rights in the Member States, SEC(2010)1589 vom 22.12.2010.

60 S. http://ec.europa.eu/internal_market/iprenforcement/directive/index_de.htm mit den verschiedenen Zusammenfassungen; s. auch die Zusammenfassung dieses Prozesses in SWD(2013) 153 final, S. 18: "An extensive consultation was carried out on the application of Directive 2004/48 on civil IPR enforcement in 2012 culminating with a conference on 26 June 2012. It was decided to continue with the on-going public consultation on the functioning of the current civil enforcement system in the EU. In December 2012, the Commission services launched a survey to gather evidence to be used for a detailed and holistic evaluation of the efficiency of existing national IP civil enforcement systems, including those implementing IPRED. The survey also raised issues such as access to justice by SMEs and costs and duration of proceedings. The results of the survey will be made publicly available in June 2013, in line with the Commission's transparency procedures. Alongside harmonised measures, remedies and sanctions provided for by civil law, voluntary collaborative approaches can strengthen the protection of both right holders and consumers."

61 Mitteilung der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss EU-Aktionsplan für einen neuen Konsens über die Durchsetzung von Immaterialgüterrechten, KOM(2014)0392 endgültig; .

62 Text der Entscheidung des Rates verfügbar unter http://data.consilium.europa.eu/doc/document/ST-15321-2014-INIT/de/pdf (01.02.2015).

63 Entscheidung des Rates, zit., Ziffern 9 und 10.

64 SWD(2015)100 final, S. 51.

65 Verfügbar unter http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf (01.02.2015).

66 Bericht der Kommission an das Europäische Parlament und den Rat über die Wirkungsweise des Memorandum of Unterstanding (MoU) über den Internethandel mit gefälschten Waren KOM(2013) 209.

1.3.2. Urheberrechtsrichtlinie

Über die Anwendung der Urheberrechts- oder Informationsrichtlinie[67] erstattete die Kommission am 30. November 2007einen ersten Bericht,[68] der auch die Umsetzung von Art. 8 Abs. 3 der Richtlinie und die Anwendung auf Internetdienstleister (inkl. diejenigen, die von der Haftungsprivilegierung gemäss der E-Commerce-Richtlinie betroffen sind) behandelt.[69] Darauffolgende Konsultationen und Studien betreffen vereinzelt Internetdienstleister, so insbesondere die öffentliche Konsultation zur Überprüfung der Regeln zum EU-Urheberrecht, deren Ergebnisse im Juli 2014 publiziert wurden, und wonach die Meinungen zur allfälligen Weiterentwicklung der Haftung von Internetdienstleistern sehr geteilt sind.[70] Konkrete Vorschläge zur Umsetzung der Konsultationsergebnisse liegen soweit ersichtlich noch nicht vor. Wie bereits erwähnt begrüsst das Europäische Parlament in seiner Entschliessung vom 09.07.2015[71] den Willen der Kommission, einen Gesetzgebungsvorschlag zur Modernisierung vorzulegen und schlägt eine Überprüfung der Haftung von Vermittlern, auch im Hinblick auf die Sorgfaltspflichten vor.[72]

Eine Studie zur Anwendung der Direktive vom Dezember 2013[73] fokussiert auf andere Aspekte (insbesondere auf das ausschliessliche Recht des Urhebers, über den Zugang zu Werken zu bestimmen: *making available to the public*, , sowie auf Ausnahmeregelungen von Urheberrechten, insbesondere für Bibliotheken, wissenschaftliche Verwendung u.ä.) und berührt die Internetdienstleister lediglich diesbezüglich (s. zu den IPR-Aspekten unten, 2.).

---

67 Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (ABl. L 167 vom 22.06.2001).

68 Report to the Council, the European Parliament and the Economic and Social Committee on the application of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, Commission staff working document, SEC 2007(1556).

69 SEC 2007(1556), S. 9.

70 European Commission, DG Internal Market and Services, Directorate Intellectual Property – Copyright, Report on the responses to the Public Consultation on the Review of the EU Copyright Rules, 07.2014, verfügbar unter http://ec.europa.eu/internal_market/consultations/2013/copyright-rules/docs/contributions/consultation-report_en.pdf, S. 83: "Consumers generally do not favour further involvement of intermediaries, neither through a modification of the liability regime provided for in the E-Commerce Directive nor through the use of injunctions that would require internet service providers (ISPs) to monitor content and prevent future infringement. They are not in favour of any active involvement of ISPs in the detection and enforcement of IPR that would require the application of filtering technologies."; nach den Konsumenten wird der Schutz der Rechtsinhaber aktuell zu stark gewichtet; auch institutionelle Users sind sehr zurückhalten (S. 84); nach den Rechtsinhabern ist das aktuelle System langsam und veraltet, hier besteht das Bedürfnis nach mehr Haftung der Provider und nach klareren Regeln, besonders gegen Anonymität, und sie fordern grenzüberschreitende Durchsetzungsmechanismen; auch andere setzen sich für mehr Effizienz ein.

71 Entschliessung des Europäischen Parlaments vom 09.07.2015 zur Umsetzung der Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.

72 Ziffer 45 der Entschliessung.

73 J.P. Triaille (Hrsg.), Study on the application of Directive 2001/29/EC on copyright and related rights in the information society, verfügbar unter http://ec.europa.eu/internal_market/copyright/docs/studies/131216_study_en.pdf.

1.4. Die Datenschutzrichtlinie

Im Bereich der Datenschutzrichtlinie[74] scheinen die Revisionsarbeiten am weitesten fortgeschritten. So sieht die Strategie zum digitalen Binnenmarkt die **Datenschutz-Grundverordnung**,[75] die 2015 verabschiedet werden soll, [76] als wichtigen Schritt zur Erhöhung des Vertrauens in digitale Dienste. Die datenschutzrechtlichen Herausforderungen des Internets sind bereits im ersten Umsetzungsbericht von 2003 erwähnt worden,[77] und in einer Mitteilung vom 7. März 2007 ist in Aussicht gestellt worden, dass die Angemessenheit der Richtlinie im Zusammenhang mit dem Internet überprüft werden.[78] Der Entwurf von 2012 sieht zwar keine Sonderregeln für Internetdienstleister vor, führt aber im Hinblick auf ISP gewisse Vorschriften aus. So soll z.B. im Zusammenhang mit dem Recht auf Löschung das Recht auf Vergessenwerden eingeführt werden, was zu einer **Pflicht** der für die Datenbearbeitung verantwortlichen Person führt, nach einer Veröffentlichung der Daten **alle Schritte zu unternehmen, um Dritte über das Löschungsgesuch zu informieren**.[79] Die Kommission schlägt ebenfalls ein spezifisches Widerspruchsrecht gegen die Verarbeitung für Direktmarketing vor.[80]

Das **Europäische Parlament** hat am 12. März 2014 in erster Lesung verschiedene Änderungen am Entwurf beschlossen.[81] Dabei geht es insbesondere beim Recht auf Löschung (Art. 17 des Entwurfs) weiter als die Kommission und sieht insbesondere unter gewissen Voraussetzungen das Recht vor, die Löschung (auch von Links) direkt (also auch bei anderen Personen, als bei der für die Datenbearbeitung verantwortlichen Person) zu beantragen.[82] Ein weiterer Vorschlag des Parlaments besteht in einem Informationsanspruch der betroffenen Person über Personen, welche Daten erhalten haben und welche die für die Datenverarbeitung zuständige Person bei einem Löschungs- oder Änderungsgesuch nicht informieren kann (Art. 13).

---

74 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31–50).

75 Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) KOM (2012) 11 endgültig vom 25.01.2012.

76 So bereits die Mitteilungen anlässlich des Datenschutztages: http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm (31.01.2015).

77 Erster Bericht der Kommission über die Durchführung der Datenschutzrichtlinie vom 15.05.2003, KOM(2003) 265 endgültig.

78 Mitteilung der Kommission an das Europäische Parlament und an den Rat vom 7. März 2007: „Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie" [KOM(2007) 87 endgültig, S. 11.

79 Art. 17 und Präambel Nr. 54 des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) KOM (2012) 11 endgültig vom 25.01.2012**.**

80 Art. 19 des Vorschlags (KOM(2012)11 endgültig).

81 Legislative Entschliessung des Europäischen Parlaments vom 12. März 2014 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

82 S. für eine Gegenüberstellung der Versionen: Europäische Kommission, Factsheet on the Right tob e Forgotten Ruling. C-131/12, verfügbar unter http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (20.04.2015), S. 5.

Der Europäische Rat für Justiz- und Inneres hat am 15. Juni 2015 (nach zähen Verhandlungen[83]) eine **allgemeine Ausrichtung zur allgemeinen Datenschutzverordnung** festgelegt. Auf dieser Grundlage konnte der Rat in Verhandlungen mit dem Europäischen Parlament eintreten, um zu einer Einigung über die neuen Regeln zu kommen (Trilog; angesichts der Beteiligung der Kommission). Inhaltlich ist der Rat einiges restriktiver als die Kommission und das Parlament – z.B. um die Entwicklung von Technologien im Zusammenhang mit grossen Datenmengen (Big Data) besser unterstützen zu können[84] – gerade auch hinsichtlich der Verbraucherrechte.[85] Insbesondere die vom Parlament eingeführte Ausweitung des Rechts auf Löschung ist nicht vorgesehen, und auch die von der Kommission vorgeschlagene Pflicht zur Information Dritter bei einem Löschungsgesuch fällt weg.[86]

Der **Trilog** zwischen den Europäischen Institutionen hat Ende Juni 2015 begonnen, wobei die Verantwortlichkeitsvorschriften soweit ersichtlich noch nicht behandelt worden sind. Ob und welche Regelungen Verantwortlichkeitsansprüche der Internetdienstleister betreffen, kann noch nicht vorhergesagt werden. Der Europäische Datenschutzbeauftragte hat eine zugängliche Übersicht über die verschiedenen Standpunkte erstellt.[87]

Schliesslich kündigt die Strategie zum digitalen Binnenmarkt eine **Überprüfung der e-Datenschutz-Richtlinie**[88] an, insbesondere um eine Ausweitung des Anwendungsbereichs der Richtlinie, der aktuell

---

83 Partielle allgemeine Ausrichtungen zu den Aufischtsbehörden sowie zu den Grundsätzen für den Schutz personenbezogener Daten wurden bereits am 13.03.2015 verabschiedet: Rat der Europäischen Union, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) – Das Prinzip der zentralen Kontaktstelle, Drucksache 6833/15 vom 09.03.2015, verfügbar unter http://data.consilium.europa.eu/doc/document/ST-6833-2015-INIT/de/pdf (24.03.2015); Rat der Europäischen Union, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) – Kapitel II, Drucksache 6834/15 vom 09.03.2015, verfügbar unter http://data.consilium.europa.eu/doc/document/ST-6834-2015-INIT/de/pdf (24.03.2015).

84 A. Sauerbrey, die letzte Lobbyschlacht um den Datenschutz, Die Zeit (zeitonline) vom 15.06.2015, verfügbar unter http://www.zeit.de/digital/datenschutz/2015-06/eu-datenschutzgrundverordnung-ministerrat-trilog-lobbyismus (14.08.2015).

85 So allgemein: http://www.zeit.de/digital/datenschutz/2015-06/datenschutz-eu-reform-justizminister-luxemburg (14.08.2015).

86 Art. 17 des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) – Vorbereitung einer allgemeinen Ausrichtung, Dokument 9565/15 vom 11.06.2015, interinstitutionelles Dossier 2012/0011, verfügbar unter http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/de/pdf (13.08.2015); s. dazu allgemein die Kritik der ehemaligen Europäischen Kommissarin, Viviane Reding, an der Haltung des Rats, verfügbar unter www.euractiv.com/sections/infosociety(more-date-protection-better-less-315404 (14.08.2015) sowie die Diskussion der Lobbyinteressen: A. Sauerbrey, die letzte Lobbyschlacht um den Datenschutz, Die Zeit (zeitonline) vom 15.06.2015, verfügbar unter http://www.zeit.de/digital/datenschutz/2015-06/eu-datenschutzgrundverordnung-minis.

87 Comparative table of GDPR texts with EDPS recommendations, verfügbar unter https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_Annex_EN.pdf (27.08.2015).

88 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

auf herkömmliche Telekommunikationsunternehmen beschränkt ist, auf Anbieter von Kommunikationsdienstleistungen mit Hilfe des Internets zu überprüfen.[89] Dies könnte durchaus dazu führen, dass zivilrechtliche Auskunftsansprüche gegenüber Internetdienstleistern eingeführt werden (so z.B. in Art. 10 der aktuellen Verordnung die Aufhebung einer Rufnummernanzeigeblockierung zur Ermittlung eines Anrufers).

2. Rechtsdurchsetzung

Momentan gibt es in der EU keine besonderen Regelungen zur Rechtsdurchsetzung gegenüber Internetdienstleistern. Im Bereich der Immaterialgüterrechte bestehen jedoch verschiedene – insbesondere akademische – Initiativen zu internationalprivatrechtlichen Aspekten.[90] Seitens der EU wurde 2013 eine Studie im Auftrag der Kommission publiziert, welche die verschiedenen europäischen Regelungen und die dazu ergangene Rechtsprechung relativ ausführlich untersucht und dabei feststellt, dass angesichts der divergierenden nationalen Rechtsprechung erhebliche Rechtsunsicherheit besteht.[91] Konkrete Vorschläge, insbesondere zu Internetdienstleistern, scheinen aktuell aber nicht vorzuliegen.

3. Rechtsprechung

The civil liability of ISPs has been scrutinized in a number of cases by the Court of Justice of the European Union (CJEU).

3.1. Promusicae – disclosure requirements imposed on access ISP

The ***Promusicae*** case[92] was the first case in which the CJEU dealt specifically with obligations imposed on an Internet service provider. It concerned a Spanish organization of producers and publishers of musical and audio visual recordings seeking an order against Telefónica, an access ISP, to require that it turned over records identifying users who were allegedly infringing Promusicae's copyrights through file sharing software. The CJEU held that **EU law required that disclosure shall be available in case of criminal proceedings** but that member states were not required to lay down similar exceptions for civil-law disputes, such as the enforcement of Promusicae's copyrights.[93] However, the court did not preclude member states from having national legislation that had similar disclosure requirements for civil-law cases. In its finding the court emphasized that **national legislation must be proportionate** and

---

89 COM(2015)192, S. 15.

90 So z.B. T. Kono, Jurisdiction and Applicable Law in Matters of Intellectual Property in G.B. Dinwoodie, R.C. Dreyfuss & A. Kur, The Law Applicable to Secondary Liability in K. B. Brown & D. V. Snyder (Hrsg.), General Reports of the XVIIIth Congress of the International Academy of Comparative Law, Doprdrecht (Springer) 2012, S. 393 ff.; G. Dinwoodie et al., Intellectual Property Cases, NYU Journal of International Law and Politics Vol 42 (2009), S. 201 ff.

91 J.P. Triaille (Hrsg.), Study on the application of Directive 2001/29/EC on copyright and related rights in the information society, verfügbar unter http://ec.europa.eu/internal_market/copyright/docs/studies/131216_study_en.pdf, S. 63 ff.

92 Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 2008 E.C.R. I-00271.

93 Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 2008 E.C.R. I-00271, para 51.

strike a fair balance between the various fundamental rights protected under EU law, which in this case primarily concerned the right to (intellectual) property and the right to privacy.[94]

3.2. Copyright cases

3.2.1. SABAM cases – question of legality of general filtering systems for the prevention of copyrights infringements

The two ***SABAM*** cases[95] concerned a Belgian collecting society (SABAM) seeking an order for an Internet service provider (Scarlet) and a social media network (Netlog) to install a filter system to help prevent future copyright infringements facilitated by their respective services. SABAM relied on national legislation implementing Article 11 of the **Enforcement Directive** and Article 8(3) of the **Copyright Directive**.

In the first case, the CJEU held that an Internet service provider cannot be imposed such filtering and blocking obligation. The court concluded that the question of the appropriate relief had to be considered in light of other European instruments, as well as general principles of European Union law and fundamental rights enshrined in the Charter of Fundamental Rights of the European Union. In particular, the court referred to: (1) the E-Commerce Directive, which in Article 15 prohibits a general obligation on Internet service providers actively to monitor data; (2) the general principle of EU law that any relief be proportionate and (3) the fundamental right of "freedom to conduct a business" as guaranteed by Article 16 of the Charter. The court found that the **requested obligation to filter all data from all customers for any future infringement of intellectual property for an unlimited time violated all those principles**.[96] The court upheld this finding in the second SABAM case which concerned the social media network and thereby extended the reasoning applied to an *access* Internet Service Provider to services offered by a *content* Internet service providers.

3.2.2. UPC Telekabel Wien – blocking requirements on an access ISP may be lawful when the choice of appropriate blocking-measures is left to the ISP

Case ***UPC Telekabel Wien***[97]**,** similar to the SABAM cases, also concerned national legislation implementing Article 8(3) of the Copyright Directive. In this case, owners of the copyright in cinematographic works requested an Austrian court for an order requiring an Austrian ISP to block the access of its customers to websites on which allegedly infringing copies of the plaintiff's works were available. The **ISP did not host the websites in question**, but merely provided internet access to its customers who could access those websites. The CJEU had to consider whether the order in question was of the type that Member States were required by Article 8(3) to make available to copyright owners, and whether the particular Austrian procedure, which resulted in a general order to the ISP to achieve a particular outcome without detailing the specific measures to employ, was compatible with the fundamental rights of the ISP and its customers.

The court found that the Austrian procedure could, under certain circumstances, fulfil Austria's obligations under Article 8(3) and be compatible with fundamental rights enshrined in the Charter of

---

94 Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 2008 E.C.R. I-00271, paras 49 and 68.

95 Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, 2012 E.C.R. I-00000 and Case C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), 2011 E.C.R. I-11959.

96 For further comments and analysis of the SABAM cases see for example G. Dinwoodie, International Landscape of Secondary Liability, 37 Colum. J.L. & Arts 463 (2014). p. 494 et seq.

97 Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, 2014 E.C.R. I-00000.

Fundamental Rights of the European Union. In essence, the court held that a **website-blocking is lawful when the choice of appropriate blocking-measures is left to the ISP and provided that measures comply with the right of internet users to freedom of information**.[98] Further, the court noted that the injunction allowed the ISP to avoid liability by proving that it had taken all reasonable measures and that it will thus **not be required to make unbearable sacrifices** in particular in the light of the fact that it is not the author of the infringement.[99] Finally, the court stated that, in order to safeguard freedom of information for the ISP's customer, national procedural rules must provide a **possibility for internet users to assert their rights before the court** once the implementing measures taken by the internet service provider are known.[100] These conditions were deduced following a balancing of the three fundamental Charter interests implicated: the interests of the intellectual property owner under Article 17; the freedom of the ISP to conduct business under Article 16; and the freedom of expression of Internet users under Article 11.[101]

3.3. L'Oréal v. Ebay – liability of operator of online marketplace

In the ***L'Oréal v. Ebay***[102] case the CJEU had to examine the question of the liability of the operator of an online market place. The case, referred to the CJEU by an English court, concerned the sale of L'Oréal products without L'Oréal's consent on the eBay marketplace. L'Oréal argued *inter alia* that eBay was accessorily liable for the infringements allegedly committed by the sellers of goods who unlawfully used L'Oréal marks in their listings and that it was entitled to relief under Article 11 of the Enforcement Directive even if eBay was not itself liable for trademark infringement.

The court held that Article 14(1)(a) of the E-Commerce Directive must be interpreted as **not exempting from liability an operator of an online marketplace when the operator plays an active role** of such a kind as to give it knowledge of, or control over, the data relating to the offers for sale, when it provides assistance which entails, in particular, optimising the presentation of the online offers for sale or promoting those offers.[103] The court ruled that eBay, as operator of the website, plays such an active role when it optimizes the presentation of the offers for sale in question or promotes them.

Hence, the court made a distinction between cases where the website operator plays an active role by providing assistance in the sale process and cases where it does not. In the former, Article 14 of the E-Commerce Directive does not insulate it from liability, whereas in the latter it does. However, operator cannot rely on the exemption from liability if it "was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful and, in the event of it being so aware, failed to act expeditiously in accordance with Article 14(1)(b) of Directive 2000/31".[104]

---

98 Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, 2014 E.C.R. I-00000, paras 51-64.

99 Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, 2014 E.C.R. I-00000, para 53.

100 Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, 2014 E.C.R. I-00000, para 57.

101 For further comments and analysis of the SABAM cases see for example G. Dinwoodie, International Landscape of Secondary Liability, 37 Colum. J.L. & Arts 463 (2014). p. 496 et seq and See Faye Fangfei Wang, Site-blocking Orders in the EU: Justifications and Feasibility, in 14th Annual Intellectual Property Scholars Conference (IPSC), Boalt Hall School of Law, University of California, Berkeley, Aug. 7-8, 2014, available at https://www.law.berkeley.edu/files/Wang_Faye_Fangfei_IPSC_paper_2014.pdf (09.04.2015).

102 Case C-324/09, L'Oréal SA v. eBay Int'l AG, 2011 E.C.R. I-6011.

103 Case C-324/09, L'Oréal SA v. eBay Int'l AG, 2011 E.C.R. I-6011, para 116.

104 Case C-324/09, L'Oréal SA v. eBay Int'l AG, 2011 E.C.R. I-6011, para 124.

3.4. Hyperlinks and similar references

3.4.1. Svensson v. Retriever Sverige AB – liability of website operator for hyperlinking

In the ***Svensson v. Retriever Sverige AB*** case[105] the CJEU dealt with the question whether a website which redirects internet users through hyperlinks to protected works which are already freely available online infringe copyright in those works. In the case, referred by a Swedish court, several journalist had commenced court proceeding against an operator of a website which provided hyperlinks to the journalists' newspaper articles published on a newspaper website.

The CJEU found that, **since the articles had already been published and were freely available on the internet, the hyperlinking could not be considered as an unlawful "communication to the public"** under Article 3(1) of the Copyright Directive. The court reasoned that the authorisation of the copyright holders is not required for a communication as the one made by means of the hyperlinks since there is no new public, i.e. the public could access the articles freely on the newspaper's website without using the hyperlinks and were thus deemed to be potential recipients of the initial communication on the newspaper website. Hence, the public using the hyperlinks should be considered as being part of the public taken into account by the copyright holders when they authorised the initial communication.[106] From the ruling, it is clear that website operators are not liable for copyright infringement through links to content residing on third-party websites, unless they are aware that the link leads to illicit content, or the link would make it possible "to circumvent restrictions put in place by the site on which the protected work appears in order to restrict public access to that work [only] to the . . . site's subscribers."[107]

3.4.2. C-348/13 BestWater – liability of website operator for "framing"

The CJEU reiterated its finding in the *Svensson v. Retriever Sverige AB* in its recent decisions in cases ***C-348/13 BestWater***[108]and *C-279/13 C-More Entertainment*[109]. Case C-348/13 BestWater concerned the use of a two minutes long promotional video clip about water pollution, created by BestWater International, a producer and seller of water filters. The video appeared on YouTube, without BestWater's knowledge or authorisation, and was used by a competitor, who linked to the clip by means of "framing", thereby making the clip visible on its own website. BestWater claimed copyright infringement of its clip and commenced proceedings before a German court which referred the case to the CJEU. The CJEU held, in essence, **that embedding videos** (i.e., enabling users to view videos hosted on a different third-party website) **does not constitute a communication to the public if the videos are already freely accessible online**. The court thus considered that inserting a protected work that is freely available online onto another website "by way of a link, using the framing technique, such as that employed by BestWater", is not a communication to the public if that work is not communicated to a new public or by a different specific technical means than the original communication.

3.4.3. C-279/13 C-More Entertainment – liability for linking to live broadcast of sporting event

In case ***C-279/13 C-More Entertainment*** a Swedish court had referred a case between C More Entertainment AB and Mr Sandberg concerning the placing by Mr Sandberg on an internet site of **clickable links by means of which internet users can gain access to the live broadcast, on another**

---

105 Case C-466/12, Svensson v. Retriever Sverige AB, 2014 E.C.R. I-0000.

106 Case C-466/12 Svensson v. Retriever Sverige AB, 2014 E.C.R. I-0000, paras 27-28.

107 Case C-466/12 Svensson v. Retriever Sverige AB, 2014 E.C.R. I-0000, para 31.

108 Case C-348/13 BestWater International GmbH contre Michael Mebes et Stefan Potsch (2014) not yet reported.

109 Case C-279/13 C More Entertainment AB v Linus Sandberg (2015) not yet reported.

site, of ice hockey games without having to pay the sum asked by the operator of the other site. In other words, Mr Sandberg created links on his internet site enabling the paywall put in place by C More Entertainment to be circumvented. The question put forward by the Swedish court was if a Member State may give wider protection to the exclusive right of authors by enabling "communication to the public" to cover a greater range of acts than provided for in Article 3(2) of Directive 2001/29.

The CJEU held that Directive 2006/115[110] gives the Member States the **option of providing for more protective provisions with regard to the broadcasting and communication to the public of transmissions made by broadcasting organisations** than those which must be instituted in accordance with Article 8(3) of that directive. It then stated that Article 3(2) of Directive 2001/29 must be interpreted as not affecting the option open to the Member States, set out in Article 8(3) of Directive 2006/115, read in conjunction with recital 16 to that directive to grant broadcasting organisations the exclusive right to authorise or prohibit acts of communication to the public of their transmissions provided that such protection does not undermine the protection of copyright.[111]

3.5. Data Protection: Google Spain – search engines and the "right to be forgotten"

The E-Commerce Directive does not give any clear guidance on how to treat the situation of search engines with regards to liability for third party content. Instead, this issue was left to the discretion of the Member States and has therefore resulted in a variety of approaches on the national level.[112]

The ***Google Spain*** case [113] is known as the case deciding the matter of the "right to be forgotten". The facts of the case are the following: In 2010 a Spanish citizen lodged a complaint at the national Data Protection Authority against a Spanish newspaper and Google Spain and Google Inc. The citizen complained that an auction notice of his repossessed home on Google's search results infringed his privacy rights because the proceedings concerning him had been fully resolved for a number of years and that the reference to these was thus entirely irrelevant. He requested, first, that the newspaper be required either to remove or alter the pages in question so that the personal data relating to him no longer appeared; and second, that Google Spain or Google Inc. be required to remove the personal data relating to him, so that it no longer appeared in the search results.

The Spanish court referred the case to the CJEU with the following questions: (a) whether the Data Protection Directive applied to search engines such as Google; (b) whether the Directive applied to Google Spain, given that the company's data processing server was in the United States; (c) whether an individual has the right to request that his or her personal data be removed from accessibility via a search engine. In its ruling the CJEU that the Data Protection Directive applies to search engine operators such as Google if they have a branch or a subsidiary in a Member State which promotes the

---

110 Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property.

111 Case C-279/13 C More Entertainment AB v Linus Sandberg (2015) not yet reported, paras 35-37.

112 First Report on the Application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, at 13, COM (03) 0702, (November 21, 2003), available at: http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2003/0702/COM_COM(2003)0702_EN.pdf (14.04.2015), see also A. Kuczerawy and J. Ausloos, European Union and Google Spain, Interdisciplinary Centre for Law & ICT (ICRI), KU Leuven (2014), available at (14.04.2015).
https://publixphere.net/i/noc/page/OI_Case_Study_European_Union_and_Google_Spain

113 Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (May 13, 2014).

selling of advertising space offered by the search engine. Further, as regards the right to be forgotten, the Court ruled that even initially lawful processing of accurate data may, in the course of time, become **incompatible with the directive** where, **having regard to all the circumstances of the case, the data appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed** and in the light of the time that has elapsed.[114] Hence, the Court held that the right to be forgotten is not absolute but will be need to be balanced against other rights, such as the right of freedom of expression and of the media.[115] Therefore, a case-by-case assessment is needed considering the type of information concerned, its sensitivity for the individual's private life and the interest of the public in having access to that information.

The European Commission has commented the case and argued that the right to be forgotten is already covered in the existing Data Protection Directive, but that this principle needs to be updated and clarified for the digital age in accordance with the **proposal for the amended Data Protection Directive**.[116]

3.6. Concluding remarks

The EU legal framework governing ISP liability is rather complex. The rules are general in scope and it is for the Member States to choose the specific measures to put in place (information duties, blocking, indemnities etc.).

The role of the CJEU is to scrutinize that the measures available on national level are compatible with EU law, i.e. relevant Directives, general principles of EU law etc. The above discussed cases demonstrate that, in particular, matters related to privacy, right to freedom of expression, freedom of information and right to pursue a business must be taken into account alongside with claims of right to (intellectual) property. Further, national measures available to hinder or remedy copyright infringements on the internet shall be effective, proportionate and dissuasive and strike a fair balance between the various rights and interests at stake.

The recent decision *UPC Telekabel Wien* clearly demonstrates the extensive range of interests that needs to be taken into account when assessing secondary liability of copyright infringements. This case may have a major impact on future cases concerning blocking obligations imposed on access ISPs in the various Member States although it remains to be seen how the national courts will rule in the specific cases.

To our knowledge, there have been no comments or indications from the CJEU on *de lege ferenda* concerning ISP liability. Indeed, since there are many different kinds of ISPs, it is difficult to adopt a detailed one-size-fits-all liability standard. The advantage of the current rules is that they allow national legislators and courts to develop a spectrum of relief dynamically as technological and social change occurs.[117]

---

114 Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (May 13, 2014), paras 92-93.

115 Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (May 13, 2014), para 85.

116 See information from the European Commission, available at http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (14.04.2015) and http://ec.europa.eu/justice/data-protection/ (14.04.2015).

117 G. Dinwoodie, International Landscape of Secondary Liability, 37 Colum. J.L. & Arts 463 (2014). p. 501.

B. DEUTSCHLAND

1. Umsetzung des Europarechts

1.1. Überblick

Der deutsche Gesetzgeber hat die für das vorliegende Gutachten relevanten europäischen Richtlinien grösstenteils wörtlich umgesetzt. Lediglich Artikel 8 Absatz 3 der Urheberrechts-/Informationsrichtlinie wurde nicht umgesetzt, da dessen Inhalt bereits im deutschen Institut der sogenannten Störerhaftung ausreichend abgedeckt ist.

Lücken ergeben sich jedoch insbesondere für die Behandlung von Hyperlinks sowie von Suchmaschinen. Hierfür fordert die Literatur eine gesetzliche Regelung.

1.2. Umsetzung der Richtlinien

Mit Ausnahme von Artikel 8 Absatz 3 Richtlinie 2001/29/EG (Urheberrechts-/Informationsrichtlinie) hat der deutsche Gesetzgeber alle für das vorliegende Gutachten relevanten Richtlinien in nationalen Gesetzen umgesetzt. Dies betrifft Artikel 12-15 Richtlinie 2000/31/EG (E-Commerce-Richtlinie), Artikel 8 Richtlinie 2004/29/EG (Durchsetzungsrichtlinie) sowie Richtlinie 95/46/EG (Datenschutzrichtlinie).

Deutschland hat die Vorschriften der E-Commerce-Richtlinie über die Verantwortlichkeit der Vermittler nahezu wörtlich im Telemediengesetz und vor dessen Inkrafttreten im diesbezüglich wortgleichen Teledienstgesetz[118] umgesetzt. § 7 Absatz 1 Satz 1 Telemediengesetz enthält den in Artikel 15 Absatz 1 E-Commerce-Richtlinie festgelegten Grundsatz, dass Vermittelnde keine allgemeine Überwachungspflicht für fremde Inhalte trifft. Gleichzeitig stellt die Norm in Satz 2 jedoch auch klar, dass Vermittelnde dennoch nach den allgemeinen Gesetzen verpflichtet sein können, Informationen zu entfernen oder deren Nutzung zu sperren. Diese Ausnahme gestattet die E-Commerce-Richtlinie ausdrücklich im jeweils letzten Absatz der Artikel 12 bis 14.[119] Von der in Artikel 15 Absatz 2 E-Commerce-Richtlinie enthaltenen Möglichkeit, auch eine Meldepflicht der Vermittelnden an die zuständige Behörde über mutmasslich rechtswidrige Tätigkeiten oder Informationen ihrer Nutzer zu regeln, hat der Gesetzgeber jedoch keinen Gebrauch gemacht. Die in den Artikeln 12, 13 und 14 E-Commerce-Richtlinie vorgegebenen Richtlinien über die Haftung der Vermittelnden bei Durchleitung, Zwischenspeicherung (Caching) oder Speicherung (Hosting) von Informationen sind in den §§ 8 bis 10 Telemediengesetz geregelt.

Den in Artikel 8 Durchsetzungsrichtlinie geregelten Auskunftsanspruch zur Durchsetzung von Ansprüchen wegen Verletzung eines Rechts des geistigen Eigentums hat der deutsche Gesetzgeber in § 19 Markengesetz[120] sowie in § 101 Urhebergesetz umgesetzt. Auch hier hat er nahezu wörtlich den Wortlaut der Richtlinie verwendet. Die Norm enthält lediglich zwei Ausnahmen, die in Artikel 8 Durchsetzungsrichtlinie nicht ausdrücklich enthalten sind. Zum einen stellen das Markengesetz und das Urhebergesetz klar, dass kein Auskunftsanspruch gegen eine Person besteht, der im mittels dieser Auskunft durchzusetzenden Verfahren ein Zeugnisverweigerungsrecht nach der Zivilprozessordnung zusteht.[121] Damit wird eine Umgehung des Zeugnisverweigerungsrechts durch die anspruchsstellende

---

118 §§ 8-11 Teledienstgesetz (TDG).

119 Art. 12 Abs. 3, Art. 13 Abs. 2, Art. 14 Abs. 3 Richtlinie 2000/31/EG (E-Commerce-Richtlinie).

120 In Verbindung mit §§ 14, 15 Markengesetz (MarkenG), welche die mittels der Auskünfte durchzusetzenden Unterlassungs- und Schadensersatzansprüche regeln.

121 § 19 Abs. 2 S. 1 Hs. 2 Markengesetz (MarkenG); § 101 Abs. 2 S. 1 Hs. 2 Urhebergesetz (UrhG).

und später klagende Person verhindert. Zum anderen schliessen beide Gesetze einen Auskunftsanspruch aus, wenn dieser im Einzelfall unverhältnismässig ist.[122] Diese Ausnahme wird auf die Erwägungsgründe der Durchsetzungsrichtlinie gestützt, wonach die Vorschriften auch den „Rechten der Verteidigung Rechnung tragen [sollen]".[123] Zudem soll dies verhindern, dass Konkurrenten in einem nicht mehr zu rechtfertigenden Masse ausgeforscht werden.[124]

Die Datenschutzrichtlinie wurde in erster Linie im Bundesdatenschutzgesetz umgesetzt. Deutschland wurde vom Europäischen Gerichtshof jedoch gerügt, die Richtlinie teilweise falsch umgesetzt zu haben. Demnach widerspreche der Datenschutzrichtlinie, dass diejenigen Stellen, die in den einzelnen Bundesländern die nichtöffentlichen Stellen und öffentlich-rechtlichen Wettbewerbsunternehmen bei deren Verarbeitung personenbezogener Daten überwachen, einer staatlichen Aufsicht unterstehen. Dadurch sei das Erfordernis der Datenschutzrichtlinie, diese Stellen ihre Aufgaben „in völliger Unabhängigkeit"[125] wahrnehmen zu lassen, falsch umgesetzt worden.[126]

Von den für dieses Gutachten relevanten Richtlinien wurde lediglich Artikel 8 Absatz 3 Urheberrechts-/Informationsrichtlinie nicht in eine eigene Vorschrift umgesetzt. Grund hierfür ist, dass der Gesetzgeber die bereits in Rechtsprechung und Literatur entwickelte sogenannte Störerhaftung[127] als ausreichend ansah.[128] Nach ständiger Rechtsprechung des Europäischen Gerichtshofs scheidet bei Richtlinien auch eine direkte Anwendung in Rechtsstreitigkeiten aus, wenn ausschliesslich Privatpersonen beteiligt sind,[129] wie es bei Fällen des Artikel 8 Absatz 3 Urheberrechts-/Informationsrichtlinie in der Regel der Fall sein wird. Selbst in Fällen, in denen der Staat als geschädigter Rechtsinhaber oder gar als Vermittler auftreten sollte, wird der Staat in dieser Hinsicht regelmässig nicht hoheitlich auftreten, sondern als Privatperson. Mithin richten sich Fälle des Artikel 8 Absatz 3 Urheberrechts-/Informationsrichtlinie in Deutschland allein nach der Störerhaftung.

1.3. Rechtsprechung

Erst Ende des Jahres 2014 hat das Landgericht München I dem Europäischen Gerichtshof einen Fragenkatalog zur Auslegung insbesondere des Artikel 12 Absatz 1 E-Commerce-Richtlinie vorgelegt.[130] Bis zur Entscheidung des Europäischen Gerichtshofs über diese Fragen hat das Gericht das von ihm zu entscheidende Verfahren ausgesetzt. In diesem Verfahren geht es um die Haftung eines WLAN-Betreibers als Access Provider, welcher das WLAN ohne Passwort betrieben und bewusst auch Dritten zugänglich gemacht hat. Die Fragen des Landgerichts München I an den Europäischen Gerichtshof beziehen sich auf die folgenden Formulierungen und Unklarheiten:

---

122 § 19 Abs. 4 Markengesetz (MarkenG); § 101 Abs. 4 Urhebergesetz (UrhG).

123 ErwGrd. 20 S. 2 Richtlinie 2004/29/EG (Durchsetzungsrichtlinie).

124 R. Ingerl/C. Rohnke, Markengesetz, 3. Aufl., München 2010, § 19 Rn. 37.

125 Art. 28 Abs. 1 Unterabs. 2 Richtlinie 95/46/EG (Datenschutzrichtlinie).

126 Europäischer Gerichtshof (EuGH), Urteil vom 09.03.2010 – C‑518/07.

127 Siehe hierzu Punkt 2.3. dieses Gutachtens zum deutschen Recht.

128 Deutscher Bundestag, Drucksache 15/38 vom 06.11.2002, Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft, S. 39 f.; Oberlandesgericht (OLG) Köln, Urteil vom 18.7.2014 – 6 U 192/11; M. Leistner & K. Grisse, Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 1), Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 2015, S. 19 ff., S. 19 f.; vgl. zu Art. 11 S. 3 Richtlinie 2004/29/EG (Durchsetzungsrichtlinie) auch Bundesgerichtshof (BGH), Urteil vom 19.04.2007 – I ZR 35/04.

129 Europäischer Gerichtshof (EuGH), Urteil vom 10.04.1984 – Rs 14/83; EuGH, Urteil vom 05.10.2004 – C-397/01 bis C-403/01.

130 Landgericht (LG) München I, Beschluss vom 18.09.2014 – 7 O 14719/12.

- „in der Regel gegen Entgelt“ (Art. 12 Abs. 1 Hs. 1 in Verbindung mit Art. 2 lit. b) E-Commerce-Richtlinie in Verbindung mit Art. 1 Nr. 2 Richtlinie 98/48/EG)
- „Zugang zu einem Kommunikationsnetzwerk zu vermitteln“ (Art. 12 Abs. 1 Hs. 1 E-Commerce-Richtlinie)
- „anbieten“ (Art. 12 Abs. 1 Hs. 1 in Verbindung mit Art. 2 lit. b) E-Commerce-Richtlinie)
- „nicht für die übermittelten Informationen verantwortlich“ (Art. 12 Abs. 1 Hs. 1 E-Commerce-Richtlinie)
- Befugnis nationaler Richter, gegenüber Access Providern anzuordnen, es künftig zu unterlassen, Dritten über einen konkreten Internetanschluss das Bereitstellen eines konkreten urheberrechtliche geschützten Werkes über Internet-Tauschbörsen zu ermöglichen (Art. 12 Abs. 1 Hs. 1 in Verbindung mit Abs. 3 E-Commerce-Richtlinie)
- Analoge Anwendbarkeit des Artikel 14 Absatz 1 Buchstabe b) E-Commerce-Richtlinie auf Unterlassungsansprüche (Art. 12 Abs. 1 Hs. 1 E-Commerce-Richtlinie)
- Anforderungen an Diensteanbieter (Art. 12 Abs. 1 Hs. 1 in Verbindung mit Art. 2 lit. b) E-Commerce-Richtlinie)
- Entgegenstehen des Artikels 12 Absatz 1 Halbsatz 1 E-Commerce-Richtlinie gegen Entscheidung nationaler Richter, gegenüber Access Providern für diese kostenpflichtig anzuordnen, es künftig zu unterlassen, Dritten über einen konkreten Internetanschluss das Bereitstellen eines konkreten urheberrechtliche geschützten Werkes über Internet-Tauschbörsen zu ermöglichen, wobei die Wahl der technische Massnahme dem Access Provider frei stünde (Art. 12 Abs. 1 Hs. 1 E-Commerce-Richtlinie)
- Entgegenstehen des Artikels 12 Absatz 1 Halbsatz 1 E-Commerce-Richtlinie gegen Entscheidung nationaler Richter, gegenüber Access Providern für diese kostenpflichtig anzuordnen, es künftig zu unterlassen, Dritten über einen konkreten Internetanschluss das Bereitstellen eines konkreten urheberrechtliche geschützten Werkes über Internet-Tauschbörsen zu ermöglichen, wobei die Wahl der technische Massnahme dem Access Provider zwar frei stünde, faktisch jedoch auf eine Stilllegung des Internetanschlusses, auf das Einführen eines Passwortes oder auf ein Untersuchen sämtlicher Kommunikation beschränkt wäre (Art. 12 Abs. 1 Hs. 1 E-Commerce-Richtlinie).[131]

Im Hinblick auf den in Artikel 8 Durchsetzungsrichtlinie geregelten Auskunftsanspruch hat der Bundesgerichtshof klargestellt, es sei auch zulässig, im nationalen Recht einen über die Fälle des Artikel 8 Durchsetzungsrichtlinie hinausgehenden[132] Auskunftsanspruch zu regeln. Dies ergebe sich aus Artikel 8 Absatz 3 Buchstabe a) dieser Richtlinie, wonach die Staaten dem Rechtsinhaber auch weitergehende Auskunftsansprüche einräumen dürfen.[133]

Von dieser Entscheidung und dieser Vorlage zum Europäischen Gerichtshof abgesehen hat unsere Recherche keine Rechtsprechung ergeben, die sich spezifisch mit den hier relevanten europäischen Richtlinien oder deren Umsetzung in das deutsche Recht befasst. Grund hierfür ist vermutlich, dass die Richtlinien nahezu wörtlich in das deutsche Recht übernommen wurden. Daher erwähnt die Rechtsprechung in ihren Entscheidungen die jeweilige Richtlinie in der Regel nur der Form halber, geht dann jedoch ausschliesslich auf die Behandlung und Auslegung der Vorschriften des nationalen deutschen Rechts ein. Für diese Rechtsprechung zum nationalen Recht siehe ausführlich unten, 2.3.

---

131 Landgericht (LG) München I, Beschluss vom 18.09.2014 – 7 O 14719/12.

132 In diesem Fall ging es um das Bestehen eines Auskunftsanspruchs gegenüber einer dritten Person nicht nur in Fällen einer Rechtsverletzung in gewerblichem Ausmasses, Bundesgerichtshof (BGH), Beschluss vom 19.04.2012 – I ZB 80/11 (*Alles kann besser werden*).

133 Bundesgerichtshof (BGH), Beschluss vom 19.04.2012 – I ZB 80/11 (*Alles kann besser werden*); sich anschliessend BGH, Beschluss vom 16.05.2013 – I ZB 50/12 und BGH, Beschluss vom 16.05.2013 – I ZB 25/12; andere Ansicht noch Oberlandesgericht (OLG) Köln, Beschluss vom 13.10.2011 – 6 W 223/11.

1.4. Allfällige Lücken und Schwierigkeiten

Das Bundesministerium für Wirtschaft und Energie hat im Juni 2015 einen überarbeiteten **Referentenentwurf** veröffentlicht, welcher eine **Änderung des Telemediengesetzes** enthält.[134] Ein solcher Referentenentwurf muss zunächst von der Regierung genehmigt werden und wird sodann als sogenannter Regierungsentwurf im Gesetzgebungsverfahren in Bundestag und Bundesrat diskutiert, bevor er angenommen und als Gesetz verabschiedet werden kann. Am 15. Juni 2015 wurde dieser Entwurf bei der Europäischen Kommission notifiziert und kann nun bis zum 16. September von der Kommission sowie von den Mitgliedstaaten kommentiert werden.[135]

Dieser Referentenentwurf **erweitert die Haftung von Host Providern auf Schadensersatz**, um so eine Durchsetzung insbesondere des Rechts auf geistiges Eigentum gegenüber Host Providern zu erleichtern.[136] Demnach soll an § 10 Telemediengesetz ein Absatz hinzugefügt werden. Dieser Absatz enthält eine **Vermutung und dadurch eine Beweislastumkehr** dafür, dass dem Host Provider Tatsachen oder Umstände **bekannt** sind, aus denen die rechtswidrige Handlung stammt, wenn es sich bei dem jeweiligen Host Provider um einen **„besonders gefahrgeneigten Dienst“** handelt.[137] Mit dieser Regelung sollen diejenigen Host Provider zur Verantwortung gezogen werden können, bei denen nach allgemeiner Lebenserfahrung davon ausgegangen werden kann, dass ihnen die rechtswidrigen Tatsachen und Informationen bekannt sind.

Mit der darauf folgenden Aufzählung[138] von **vier Konstellationen, in welchen dies in der Regel der Fall sei**, soll mehr Rechtsklarheit geschaffen werden. Demnach solle es sich um einen solchen besonders gefahrgeneigten Dienst insbesondere dann handeln, wenn die weit überwiegende Anzahl der vom Host Provider gespeicherten oder verwendeten Informationen rechtswidrig sei. Massgebend sei hierfür keine absolute Zahl, sondern ein relativer Wert von weit über 50% der gespeicherten Informationen. Eine zweite mögliche Konstellation sei, dass der Host Provider eine solch rechtswidrige Nutzung

---

134 Bundesministerium für Wirtschaft und Energie, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) vom 15.06.2015, abrufbar unter http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan,did=695334.html (22.07.2015).

135 Bundesministerium für Wirtschaft und Energie, Mehr Rechtssicherheit bei WLAN: Geänderter Gesetzesentwurf bringt erhebliche Vereinfachungen, verfügbar unter http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan,did=695334.html (22.07.2015); zum Notifizierungsverfahren siehe auch EUROPÄISCHE KOMMISSION, Das Notifizierungsverfahren in Kürze, verfügbar unter http://ec.europa.eu/growth/tools-databases/tris/de/about-the-9834/the-notification-procedure-in-brief1/ (22.07.2015).

136 Bundesministerium für Wirtschaft und Energie, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) vom 15.06.2015, abrufbar unter http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan,did=695334.html (22.07.2015), S. 15 f.

137 Bundesministerium für Wirtschaft und Energie, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) vom 15.06.2015, abrufbar unter http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan,did=695334.html (22.07.2015), S. 7, dort § 10 Abs. 2 S. 1 Telemedienreferentenentwurf (TMGRefEntw).

138 Bundesministerium für Wirtschaft und Energie, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) vom 15.06.2015, abrufbar unter http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan,did=695334.html (22.07.2015), S. 7, dort § 10 Abs. 2 S. 2 Nr. 1-4 Telemedienreferentenentwurf (TMGRefEntw).

durch eigene Massnahmen gezielt fördere. Hier sei entscheidend, dass der Host Provider eine rechtswidrige Nutzung zielgerichtet fördere, eine Förderung lediglich der Gefahr rechtswidriger Nutzungen sei hingegen nicht ausreichend. Drittens solle es sich auch dann um einen besonders gefahrgeneigten Dienst handeln, wenn der Host Provider damit werbe, Rechtsverstösse auf seiner Internetseite seien nicht verfolgbar. Die Werbung müsse gezielt darauf hinweisen, dass die Internetseite so konstruiert sei, dass auch bei Rechtsverstössen keine Verfolgung drohe. Schliesslich nennt der Referentenentwurf als vierte Konstellation, wenn keine Möglichkeit bestehe, die rechtswidrigen Inhalte durch die in ihrem Recht verletzte Person entfernen zu lassen. Dies sei beispielsweise dann der Fall, wenn entweder die berechtigte Person den Host Provider nicht über den rechtswidrigen Inhalt informieren könne oder der Host Provider den rechtswidrigen Inhalt nicht entfernen könne.[139]

Auch im Hinblick auf die **Haftung von Access Providern** enthält der Referentenentwurf eine Neuerung. In der jüngsten Vergangenheit hat sich Gerichten wiederholt die Frage gestellt, ob Betreibende eines WLAN als Access Provider anzusehen sind.[140] Diese Rechtsunsicherheit führt auch dazu, dass beispielsweise Betreibende von Cafés oder anderen privaten oder auch öffentlichen Einrichtungen wie Bibliotheken derzeit oft kein WLAN für Ihre Kunden anbieten. Um jedoch eine breite Abdeckung mit WLAN in der Öffentlichkeit zu ermöglichen, hat das Bundesministerium für Wirtschaft und Energie in seinem Referentenentwurf auch eine Änderung des § 8 Telemediengesetz vorgesehen, welcher sich mit der Haftung von Access Providern befasst.

Der Referentenentwurf stellt klar, dass **Betreibende eines WLAN Access Providern im Sinne des Telemediengesetzes gleichgestellt sind**. Sie **haften somit nur im beschränkten Rahmen der E-Commerce-Richtlinie auf Schadensersatz**.[141] Darüber hinaus sollen Betreibende eines WLAN[142] auch auf **Beseitigung und Unterlassung** wegen einer rechtswidrigen Handlung von Nutzenden dieses WLANs nur dann haften, wenn sie **keine zumutbaren Massnahmen ergriffen** haben, um diese rechtswidrige Nutzung zu verhindern. Betreibende eines WLAN können sich demnach von der Haftung

---

139 Bundesministerium für Wirtschaft und Energie, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) vom 15.06.2015, abrufbar unter http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan,did=695334.html (22.07.2015), S. 16 f.

140 Siehe hierzu unten, 2.3.1.2.

141 Bundesministerium für Wirtschaft und Energie, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) vom 15.06.2015, abrufbar unter http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan,did=695334.html (22.07.2015), S. 6, dort § 8 Abs. 3 Telemedienreferentenentwurf (TMGRefEntw).

142 Die ursprüngliche Fassung dieses Referentenentwurfs sah vor, dies nur auf solche WLAN-Betreibende anzuwenden, die ihr WLAN geschäftsmässig zur Verfügung stellen (sowohl mit als auch ohne Gewinnerzielungsabsicht, wie Hotels, Internet-Cafés, Arztpraxen oder Sportvereine) sowie auf öffentliche Einrichtungen (wie Bibliotheken, Schulen, Universitäten, Bürgerämter oder Freizeitanlagen). Private WLAN-Betreibende sollte die gleiche Sorgfaltspflicht treffen, jedoch mit der zusätzlichen Voraussetzung, dass diese die Person, die ihr WLAN nutzt, auch namentlich kennen sollten; Bundesministerium für Wirtschaft und Energie, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) vom 11.03.2015, abrufbar unter https://www.bmwi.de/BMWi/Redaktion/PDF/ST/telemedienaenderungsgesetz,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (22.07.2015), S. 4, 5, 6, 11, 12.

auf Unterlassen wegen Rechtsverstössen Dritter befreien, wenn sie „angemessene Sicherungsmassnahmen gegen den unberechtigten Zugriff […] durch aussenstehende Dritte ergriffen ha[ben]".[143] Um der Technologieneutralität Rechnung zu tragen nennt diese überarbeitete Fassung des ersten Referentenentwurfs keine bestimmten Sicherheitsmassnahmen. Aus dem Kommentar zum Entwurf geht jedoch hervor, dass eine Verschlüsselung des Routers in Betracht komme, wie beispielsweise in Form des WPA2-Standards.[144] Darüber hinaus dürfen die WLAN Betreibenden Zugang zum Internet nur solchen Personen gewähren, die erklärt haben, bei der Nutzung des WLAN keine Rechtsverstösse zu begehen.[145] Dies könne beispielsweise durch ein anzuklickendes Kästchen mit den Nutzungsbedingungen zu Beginn der Internetnutzung geschehen. Ebenso könnten die Betreibenden des WLAN den Nutzenden ein Passwort zusammen mit den Nutzungsbedingungen aushändigen.[146]

Nicht von diesem Referentenentwurf erfasst sind jedoch die Haftung von Suchmaschinen und Hyperlinks. Mangels ausdrücklicher Regelung sind die §§ 7-10 Telemediengesetz, welche die E-Commerce-Richtlinie umsetzen, nicht auf Suchmaschinen und Hyperlinks anwendbar.

Bei Hyperlinks handelt es sich lediglich um technische Verweise innerhalb eines HTML-Textes und daher um technische Übertragungen, die eine Schnittstelle zwischen einem technischen Vorgang und einer inhaltlichen Leistung darstellen.[147] Mithin können Hyperlinks keinem der im Telemediengesetz aufgezählten Provider-Typen zugeordnet werden.[148] Auch eine analoge Anwendung des Telemediengesetzes scheidet aus, da zwar eine Regelungslücke vorliegt, diese jedoch nicht planwidrig ist. Zudem sind Hyperlinks nicht ausreichend mit den Leistungen von Internet Service Providern vergleichbar.[149]

Ebenso stellt sich bei Suchmaschinen ein ähnliches Problem. Auch diese hat der Gesetzgeber bewusst nicht gesetzlich geregelt, sodass auch hier eine analoge Anwendung der §§ 7-10 Telemediengesetz

---

143 Bundesministerium für Wirtschaft und Energie, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) vom 15.06.2015, abrufbar unter http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan,did=695334.html (22.07.2015), S. 7, dort § 8 Abs. 4 S. 1, 2 Nr. 1 Telemedienreferentenentwurf (TMGRefEntw).

144 Bundesministerium für Wirtschaft und Energie, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) vom 15.06.2015, abrufbar unter http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan,did=695334.html (22.07.2015), S. 15.

145 Bundesministerium für Wirtschaft und Energie, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) vom 15.06.2015, abrufbar unter http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan,did=695334.html (22.07.2015), S. 7, dort § 8 Abs. 4 S. 1, 2 Nr. 2 Telemedienreferentenentwurf (TMGRefEntw).

146 Bundesministerium für Wirtschaft und Energie, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) vom 15.06.2015, abrufbar unter http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan,did=695334.html (22.07.2015), S. 15.

147 H. Hören & Yankova, The Liability of Internet Intermediaries – The German Perspective, International Review of Intellectual Property and Competition Law (IIC) 2012, S. 501 ff., S. 509.

148 I. Garrote Fernández-Díez, Comparative Analysis on National Approaches to the Liability of Internet Intermediaries for Infringement of Copyright and Related Rights, abrufbar unter http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries_garrote.pdf (22.07.2015), S. 39.

149 I. Stenzel, Ergänzung der Reform der Telemedien um eine Haftungsprivilegierung für Hyperlinks notwendig, MultiMedia und Recht (MMR) 2006, S. V.

ausscheidet.[150] Zu Beginn wurden Suchmaschinen teilweise als Content Provider angesehen.[151] Seit der Entscheidung *Google France* des Europäischen Gerichtshofs[152] wenden die deutschen Gerichte jedoch die in dieser Entscheidung entwickelten Haftungsgrundsätze an.[153]

Aufgrund dieser Lücken wird in der Literatur gefordert, die Haftung beim Setzen von Hyperlinks sowie von Suchmaschinenbetreibern im Telemediengesetz ausdrücklich zu regeln.[154]

2. Nationales Recht

2.1. Überblick

Bisher hat der deutsche Gesetzgeber die Haftung von Providern nur in dem Masse geregelt, wie dies von den europäischen Richtlinien gefordert wird.[155]

Diese in den §§ 7-10 Telemediengesetz umgesetzten Vorschriften dienen sodann als Filter, bevor die eigentlichen Anspruchsgrundlagen und –gegennormen zur Anwendung kommen.[156] Nach diesem Filter bemisst sich, ob eine Haftung auf Schadensersatz in Frage kommt. Ist dies der Fall, so müssen zusätzlich die Voraussetzungen einer eigenständigen Anspruchsgrundlage vorliegen. Die in Frage kommenden Anspruchsgrundlagen verlangen jeweils Vorsatz oder Fahrlässigkeit, sodass die Haftung verschuldensabhängig ist.

Jedoch hat der Gesetzgeber auch von der in der E-Commerce-Richtlinie enthaltenen Möglichkeit Gebrauch gemacht, den Filter der §§ 7-10 Telemediengesetz nur auf Schadensersatzansprüche anzuwenden und nicht auch auf andere Ansprüche. Mithin gilt diese beschränkte Haftung nicht im Rahmen von Unterlassungsklagen oder Auskunftsansprüchen, wobei letztere nur eine sehr untergeordnete Rolle spielen. Unterlassungsklagen unterscheiden sich von Klagen auf Schadensersatz auch dadurch, dass sie regelmässig verschuldensunabhängig sind. Auch für diese Ansprüche gilt, dass eine eigene Anspruchsgrundlage vorliegen muss.

Für alle drei Klagearten, also auf Schadensersatz, Unterlassen oder Auskunft, richtet sich die eigentliche Anspruchsgrundlage nach der konkreten Rechtsverletzung. Die im Rahmen der Tätigkeit von Providern wichtigsten Anspruchsgrundlagen entstammen dem Urheberrecht, dem Markenrecht, dem Wettbewerbsrecht, zusätzlich spielt auch der allgemeine Anspruch wegen unerlaubter Handlung eine

---

150 M. Rath, Das Recht der Internet-Suchmaschinen, Stuttgart 2005, S. 384.

151 C. Busch, Secondary Liability of Service Providers, in M. Schmidt-Kessel, German National Reports on the 10th International Congress of Comparative Law, Tübingen 2014, S. 765 ff., S. 772; H. Hören & S. Yankova, The Liability of Internet Intermediaries – The German Perspective, International Review of Intellectual Property and Competition Law (IIC) 2012, S. 501 ff., S. 515.

152 Europäischer Gerichtshof (EuGH), Urteil vom 23.03.2010 – C-236/08 bis C-238/08 (*Google France*).

153 Bundesgerichtshof (BGH), Urteil vom 29.04.2010 – I ZR 69/08 (*Vorschaubilder I*); BGH, Urteil vom 19.10.2011 – I ZR 140/10 (*Vorschaubilder II*); H. Hören & S. Yankova, The Liability of Internet Intermediaries – The German Perspective, International Review of Intellectual Property and Competition Law (IIC) 2012, S. 501, S. 509.

154 I. Stenzel, Ergänzung der Reform der Telemedien um eine Haftungsprivilegierung für Hyperlinks notwendig, MultiMedia und Recht (MMR) 2006, S. V ff.

155 Siehe hierzu Punkt 1.2. dieses Gutachtens zum deutschen Recht.

156 C. Busch, Secondary Liability of Service Providers, in: Schmidt-Kessel, German National Reports on the 10th International Congress of Comparative Law, Tübingen 2014, S. 765 ff., S. 766; H. Hören, in W. Kilian & B. Heussen, Computerrechts-Handbuch: Informationstechnologie in der Rechts- und Wirtschaftspraxis, 32. Ergänzungslieferung, München 2013, Teil 14, Vertragsrechtliche Fragen, Rn. 18.

Rolle. Jedoch haben diese Ansprüche gemein, dass es sowohl dem Täter einer solchen Rechtsverletzung als auch seinem Gehilfen auf die tatsächliche Rechtsverletzung ankommen muss. Ein solcher Vorsatz wird bei Providern nur in sehr seltenen Fällen vorliegen, sodass oft kein Anspruch gegen den Provider besteht. Um diese Lücke zu schliessen, hat die Rechtsprechung die sogenannte Störerhaftung auf Provider ausgeweitet. Diese gründet sich auf eine Analogie zu § 1004 Bürgerliches Gesetzbuch, welcher einen Anspruch auf Beseitigen und Unterlassen einer Störung des Eigentums regelt. Allerdings meint diese Norm materielles Eigentum, weshalb sie auf immaterielle Rechtsgüter lediglich analog anwendbar ist. Schadensersatz kann auf dieser Grundlage aufgrund des eindeutigen Wortlauts der Norm[157] nicht eingeklagt werden.

2.2. Sonderbestimmungen für ISP

Im deutschen Recht existieren derzeit keine Sonderbestimmungen für Internet Service Provider, die über die genannten europäischen Richtlinien und deren Umsetzung[158] hinausgehen.

2.3. Anwendung der allgemeinen Bestimmungen auf ISP

2.3.1. Unterlassungsansprüche

In § 7 Telemediengesetz[159] hat der deutsche Gesetzgeber von der im jeweils letzten Absatz der Artikel 12 bis 14 E-Commerce-Richtlinie enthaltenen Möglichkeit Gebrauch gemacht, Ansprüche auf Beseitigung und Unterlassen der Rechtsverletzung auch unabhängig der beschränkten Providerhaftung zu erlauben. Daraus ergibt sich, dass die in den §§ 8-10 Telemediengesetz umgesetzten Vorschriften der E-Commerce-Richtlinie über die Haftung von Providern bei Unterlassungsklagen im deutschen Recht keine nennenswerte Rolle spielen.

Zu beachten sind allerdings stets die beiden in § 7 Telemediengesetz enthaltenen Grundsätze: Während Absatz 2 Satz 1 festlegt, dass die Provider keine allgemeine **Überwachungspflicht** trifft,[160] stellt Absatz 1 der Norm klar, dass alle Provider für ihre eigenen Inhalte haften. Content Provider, d.h. solche Provider, die eigene Inhalte anbieten wie beispielsweise Kommentare oder Informationen, haften also stets in vollem Umfang für ihre Inhalte. Aus dem erstgenannten Grundsatz ergibt sich jedoch, dass eine Haftung erst dann entsteht, wenn der Provider auf rechtswidrige Inhalte selbst aufmerksam wird oder von jemandem aufmerksam gemacht wird. Er muss also Kenntnis vom jeweiligen Verstoss haben. Wird die Haftung eines Providers bejaht, so richtet sie sich grundsätzlich darauf, den Zugang zu den rechtswidrigen Inhalten zu sperren und angemessene und zumutbare präventive Massnahmen zu ergreifen, um zukünftige Verstösse dieser Art zu verhindern.

Massgebend sind allein die Voraussetzungen der einzelnen Anspruchsgrundlagen. Hierfür kommen die gesetzlichen Spezialnormen verschiedener Rechtsbereiche in Betracht sowie die allgemeine Haftung bei unerlaubter Handlung. In der Praxis häufiger sind jedoch die Fälle der von der Rechtsprechung entwickelten Störerhaftung.

---

157 § 1004 Bürgerliches Gesetzbuch (BGB):
„(1) Wird das Eigentum in anderer Weise als durch Entziehung oder Vorenthaltung des Besitzes beeinträchtigt, so kann der Eigentümer von dem Störer die Beseitigung der Beeinträchtigung verlangen. Sind weitere Beeinträchtigungen zu besorgen, so kann der Eigentümer auf Unterlassung klagen.
(2) Der Anspruch ist ausgeschlossen, wenn der Eigentümer zur Duldung verpflichtet ist.“

158 Siehe hierzu Punkt 1.2. dieses Gutachtens zum deutschen Recht.

159 § 7 Abs. 2 S. 2 Telemediengesetz (TMG).

160 Der Bundesgerichtshof (BGH) hat hierzu auch ausgeführt, dass Betreiber von Internetauktionsseiten keine Pflicht trifft, manuell jedes Foto darauf zu überprüfen, ob es vom Original abweicht, BGH, Urteil vom 22.07.2010 – I ZR 139/08 (*Kinderhochstühle im Internet*).

2.3.1.1. Gesetzliche Anspruchsgrundlagen

Die relevantesten spezialgesetzlichen Anspruchsgrundlagen auf Unterlassen und Beseitigen einer Störung gegen Provider sind § 97 Absatz 1 Urhebergesetz, §§ 14 Absatz 5, 15 Absatz 4 Markengesetz sowie § 8 Unlauterer Wettbewerb-Gesetz. Zudem kann die Generalklausel des § 823 Absatz 1 Bürgerliches Gesetzbuch insbesondere in Verbindung mit dem allgemeinen Persönlichkeitsrecht[161] eine Rolle spielen. In der Rechtsprechung scheinen jedoch Verstösse gegen das Urhebergesetz die grösste Relevanz zu haben.

Access Provider haften grundsätzlich nur in sehr seltenen Fällen und dies derzeit nur im Rahmen der Störerhaftung.[162] Für Klagen wegen Verstössen gegen das Urhebergesetz hat die Rechtsprechung vielfach festgestellt, Access Provider seien nicht verpflichtet, Inhalte zu blockieren. Da sie selbst keinen direkten Einfluss auf die rechtswidrigen Inhalte hätten, könnten sie nicht als Täter oder Teilnehmer eines solchen Rechtsverstosses angesehen werden. Auch präventive Kontrollmassnahmen seien schon rein tatsächlich unzumutbar.[163]

Im Gegensatz hierzu haften **Content Provider** grundsätzlich **in vollem Umfang**, da es sich um ihre eigenen Informationen handelt.[164]

Für **Host Provider** lässt sich als Grundsatz zusammenfassen, dass sie haften, sofern sie sich die von Nutzern eingestellten Inhalte zu eigen machen. Durch diesen Vorgang werden sie Content Providern vergleichbar. Schwierigkeiten bereitet jedoch die Abgrenzung, wann sich ein Host Provider einen zuvor fremden Inhalt zu eigen macht.[165] Der Bundesgerichtshof hat hierfür verschiedene Kriterien entwickelt, die jedoch keine absolute Wirkung haben, sondern vom Einzelfall abhängen. Demnach kann ein **Anerkennen der Inhalte** als eigene Inhalte insbesondere dann vorliegen, wenn der Host Provider den Inhalt eines Beitrags vor dem Hochladen des Inhalts auf seine Richtigkeit hin überprüft.[166] Nicht ausreichend sei dabei allerdings allein der Fakt, dass Nutzer deutlich erkennen könnten, dass der Inhalt von einem Dritten beigetragen wurde. Zudem seien auch starke Indizien für ein Anerkennen des Inhalts, wenn der Host Provider den Inhalt in sein eigenes Layout integriert sowie wenn er einen wirtschaftlichen Vorteil aus dem Inhalt bezieht.[167] Die Rechtsprechung hat diese Kriterien zum Teil weiter ausgeführt, so komme es beispielsweise auf die „Gesamtschau […] aus der Perspektive eines objektiven Beobachters“ an.[168]

Im **Wettbewerbsrecht** ergibt sich noch eine Besonderheit. Hier soll nach der Rechtsprechung der Provider selbst als Täter und nicht bloss als Teilnehmer einer wettbewerbswidrigen Handlung haften.

---

161 Das allgemeine Persönlichkeitsrecht ist gesetzlich nicht ausdrücklich geregelt, wird jedoch aus Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz (GG) hergeleitet.

162 Siehe zu diesen Fällen Punkt 2.3.1.2. dieses Gutachtens zum deutschen Recht.

163 Oberlandesgericht (OLG) Frankfurt a.M., Beschluss vom 22.01.2008 – 6 W 10/08; Landgericht (LG) Düsseldorf, Urteil vom 13.12.2007 – 12 O 550/07; LG Hamburg, Urteil vom 12.03.2010 – 308 O 640/08; LG Kiel, Urteil vom 23.11.2007 – 14 O 125/07.

164 § 7 Abs. 1 Telemediengesetz (TMG).

165 J. B. Nordemann, Haftung von Providern im Urheberrecht: Der aktuelle Stand nach dem EuGH-Urteil v. 12. 7. 2011 – EUGH 12.07.2011 Aktenzeichen C-324/09 – L'Oréal/eBay, Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 2011, S. 977 ff., S. 977 f.; H. Hören & S. Yankova, The Liability of Internet Intermediaries – The German Perspective, International Review of Intellectual Property and Competition Law (IIC) 2012, S. 501 ff., S. 510.

166 Das Fehlen einer solchen Vorabprüfung hat das Oberlandesgericht (OLG) Hamburg in einer Entscheidung als Grund angenommen, eine Haftung des Providers abzulehnen, OLG Hamburg, Urteil vom Urteil vom 29.09.2010 – 5 U 9/09 (*Sevenload*).

167 Bundesgerichtshof (BGH), Urteil vom 12.11.2009 – I ZR 166/07 (*marions-kochbuch.de*)

168 Kammergericht (KG) Berlin, Beschluss vom 10.07.2009 – 9 W 119/08.

Dies ergebe sich daraus, dass ein Verstoss gegen die Vorschriften des Gesetzes über den unlauteren Wettbewerb vorliege, wenn jemand gegen eine wettbewerbsrechtliche Sorgfaltspflicht verstosse. Letztere ergeben sich aus § 3 Unlauterer Wettbewerb-Gesetz. Demnach muss jede Partei, die eine wirtschaftliche Gefahrenquelle kreiert, nach dem Wettbewerbsrecht alle möglichen und zumutbaren Vorsichtsmassnahmen ergreifen, um die wirtschaftlichen Interessen der Konkurrenten so gut es geht zu schützen.[169] Daraus ergebe sich für Host-Provider, dass diese **unmittelbar hafteten**, wenn sie, trotz Kenntnis von einem Verstoss gegen das Wettbewerbsrecht auf von ihnen zur Verfügung gestellten Websites, den Zugang zu diesen Seiten nicht sperrten.[170]

2.3.1.2. Störerhaftung

Die von der Rechtsprechung entwickelte Störerhaftung beruht nicht auf der Haftung wegen unerlaubter Handlung, sondern auf der **Eigentumsstörung**. § 1004 Bürgerliches Gesetzbuch wird hierfür analog angewendet. Damit schliesst die Rechtsprechung eine Regelungslücke, da Provider selbst nur selten Täter von oder Teilnehmer bei Urheberrechts- und Markenrechtsverletzungen sind.

Demnach haftet derjenige verschuldensunabhängig auf Unterlassen und Beseitigen einer Störung, der das Eigentum eines anderen **adäquat kausal stört**.[171] In analoger Anwendung gilt dies auch für Störungen des geistigen Eigentums. Ein Anspruch auf Schadensersatz lässt sich aufgrund des eindeutigen Wortlauts des § 1004 Bürgerliches Gesetzbuch[172] aus der Störerhaftung jedoch nicht ableiten.

Um diese weitgehende Haftung etwas einzugrenzen, versucht die Rechtsprechung, verschiedene Kriterien zu entwickeln. Diese sind jedoch stark einzelfallabhängig.[173] Grundsätzlich lassen sie sich wie folgt zusammenfassen: Dem Provider muss eine im jeweiligen Einzelfall festzustellende **Sorgfaltspflicht obliegen, Inhalte zu überprüfen**.[174] Diese Sorgfaltspflicht muss für den Provider auch **zumutbar** sein.[175] Hierfür kann allgemein gesagt werden, dass die Anforderungen an den Provider, den mutmasslich rechtswidrigen Inhalt zu überprüfen, steigen, je mehr konkrete Hinweise es auf eine Rechtsgutsverletzung gibt.[176] Wie bereits dargestellt trifft den Provider grundsätzlich keine allgemeine

---

169 Bundesgerichtshof (BGH), Urteil vom 12.07.2007 – I ZR 18/04 (*jugendgefährdende Medien bei eBay*).

170 H. Hören & S. Yankova, The Liability of Internet Intermediaries – The German Perspective, International Review of Intellectual Property and Competition Law (IIC) 2012, S. 501 ff., S. 523 f.

171 § 1004 Abs. 1 S. 1 Bürgerliches Gesetzbuch (BGB).

172 „Beseitigungs- und Unterlassungsanspruch:
(1) Wird das Eigentum in anderer Weise als durch Entziehung oder Vorenthaltung des Besitzes beeinträchtigt, so kann der Eigentümer von dem Störer die Beseitigung der Beeinträchtigung verlangen. Sind weitere Beeinträchtigungen zu besorgen, so kann der Eigentümer auf Unterlassung klagen.
(2) Der Anspruch ist ausgeschlossen, wenn der Eigentümer zur Duldung verpflichtet ist."

173 A. Ohly, Die Verantwortlichkeit von Intermediären, Zeitschrift für Urheber- und Medienrecht (ZUM) 2015, S. 308 ff., S. 312.

174 Bundesgerichtshof (BGH), Urteil vom 17.05.2001 – I ZR 251/99; BGH, Urteil vom 22.07.2010 – I ZR 139/08; BGH, Urteil vom 25.10.2011 – VI ZR 93/10.

175 Siehe hierzu auch J. Ensthaler/M. Heinemann, Die Fortentwicklung der Providerhaftung durch die Rechtsprechung, Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 2012, S. 433 ff., S. 436 ff.

176 H. Hören/S. Yankova, The Liability of Internet Intermediaries – The German Perspective, International Review of Intellectual Property and Competition Law (IIC) 2012, S. 501 ff., S. 504 f.; siehe auch Bundesgerichtshof (BGH), Urteil vom 12.07.2012 – I ZR 18/11 (*Alone in the Dark*) und BGH, Urteil vom 15.08.2013 – I ZR 80/12 (*RapidShare*) sowie Freedom House, Freedom on the Net 2014: Germany, verfügbar unter https://freedomhouse.org/sites/default/files/resources/Germany.pdf (22.07.2015), S. 10. Basierend auf Rechtsprechung bis 2008 hat T. Wilmer ausserdem eine Matrix mit verschiedenen Stufen der Sorgfaltspflicht entwickelt: T. Wilmer, Überspannte Prüfpflichten für Host-Provider? Vorschlag für eine Haftungsmatrix, in Neue Juristische Wochenschrift (NJW) 2008, S. 1845 ff., S. 1850.

Überprüfungspflicht,[177] allerdings kann bei leicht erkennbaren Verstössen die Pflicht bestehen, diese in Zukunft zu verhindern.[178] Aufgrund dieser Kriterien hat sich eine Einzelfallkasuistik ergeben, die im Rahmen dieses Gutachtens nicht umfassend wiedergegeben werden kann.

Zur Haftung bei **Hyperlinks** sowie von Suchmaschinen lässt sich jedoch folgendes sagen: Im Hinblick auf Hyperlinks hat der Bundesgerichtshof entschieden, dass Links zu urheberrechtlich geschützten Werken keine Verletzung des Urheberrechts darstellen. Stattdessen habe sich der Rechtsinhaber konkludent mit einer Verwendung bereit erklärt, indem er keine technischen Schutzvorkehrungen gegen die Verwendung seiner Werke getroffen habe.[179] Hingegen hat das Oberlandesgericht München eine Urheberrechtsverletzung angenommen, als in einem Artikel über eine neue Software zum Kopieren von DVDs auch ein direkter Link zum Produzenten dieser Software enthalten war. Im Zusammenhang mit dem Artikel habe der Link die Suche nach dem rechtswidrigen Inhalt deutlich erleichtert, sodass eine Haftung als Störer angenommen werden müsse.[180] Der Bundesgerichtshof hat dem jedoch widersprochen mit dem Argument, dieses Vorgehen sei von dem Grundrecht auf Pressefreiheit geschützt.[181]

Bei der Haftung von **Suchmaschinen** scheint sich ein Wandel der Rechtsprechung abzuzeichnen. Seit der *Google France*-Entscheidung des Europäischen Gerichtshofs werden Suchmaschinen, die neutral sind und keine Kenntnis oder Kontrolle über die gespeicherten Daten haben, in Zukunft als Host Provider angesehen werden und damit nur in beschränktem Masse haften.[182] Eine Besonderheit ergibt sich jedoch bei der sogenannten *Autocomplete*-Funktion. Schlägt die Suchmaschine bei Eingabe eines Suchbegriffs nach einem bestimmten Algorithmus in diesem Zusammenhang weitere Suchbegriffe vor, so entsteht für den Betreiber der Suchmaschine eine Prüfpflicht dieser Suchvorschläge. Dies begründet der Bundesgerichtshof damit, der Algorithmus sei ein eigener oder zumindest zu eigen gemachter Inhalt des Suchmaschinenbetreibers. Allerdings treffe ihn diese Pflicht erst, wenn er Kenntnis von rechtsverletzenden Suchvorschlägen habe.[183] Diese Regelung ist besonders dann relevant, wenn das allgemeine Persönlichkeitsrecht betroffen ist.[184]

Eine Haftung von **Access Providern** scheint derzeit in Deutschland nur insofern möglich zu sein, wenn beispielsweise natürliche Personen, Betreibende von Internet-Cafés, Hotels oder Ferienwohnungen die Nutzung ihres WLANs zur Verfügung stellen, dulden oder nicht ausreichend gegen die Benutzung durch Dritte sichern.[185] Indem sie andere ihr WLAN benutzen lassen, werden sie zu Access Providern, die sodann für Rechtsverletzungen durch Dritte mittels des von ihnen betriebenen WLANS als Störer haften. Die Störerhaftung ist jedoch ausschliesslich auf Unterlassen und Beseitigen der Störung

---

177 § 7 Abs. 2 S. 1 Telemediengesetz (TMG); Oberlandesgericht (OLG) Hamburg, Urteil vom 01.07.2015 – 5 U 87/12 und 5 U 175/10.

178 Bundesgerichtshof (BGH), Urteil vom 15.10.1998 – I ZR 120/96.

179 Bundesgerichtshof (BGH), Urteil vom 17.07.2003 – I ZR 259/00 (*Paperboy*).

180 Oberlandesgericht (OLG) München, Urteil vom 28.07.2005 – 29 U 2887/05 (*AnyDVD*).

181 Bundesgerichtshof (BGH), Urteil vom 20.10.2010 – I ZR 191/08 (*AnyDVD*).

182 Bundesgerichtshof (BGH), Urteil vom 29.04.2010 – I ZR 69/08 (*Vorschaubilder I*); BGH, Urteil vom 19.10.2011 – I ZR 140/10 (*Vorschaubilder II*); H. Hören & S. Yankova, The Liability of Internet Intermediaries – The German Perspective, International Review of Intellectual Property and Competition Law (IIC) 2012, S. 501 ff., S. 515.

183 Bundesgerichtshof (BGH), Urteil vom 14.05.2013 – VI ZR 269/12 (*Autocomplete*).

184 H. Hören, in W. Kilian & B. Heussen, Computerrechts-Handbuch: Informationstechnologie in der Rechts- und Wirtschaftspraxis, 32. Ergänzungslieferung, München 2013, Teil 14, Vertragsrechtliche Fragen, Rn. 30.

185 Bundesgerichtshof (BGH), Urteil vom 12.05.2010 – I ZR 121/08 (*Sommer unseres Lebens*); Landgericht (LG) Frankfurt a.M., Urteil vom 18.08.2010 – 2-06 S 19/09; LG Hamburg, Urteil vom 25.11.2010 – 310 O 433/10; LG Frankfurt a.M., Urteil vom 28.06.2013 – 2-06 O 304/12.

gerichtet und nicht auf Schadensersatz. Mit der Störerhaftung haben die Gerichte von der im jeweils letzten Absatz der §§ 12-14 E-Commerce-Richtlinie enthaltenen Möglichkeit Gebrauch gemacht, ein Rechtsinstitut zu entwickeln, welches neben und unabhängig von der E-Commerce-Richtlinie anwendbar ist. Da die Vorschriften der E-Commerce-Richtlinie sowie deren Umsetzung im Telemediengesetz für die Störerhaftung irrelevant sind, gehen die Gerichte in ihren Entscheidungen auf diese auch nicht ein. Sie klassifizieren die Betreibenden des jeweiligen WLAN-Anschlusses daher nicht ausdrücklich als Access Provider oder als anderen Provider. Lediglich aus der Literatur geht hervor, dass Betreibende eines WLAN-Anschlusses dem Wesen nach Access Provider seien.[186] Im Unterschied zu Access Providern im engeren Sinne, welche den Zugang zum Internet für eine unüberschaubare Vielzahl von Menschen ermöglichen, seien den genannten Access Providern Schutzmassnahmen zumutbar. So sei es den Betreibenden eines Internet-Cafés möglich und zumutbar, die für File Sharing erforderlichen Ports zu sperren.[187] Umgekehrt konnte sich ein Hotelbetreibender gegen eine Haftung für Rechtsverletzungen ihrer Gäste dadurch schützen, indem er diese zuvor darauf hingewiesen hatte, die gesetzlichen Vorschriften bei der Nutzung des WLANs einzuhalten.[188] Mitte 2014 sowie Ende 2013 haben sich zwei Oberlandesgerichte ausführlich mit der Haftung von Access Providern auseinander gesetzt und diese verneint. Hierbei verwiesen die Gerichte insbesondere darauf, Schutzmassnahmen seien technisch gesehen nicht wirksam genug und blockierten zudem gleichzeitig den Zugang zu rechtmässigen Inhalten,[189] welches einen Eingriff in die Meinungsfreiheit[190] darstelle. Zudem fehle eine ausdrückliche gesetzliche Grundlage, um in das als Grundrecht geschützte Fernmeldegeheimnis[191] eingreifen zu dürfen.[192] Gegen beide Urteile wurde jedoch Revision eingelegt und zugelassen, sodass sich nun der Bundesgerichtshof mit der Frage der Haftung von Access Providern auseinander setzen wird. Zudem hat ein Landgericht Ende 2014 ein Verfahren, in welchem die Frage aufgeworfen wird, ob es sich bei einem WLAN-Betreiber um einen Access Provider handelt, dem Europäischen Gerichtshof vorgelegt, damit dieser zur Auslegung insbesondere des Artikels 12 E-Commerce-Richtlinie Stellung nehme.[193]

Im **Wettbewerbsrecht** ist die Anwendung der Störerhaftung sehr **umstritten**, da das Wettbewerbsrecht selbst Teil des Rechts der unerlaubten Handlung ist. Für das Wettbewerbsrecht gelten daher besondere Verhaltensregeln im Rahmen des geschäftlichen Handelns. Dementsprechend scheint die Rechtsprechung nun auch dazu überzugehen, die Störerhaftung nicht mehr in wettbewerbsrechtlichen Fällen anzuwenden. Stattdessen behandelt sie Provider nunmehr vermehrt als unmittelbare Täter.[194] Eine ausdrückliche Entscheidung, wonach die Störerhaftung im Wettbewerbsrecht nicht mehr anwendbar sein soll, steht jedoch noch aus.

---

186 K. Nenninger, Anmerkung zu Bundesgerichtshof (BGH), Urteil vom 12.5.2010 – I ZR 121/08 (*Sommer unseres Lebens*), Neue Juristische Wochenschrift (NJW) 2010, S. 2064 ff., S. 2064; S. Leible & D. Jahn, Anmerkung zu Bundesgerichtshof (BGH), Urteil vom 12.5.2010 – I ZR 121/08 (*Sommer unseres Lebens*), Kommentierte BGH-Rechtsprechung Lindenmaier-Möhring (LMK) 2010, 306719; R. Mantz, Die Haftung des Betreibers eines gewerblich betriebenen WLANs und die Haftungsprivilegierung des § 8 TMG: Zugleich Besprechung von LG Frankfurt a. M., Urt. v. 28. 6. 2013 – 2-06 O 304/12 – Ferienwohnung, Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report (GRUR-RR) 2013, S. 497 ff., S. 499; C. Busch, Secondary Liability of Service Providers, in: M. Schmidt-Kessel, German National Reports on the 10th International Congress of Comparative Law, Tübingen 2014, S. 765 ff., S. 774.

187 Landgericht (LG) Hamburg, Urteil vom 25.11.2010 – 310 O 433/10.

188 Landgericht (LG) Frankfurt a.M., Urteil vom 18.08.2010 – 2-06 S 19/09.

189 Sogenanntes Overblocking.

190 Art. 5 Grundgesetz (GG).

191 Art. 10 Grundgesetz (GG).

192 Oberlandesgericht (OLG) Hamburg, Urteil vom 21.11.2013 – 5 U 68/10; OLG Köln, Urteil vom 18.07.2014 – 6 U 192/11 (*Goldesel*).

193 Landgericht (LG) München I, Beschluss vom 18.09.2014 – 7 O 14719/12; siehe hierzu oben, 1.3.

194 Siehe hierzu unter Punkt 2.3.1.1. dieses Gutachtens zum deutschen Recht.

2.3.2. Reparatorische Ansprüche

Reparatorische Ansprüche auf Schadensersatz gegen Provider haben nur selten Erfolg. Grund hierfür ist die Filterfunktion der §§ 8-10 Telemediengesetz, welche die Artikel 12-14 E-Commerce-Richtlinie umsetzen. Ansprüche, die damit nicht herausgefiltert werden, müssen sodann auf einer Anspruchsgrundlage beruhen. Hierfür kommen gegen Provider insbesondere § 97 Absatz 2 Urhebergesetz, § 14 Absatz 6 Sätze 1-3 und § 15 Absatz 5 Sätze 1-2 Markengesetz sowie § 9 Satz 1 Unlauterer Wettbewerb-Gesetz in Betracht. Zudem greifen die allgemeinen Anspruchsgrundlagen des Rechts der unerlaubten Handlung wie insbesondere § 823 Absatz 1 Bürgerliches Gesetzbuch. Diese haben gemein, dass der Täter mit Vorsatz oder Fahrlässigkeit gehandelt haben muss, die Ansprüche sind also im Gegensatz zu Unterlassungsklagen verschuldensabhängig.

2.3.3. Informationsansprüche

In der veröffentlichten Rechtsprechung spielen Ansprüche auf Auskunft gegen Provider nur eine untergeordnete Rolle, lediglich vereinzelt setzen sich die Gerichte mit solchen Ansprüchen auseinander.[195] Anspruchsgrundlagen können hier insbesondere § 101 Absätze 1 und 2 Urhebergesetz und § 19 Absätze 1 und 2 Markengesetz sein. Für Access Provider ist hier von Interesse, dass gegen sie zwar in der Regel Unterlassungsklagen nicht in Betracht kommen, sie aber durchaus auf Auskunft in Anspruch genommen werden können.[196]

2.4. Bezug zwischen den verschiedenen Bestimmungen

Mangels spezialgesetzlicher Regelungen zur Haftung von Providern stellt sich die Frage nicht, wie die speziellen und die allgemeingesetzlichen Vorschriften zueinander stehen. Zur Beziehung der einzelnen allgemeinen Vorschriften und Haftungsgrundlagen siehe oben, 2.1.

3. Rechtsdurchsetzung

3.1. Überblick

Besondere Regelungen zur Durchsetzung von Ansprüchen gegen Provider gibt es im deutschen Recht derzeit nicht. Lediglich die bereits erwähnten Auskunftsansprüche können in diesem Zusammenhang von Interesse sein. Auch die Kosten des Verfahrens unterliegen den allgemeinen Vorschriften des Zivilprozesses.

3.2. Nationale Sachverhalte

Wie bereits dargestellt[197] hat der deutsche Gesetzgeber Artikel 8 der Durchsetzungsrichtlinie in § 19 Markengesetz sowie in § 101 Urhebergesetz umgesetzt. Diese enthalten detaillierte Regelungen zu Ansprüchen auf Auskunft zum Zwecke der Durchsetzung von anderen Ansprüchen. Sofern die Auskunft darauf gerichtet ist, eine IP-Adresse einer Person zuzuordnen, so ist hierfür eine vorherige richterliche Anordnung über die Zulässigkeit der Verwendung der IP-Adresse erforderlich.[198] Zuständig für diese

---

195 Bundesgerichtshof (BGH), Beschluss vom 19.04.2012 – I ZB 80/11 (*Alles kann besser werden*); BGH, Beschluss vom 16.05.2013 – I ZB 50/12; BGH, Beschluss vom 16.05.2013 – I ZB 25/12; Oberlandesgericht (OLG) München, Beschluss vom 26.07.2011 – 29 W 1268/11; OLG München, Beschluss vom 12.12.2011 – 29 W 1708/11; OLG Köln, Beschluss vom 13.10.2011 – 6 W 223/11.

196 Oberlandesgericht (OLG) Hamburg, Urteil vom 17.02.2010 – 5 U 60/09.

197 Siehe hierzu unter Punkt 1.2. dieses Gutachtens zum deutschen Recht.

198 § 101 Abs. 9 S. 1 Urhebergesetz (UrhG); § 19 Abs. 9 S. 1 Markengesetz (MarkenG); Bundesgerichtshof (BGH), Beschluss vom 19.04.2012 – I ZB 80/11 (*Alles kann besser werden*); BGH, Beschluss vom

richterliche Anordnung ist die Zivilkammer desjenigen Landgerichts, in dessen Bezirk die zur Auskunft verpflichtete Person ihren Wohnsitz, ihren Sitz oder eine Niederlassung hat,[199] wobei die Kosten der Anordnung die verletzte Person trägt.[200] Darüber hinaus scheint es keine besondere Regelung der Kosten des Verfahrens für Ansprüche gegen Provider zu geben. Unsere Recherche hat hierzu auch keine Kommentare der Literatur gefunden. Grund hierfür ist vermutlich das gänzliche Fehlen von Spezialregelungen für die Providerhaftung.

In der Praxis werden oftmals sogenannte Mahnungen an Verletzende von Rechten des geistigen Eigentums verschickt. Bei dem Mahnverfahren im deutschen Recht handelt es sich um ein besonderes Gerichtsverfahren, welches der schnelleren Durchsetzung von Geldforderungen dient.[201] Daraus ergibt sich jedoch auch, dass sie nicht dafür verwendet werden können, Unterlassungs- und Beseitigungsansprüche durchzusetzen. Daher haben sie zwar eine grosse praktische Bedeutung gegenüber den Nutzern rechtswidriger Inhalte im Internet, jedoch nur eine geringe Bedeutung zur Durchsetzung von Ansprüchen gegen Provider.

3.3. Internationale Sachverhalte

Grundsätzlich finden auf internationale Sachverhalte die Vorschriften der Rom II Verordnung Anwendung.[202] In manchen Fällen ist jedoch ein Rückgriff auf die nationalen Vorschriften zum internationalen Privatrecht erforderlich. So ist beispielsweise für Verletzungen des allgemeinen Persönlichkeitsrechts Artikel 40 Einführungsgesetz zum Bürgerlichen Gesetzbuche einschlägig. Demnach bemessen sich Schadensersatzansprüche wegen unerlaubter Handlung nach dem Recht des Staates, in welchem die Handlung stattgefunden hat.[203] Die geschädigte Person kann jedoch verlangen, dass stattdessen das Recht des Staates angewendet wird, in welchem die Verletzung eingetreten ist.[204] Der Bundesgerichtshof hat hierzu im *Autocomplete*-Fall entschieden, dass die Verletzung des allgemeinen Persönlichkeitsrechts in dem Staat eintritt, in welchem die Achtung der Person gefährdet ist.[205]

Zur Durchsetzung von Ansprüchen bei internationalen Sachverhalten hat unsere Recherche keine Besonderheiten ergeben.

3.4. Vorschläge

Unsere Recherche hat keine Reformprojekte ergeben.

16.05.2013 – I ZB 50/12; BGH, Beschluss vom 16.05.2013 – I ZB 25/12; C. Busch, Secondary Liability of Service Providers, in M. Schmidt-Kessel, German National Reports on the 10th International Congress of Comparative Law, Tübingen 2014, S. 765 ff., S. 776.

199 § 101 Abs. 9 S. 2, 3 Urhebergesetz (UrhG); § 19 Abs. 9 S. 2, 3 Markengesetz (MarkenG).

200 § 101 Abs. 9 S. 5 Urhebergesetz (UrhG); § 19 Abs. 9 S. 5 Markengesetz (MarkenG).

201 §§ 688 ff. Zivilprozessordnung (ZPO).

202 Siehe hierzu C. Busch, Secondary Liability of Service Providers, in M. Schmidt-Kessel, German National Reports on the 10th International Congress of Comparative Law, Tübingen 2014, S. 765 ff., S. 778.

203 Art. 40 Abs. 1 S. 1 Einführungsgesetz zum Bürgerlichen Gesetzbuche (EGBGB).

204 Art. 40 Abs. 1 S. 2 Einführungsgesetz zum Bürgerlichen Gesetzbuche (EGBGB).

205 Bundesgerichtshof (BGH), Urteil vom 14.05.2013 – VI ZR 269/12 (*Autocomplete*).

C. FRANKREICH

1. Transposition du droit européen

1.1. Vue d'ensemble

En France, la question de la responsabilité des fournisseurs de services internet est essentiellement régie par la loi du 21 juin 2004 n°2004-575 pour la confiance dans l'économie numérique (ci-après « LCEN »). Celle-ci prévoit des règles différentes pour la responsabilité selon les activités des fournisseurs de services liés à internet.

1.2. Transposition des directives

Conformément à la directive 2000/31/CE sur le commerce électronique, la LCEN régit différemment la responsabilité des fournisseurs de services liés à internet selon les activités qu'ils exercent.

En ce qui concerne les **fournisseurs d'accès à internet**, cette loi a introduit dans le code des postes et communications électroniques, conformément à l'art. 12 de la directive 2000/31/CE sur le commerce électronique, le principe de leur **irresponsabilité**. La responsabilité des fournisseurs d'accès pourra toutefois être mise en cause dans les hypothèses d'**exceptions** prévues par cette même disposition, conformément à la directive précitée. En effet, l'art. L32-3-3 du Code des postes et communications électroniques prévoit :

> « Toute personne assurant une activité de transmission de contenus sur un réseau de communications électroniques ou de fourniture d'accès à un réseau de communications électroniques ne peut voir sa responsabilité civile ou pénale engagée à raison de ces contenus que dans les cas où soit elle est à l'origine de la demande de transmission litigieuse, soit elle sélectionne le destinataire de la transmission, soit elle sélectionne ou modifie les contenus faisant l'objet de la transmission »[206].

Quant aux personnes qui exercent des **activités de stockage automatique** de contenus transmis par les utilisateurs (activités de copie cache), le code des postes et communications électroniques prévoit, conformément aux dispositions de la directive sur le commerce électronique, que leur responsabilité civile ou pénale ne peut être mise en cause que dans un nombre restreint d'hypothèses. En effet, l'art. L.32-3-4 du code des postes et communications électroniques prévoit:

> « Toute personne assurant dans le seul but de rendre plus efficace leur transmission ultérieure, une activité de stockage automatique, intermédiaire et temporaire des contenus qu'un prestataire transmet ne peut voir sa responsabilité civile ou pénale engagée à raison de ces contenus que dans l'un des cas suivants :
>
> 1° Elle a modifié ces contenus, ne s'est pas conformée à leurs conditions d'accès et aux règles usuelles concernant leur mise à jour ou a entravé l'utilisation licite et usuelle de la technologie utilisée pour obtenir des données ;
>
> 2° Elle n'a pas agi avec promptitude pour retirer les contenus qu'elle a stockés ou pour en rendre l'accès impossible, dès qu'elle a effectivement eu connaissance, soit du fait que les contenus transmis initialement ont été retirés du réseau, soit du fait que l'accès aux contenus transmis initialement a été rendu impossible, soit du fait que les autorités judiciaires ont ordonné de retirer du réseau les contenus transmis initialement ou d'en rendre l'accès impossible. »[207]

---

206 Art. L32-3-3 Code des postes et communications électroniques.

207 Art. L32-3-4 Code des postes et communications électroniques.

Les **fournisseurs d'hébergement internet** sont, quant à eux, soumis à un régime autonome de responsabilité. La LCEN définit, en son article 6.I.2, les hébergeurs comme les « personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services »[208].

La LCEN dispose que la **responsabilité *civile* des hébergeurs** en raison de contenu illicite hébergé sur internet par leurs soins ne peut être engagée « du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible »[209]. Il y a donc deux conditions à la mise en cause de la responsabilité civile de l'hébergeur : (i) la **connaissance effective** du caractère illicite du contenu, et, à partir de ce moment-là, (ii) le **défaut d'agir** promptement pour retirer les données en cause ou en rendre l'accès impossible.

Pour faciliter la preuve de la connaissance effective du caractère illicite du contenu, la loi pose une **présomption simple de connaissance des faits litigieux** par l'hébergeur lorsqu'il reçoit notification de différents éléments énumérés par la LCEN, tels que la date des faits, leur description, leur localisation, les motifs pour lesquels le contenu doit être retiré avec mention des dispositions légales et les justifications de fait, copie de la correspondance adressées à l'auteur ou l'éditeur des informations par laquelle il est demandé leur interruption, leur retrait ou modification ou justification de ce que l'auteur ou l'éditeur n'a pu être contacté. Cette procédure de notification facultative permet de démontrer la connaissance par l'hébergeur du contenu illicite qu'il héberge, et ainsi, le contraindre à agir promptement. Ceci dit, d'après le texte de la loi, si la notification permet de présumer la connaissance effective du caractère illicite du contenu, cette connaissance peut également être prouvée par tous autres moyens.

Il ne suffit pas de notifier l'existence d'un contenu illicite pour que l'hébergeur soit reconnu responsable faute d'avoir retiré promptement ledit contenu d'internet. En effet, la notification n'a pas de pouvoir coercitif quant au retrait demandé, l'hébergeur disposant d'un pouvoir d'appréciation quant au caractère illicite ou non du contenu visé.

Nous revenons sur les conditions de la mise en cause de la responsabilité civile des hébergeurs dans les sections suivantes du présent rapport.

Quant à la **responsabilité *pénale*** des hébergeurs, celle-ci ne sera pas engagée « si [les hébergeurs] n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où [ils] en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible »[210].

Enfin, l'activité d'**éditeur** dans le domaine d'internet n'est pas définie dans la LCEN, ce qui a donné, dans la jurisprudence récente, une confusion entre les notions de éditeur de site internet, éditeur de contenus et éditeur de service de communication en ligne. De manière générale, on relève que le statut d'éditeur est en principe octroyé aux intermédiaires qui exercent une activité éditoriale vis-à-vis des contenus litigieux[211].

---

208 Art. 6.I.2 LCEN

209 Ibidem.

210 Art. 6.I.3 LCEN.

211 Elise Ricbourg-Attal , La responsabilité civile des acteurs de l'internet, Du fait de la mise en ligne de contenus illicites, Larcier, 2014, p. 252, n° 312.

En application de la LCEN, l'éditeur de service de communication au public en ligne a une **obligation de mettre à disposition du public les données permettant de l'identifier** ainsi que le nom du directeur et du co-directeur de la publication et, le cas échéant, du responsable de la rédaction, sous peine de sanctions pénales. Lorsque l'activité d'éditeur est exercée à titre non professionnel, le fournisseur de contenus peut se limiter à publier sur son site les nom, dénomination ou raison social du fournisseur d'hébergement, sous réserve d'avoir communiqué à ce dernier les éléments d'identification le concernant.

La LCEN ne prévoit toutefois **pas de régime de responsabilité spécifique pour les éditeurs de site internet**. La jurisprudence a comblé cette lacune : dès qu'une activité éditoriale intervient, l'éditeur est soumis à un régime de responsabilité de droit commun sauf dans l'hypothèse où il relève de la qualification d'éditeur de presse[212].

La directive 2004/48/CE relative au respect des droits de propriété intellectuelle, qui a introduit, en particulier, un **droit d'information** pour les utilisateurs sur l'origine et les réseaux de distribution des marchandises ou des services qui portent atteinte à un droit de propriété intellectuelle, a été transposée en droit français par la loi 2007-1544 du 29 octobre 2007 qui a inséré des dispositions correspondantes dans le code de la propriété intellectuelle. Nous revenons sur ce droit d'information ci-dessous, dans la section 2.2.3.

La directive 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, prévoyant, notamment la possibilité de condamner les intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit d'auteur ou à un droit voisin, a été transposée en droit français par la **loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information**[213]. Cette loi a introduit un grand nombre de dispositions nouvelles dans le code de la propriété intellectuelle, y compris permettant d'ordonner aux fournisseurs de services sur internet de prendre les mesures nécessaire pour faire cesser le dommage. Nous revenons sur ces mesures ci-dessous, dans la section 2.2.1.

Enfin, la directive 95/46/CE relative au traitement des données personnelles a été transposée en droit français par la **loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel** et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[214].

1.3. Jurisprudence

Compte tenu du nombre très important de décisions rendues en matière de responsabilité des intermédiaires de services internet, seuls quelques thèmes importants de la matière seront présentés ci-après. De plus, par souci de pertinence, il sera uniquement fait état des décisions intervenues après l'entrée en vigueur de la LCEN.

Une des premières questions se posant dans le cadre de la jurisprudence est celle du statut des intermédiaires de service liés à internet. Dans une affaire qui concernait l'existence de sites internet mettant à disposition des bandes dessinées complètes sous la forme de fichiers, la responsabilité du prestataire internet qui avait mis à disposition sa capacité de stockage, la société Tiscali Media, fut

---

212 Voir : *infra* section 1.3

213 Loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information, J.O. n° 178, du 3 août 2006, p. 11529.

214 Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O. n°182 du 7 août 2004, p. 14063.

recherchée. La position de la Cour d'Appel de Paris – confirmée par la Cour de Cassation dans son arrêt du 14 janvier 2010[215] – a été de considérer que le rôle de Tiscali Media correspondait à celui d'un **éditeur**, et non celui d'un simple fournisseur d'hébergement, dès lors que la société **proposait et gérait elle-même des espaces publicitaires payants** sur les pages personnelles des internautes. Il en résultait qu'en mettant à disposition du public les fichiers en cause, la société avait commis des actes de contrefaçon. D'autres décisions ont suivi une approche différente, préférant écarter la commercialisation du site comme critère de détermination du statut. Ainsi, dans une autre affaire, la Cour d'Appel de Paris a considéré que l'exploitation d'un site par la commercialisation d'espaces publicitaires, si elle n'induit pas une capacité d'action du service sur les contenus mis en ligne, n'est pas de nature à justifier de la qualification d'éditeur du service en cause[216].

La jurisprudence a également eu l'occasion de préciser et clarifier les conditions de la responsabilité civile de l'hébergeur. En ce qui concerne le caractère illicite du contenu hébergé, le Conseil Constitutionnel a déclaré, dans sa décision du 10 juin 2004, que les dispositions visées de la LCEN

> «…ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas *manifestement* un tel caractère ou si son retrait n'a pas été ordonné par un juge»[217].

Si le caractère **manifestement illicite** ne fait pas de doute pour ce qui concerne les hypothèses de contenu à caractère pédopornographique ou encore des propos qui font l'apologie des crimes de guerre ou qui incitent à des actes de terrorisme, il existe une vraie **difficulté d'appréciation** dans de nombreux autres cas tels que la diffamation, l'injure ou encore l'atteinte à la vie privée (voir infra, section 1.4.).

Dans un arrêt du 4 avril 2013, la Cour d'appel de Paris, se prononçant en référé, a considéré que :

> « qu'à l'exception de certaines diffusions expressément visées par la loi relatives à la pornographie enfantine, à l'apologie des crimes contre l'humanité et à l'incitation à la haine raciale que l'hébergeur doit, sans attendre une décision de justice, supprimer, sa responsabilité civile ne peut être engagée du fait des informations stockées s'il n'a pas effectivement eu connaissance de leur caractère illicite ou si, dès le moment où il en a eu connaissance, il a agi promptement pour retirer les données ou en rendre l'accès impossible »[218].

Toujours en ce qui concerne la mise en cause de la responsabilité de l'hébergeur pour le contenu d'un site qu'il héberge, on relève encore que, dans une affaire où un film avait été mis à la disposition du public sur internet, la responsabilité de l'hébergeur, la société Dailymotion, avait été recherchée. La Cour de Cassation dans son arrêt du 17 février 2011, a considéré que la Cour d'Appel avait valablement constaté que la notification relative au contenu illicite du site hébergé, faite à Dailymotion, ne contenait pas tous les éléments permettant de vérifier l'existence et la localisation des vidéos en question, et que, partant, il n'avait eu connaissance effective qu'au stade de l'assignation en justice.

---

215 Cass., 14 janvier 2010, n° 06-18855, www.legifrance.gouv.fr (27.01.2015).

216 Paris, 6 mai 2009, D. 2009, AJ 1410, obs. Astaix.

217 Conseil Constitutionnel, DC 2004-496, 10 juin 2004 (nous soulignons) : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2004/2004-496-dc/decision-n-2004-496-dc-du-10-juin-2004.901.html (27.01.2015).

218 CA, 4 avril 2013, disponible sur : www.legalis.net (27.01.2015). Compte tenu de son caractère préalable à la récente loi du 13 novembre 2014 renforçant les dispositions relative à la lutte contre le terrorisme, l'arrêt de la cour d'appel ne prend pas en compte, dans sa conception des activités manifestement illicites, les infractions visées par la récente loi à l'art. 421-2-5 code pénal : provocations à des actes terroristes et apologie des actes de terrorisme. Ces infractions doivent toutefois logiquement être considérées comme des activités manifestement illicites.

Pour cette raison, la Cour d'appel était fondée à considérer qu'aucun manquement à l'obligation de promptitude à retirer le contenu illicite ou à en interdire l'accès ne pouvait être reproché à la société Dailymotion[219].

Quant au **délai dans lequel les informations illicites doivent être retirées** d'internet par l'hébergeur du site, la jurisprudence s'est attelée à préciser le délai attendu entre la connaissance et la réaction technique. Toutefois, l'analyse de la jurisprudence révèle un manque d'uniformité sur cette question. Il s'agit, pour le juge, d'effectuer une **appréciation *in concreto*** pour chaque espèce[220].

Enfin, par quatre arrêts en date du 14 janvier 2011, la cour d'appel de Paris a sanctionné la société Google pour contrefaçon[221]. Dans un de ces litiges l'opposant à la société Bac films, la cour a constaté que si la vidéo litigieuse avait bien été retirée, la défenderesse n'avait pas **empêché toute nouvelle diffusion des fichiers litigieux**, engageant ainsi sa responsabilité de droit commun celle-ci s'étant rendue coupable de contrefaçon. La cour a refusé de considérer que chaque remise en ligne constitue un fait nouveau nécessitant une notification distincte telle que prévue par la LCEN.

En raison de l'absence d'un régime légal de **responsabilité des éditeurs** en matière de site internet, la **jurisprudence** a développé deux types de solutions. Tout d'abord, les tribunaux ont, à plusieurs reprises, appliqué le **système de responsabilité en cascade** prévu par la loi du 29 juillet 1982 sur la communication audiovisuelle. Ce **régime de responsabilité pénale** prévoit, en cas d'atteinte à l'intimité et à la vie privée mais aussi en cas de diffamation et injure de même qu'en cas de provocation à la discrimination, diffamation et injure raciale, que le directeur de la publication sera poursuivi comme auteur principal ; à défaut, c'est l'auteur de l'information qui sera poursuivi comme auteur principal, et, à défaut d'auteur, le producteur[222]. De plus, lorsque le directeur de la publication est mis en cause, l'auteur est poursuivi comme complice. L'article 93-3 de la loi de 1982 prévoit toutefois que « [l]orsque l'infraction résulte du contenu d'un message adressé par un internaute à un service de communication au public en ligne et mis par ce service à la disposition du public dans un espace de contributions personnelles identifié comme tel, le directeur ou le codirecteur de publication ne peut pas voir sa responsabilité pénale engagée comme auteur principal s'il est établi qu'il n'avait pas effectivement connaissance du message avant sa mise en ligne ou si, dès le moment où il en a eu connaissance, il a agi promptement pour retirer ce message ». Comme dans toute procédure pénale, la mise en cause de la responsabilité pénale s'accompagne de **l'indemnisation du préjudice** subi par la victime ayant porté plainte.

Cependant, les techniques mises en œuvre sur internet, tout particulièrement les liens hypertextes, n'autorisent pas une approche de la responsabilité purement éditoriale. Dans ce genre de cas, c'est donc plutôt la **responsabilité de droit commun** qui est mise en cause. Ainsi, la Cour d'appel de Paris a retenu, dans un arrêt du 19 septembre 2001, la responsabilité d'un fournisseur de liens hypertexte, en considérant que :

> « si le lien hypertexte constitue un simple mécanisme permettant à l'utilisateur en cliquant sur un mot ou un bouton de passer d'un site à un autre, et si la création, au sein d'un site, d'un tel lien permettant l'accès direct à d'autres sites n'est pas en soi de nature à engager la responsabilité de l'exploitant du site d'origine à raison du contenu du site auquel il renvoie (...) il en est toutefois autrement lorsque la création de ce lien procède d'une démarche délibérée et malicieuse, entreprise en toute connaissance de cause par l'exploitant du site d'origine,

---

219 Cass. 17 février 2011, n°09.67896, disponible sur : www.legifrance.gouv.fr (27.01.2015).

220 Frédérique Chopin, Cybercriminalité, in Dalloz.fr, mars 2014, n°353.

221 CA Paris, 14 janv. 2011, n° 09/11779 : www.legalis.net (27.01.2015).

222 Art. 93-3 de la loi du 29 juillet 1982, disponible sur : www.legifrance.gouv.fr.

lequel doit alors répondre du contenu du site auquel il s'est, en créant ce lien, volontairement et délibérément associé dans un but déterminé »[223].

1.4. Lacunes et difficultés

A défaut de précision sur ce qui doit être compris comme « **manifestement illicite** », selon les termes du Conseil Constitutionnel, la doctrine s'est divisée en deux courants. D'une part, un courant réduit la notion aux contenus dits odieux prévus par l'al. 2 de l'art. 6-I-7 LCEN, c'est-à-dire l'apologie des crimes contre l'humanité, l'incitation à la haine raciale et à la violence, la pornographie enfantine, ainsi que les atteintes à la dignité humaine. Il paraît logique d'ajouter à cette liste les infractions visées par la loi du 13 novembre 2014 concernant les actes de provocation au terrorisme et l'apologie des actes terroristes. D'autre part, un autre courant a une vision plus large de la notion d'activités manifestement illicites, puisqu'il vise tout ce qui est objectivement illicite, c'est-à-dire tous les cas où le caractère illicite découle « d'un manquement délibéré à une disposition de droit positif explicite et dénuée d'ambigüité»[224]. On classerait ainsi dans cette catégorie, outre les actes visés par le premier courant, certaines atteintes au droit de la vie privée. Dans tous les cas, les atteintes à la propriété intellectuelle ne sont pas incluses dans cette catégorie.[225]

En ce qui concerne la procédure de notification prévue à l'art. 6-I-5 LCEN, bien que celle-ci ne soit qu'un élément de preuve de la condition de fond d'après le texte, soit la **connaissance effective du caractère illicite des activités hébergées**, certaines juridictions ont tenté de faire du formalisme prévu par l'article précité une condition de validité de la connaissance effective. Ce faisant, elles ont considéré que si les requérants ne respectaient pas le formalisme de la procédure de notification, par exemple en ne mentionnant pas l'entièreté des informations, leur demande de retrait des activités illicite devait être rejetée. Il convient toutefois de rappeler que, selon le texte de la loi, la procédure de notification crée une présomption simple de connaissance effective du caractère illicite de l'activité hébergée. Il en résulte que le non-respect de la procédure de notification n'emporte pas automatiquement le défaut de connaissance effective et donc le rejet de la demande. Comme le précise très clairement un jugement du 10 juillet 2009 du Tribunal de Grande Instance de Paris, ladite connaissance effective peut « également être prouvée par tous autres moyens de droit »[226].

2. Droit national

2.1. Vue d'ensemble

La LCEN est une législation spécifique aux activités intervenant numériquement. La section relative à la communication au public en ligne contient un dispositif relativement complet visant à assurer aux autorités judiciaires, et indirectement aux utilisateurs, toutes mesures visant la cessation du contenu illicite d'internet, la réparation du préjudice subi ainsi que la communication des informations utiles concernant l'auteur des activités illicites. Nous les détaillons ci-après.

---

223 CA Paris, 4e ch., sect. A, 19 sept. 2001, NRJ et B. c/ Europe 2 Communication : Légipresse 2001, n° 186, III, p. 196

224 C. Castets-Renard, Droit de l'internet : droit français et européen, n°789 ; Elise Ricbourg-Attal ; La responsabilité civile des acteurs de l'internet, Du fait de la mise en ligne de contenus illicites, Larcier, 2014, p. 188, n° 223.

225 Elise Ricbourg-Attal ; La responsabilité civile des acteurs de l'internet, Du fait de la mise en ligne de contenus illicites, Larcier, 2014, p. 187-188, n° 223.

226 TGI Paris, 10 juillet 2009 ; voir en ce sens aussi : Frédérique Chopin, Cybercriminalité, in Dalloz.fr, mars 2014, n°352 ; Elise Ricbourg-Attal ; La responsabilité civile des acteurs de l'internet, Du fait de la mise en ligne de contenus illicites, Larcier, 2014, p. 191, n° 228.

2.2. Dispositions particulières aux fournisseurs de services liés à internet

En application des articles 12 al. 3, 13 al. 2 et 14 a. 3 de la directive 2000/31/CE sur le commerce électronique, les fournisseurs d'hébergement ou d'accès à internet peuvent être contraints, par la voie judiciaire, à cesser ou à prévenir le dommage occasionné par le contenu d'un site internet[227]. En effet, la LCEN prévoit que « l'autorité judiciaire peut prescrire en référé ou sur requête, [au fournisseur d'hébergement] ou, à défaut, [au fournisseur d'accès à des services de communication au public en ligne], toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'une service de communication au public en ligne »[228]. Ces actions en cessation peuvent aboutir tant à des mesures provisoires qu'à des décisions définitives. La demande peut être mise en œuvre auprès de l'hébergeur ou auprès des différents fournisseurs d'accès à internet ; il convient alors de réitérer l'opération auprès de chaque intermédiaire technique. Au vu du caractère général de cette disposition, elle doit être considérée comme susceptible de s'appliquer **indépendamment du motif de l'illicéité** du contenu constatée par le juge.

On relève, toutefois, que le domaine de la **propriété intellectuelle connaît une disposition similaire**, de nature à permettre au juge d'ordonner aux fournisseurs d'accès, d'hébergement et de contenus de prendre toutes les mesures en vue de faire cesser une atteinte aux droits de propriété intellectuelle.

Ainsi, l'art. 336-2 du code de la propriété intellectuelle prévoit qu'en présence d'une atteinte à un droit d'auteur ou à un droit voisin occasionnée par le contenu d'un service de communication au public en ligne, le tribunal de grande instance, statuant le cas échéant en la forme des référés, peut ordonner à la demande des titulaires de droits sur les œuvres et objets protégés, de leurs ayants droit, des sociétés de perception et de répartition des droits d'auteur ou des organismes de défense professionnelle, **toutes mesures propres à prévenir ou à faire cesser une telle atteinte à un droit d'auteur ou un droit voisin, à l'encontre de toute personne susceptible de contribuer à y remédier**. [229]

De plus, aux fins de renforcer la lutte contre le terrorisme en particulier, le législateur français a récemment[230] introduit une nouvelle disposition dans la LCEN, en application de laquelle les fournisseurs d'hébergement ainsi que les fournisseurs de contenus peuvent être contraints, par **décision de l'autorité administrative compétente** – et donc, sans intervention judiciaire – de **retirer** les contenus internet qui constituent des infractions aux dispositions pénales sanctionnant la **pédopornographie**[231] ou le fait de provoquer à des actes de **terrorisme** et de faire l'apologie du

---

227 Il convient de préciser que le prestataire d'activités de stockage automatique, visé à l'art. 13 al.2 de la directive 2000/31/CE sur le commerce électronique peut également faire l'objet d'une action en cessation même s'il n'est pas visé de manière expresse par la LCEN. En effet, le prestataire d'activités de stockage automatique est *de facto* soit un fournisseur d'accès qui pour les besoins de son activité utilise la technique de stockage temporaire, soit un fournisseur d'hébergement ou hébergeur qui stocke les données pendant la durée souhaitée par son client (L. Grynbaum, C. Le Goffic, L. Morlet-Haïdara, Droit des activités numériques, Paris, 2014, p. 916, n°1252).

228 Art. 6.I.8 LCEN.

229 Dans le même sens, l'art. 336-1 du code de la propriété intellectuelle prévoit que : « Lorsqu'un logiciel est principalement utilisé pour la mise à disposition illicite d'œuvres ou d'objets protégés par un droit de propriété littéraire et artistique, le président du tribunal de grande instance, statuant en référé, peut ordonner sous astreinte toutes mesures nécessaires à la protection de ce droit et conformes à l'état de l'art.
Les mesures ainsi ordonnées ne peuvent avoir pour effet de dénaturer les caractéristiques essentielles ou la destination initiale du logiciel. »

230 Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions sur la lutte contre le terrorisme, disponible sur : www.legifrance.gouv.fr.

231 Art. 227-23 code pénal prévoit : Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un

terrorisme[232] [233]. Ce faisant, les fournisseurs d'hébergement et de contenu concernés sont tenus d'informer les fournisseurs d'accès.

D'après le décret du 5 février 2015[234] chargé de mettre en œuvre les dispositions récemment introduite dans la LCEN par la loi du 13 novembre 2014 renforçant la lutte contre le terrorisme, l'autorité administrative en charge du blocage administratif de ces sites internet est la direction générale de **la police nationale**, office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. Au sein de cette autorité administrative, **seuls certains agents individuellement désignés** et dûment habilités par le chef de l'office sont autorisés à mettre en œuvre la procédure de blocage.

Le dispositif mis en place prévoit qu'en l'absence de retrait de ces contenus dans un délai de 24 heures, ladite autorité administrative peut **notifier aux fournisseurs d'accès la liste des adresses électroniques** des services de communication au public en ligne contrevenant auxdites dispositions pénales, ceux-ci étant alors tenus d'empêcher sans délai l'accès à ces adresses, et donc de les **bloquer**. D'après le décret du 5 février 2015, la transmission des adresses électroniques concernées s'effectue selon un mode sécurisé qui en garantit l'intégrité et la confidentialité[235]. De plus, les adresses électroniques concernées comportent soit un nom de domaine (DNS), soit un nom d'hôte caractérisé par un nom de domaine précédé du nom de serveur. Dans les 24 heures de la notification susmentionnée, les fournisseurs d'accès à internet doivent empêcher par tout moyen approprié l'accès aux services fournis par les adresses électroniques figurant sur la liste et le transfert vers ces services.

---

caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou représentation.
Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines.
Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques.
Le fait de consulter habituellement ou en contrepartie d'un paiement un service de communication au public en ligne mettant à disposition une telle image ou représentation, d'acquérir ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30 000 euros d'amende.
Les infractions prévues au présent article sont punies de dix ans d'emprisonnement et de 500 000 euros d'amende lorsqu'elles sont commises en bande organisée.
La tentative des délits prévus au présent article est punie des mêmes peines.
Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image. »

232 Art. 421-2-5 code pénal prévoit : « Le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes est puni de cinq ans d'emprisonnement et de 75 000 € d'amende.
Les peines sont portées à sept ans d'emprisonnement et à 100 000 € d'amende lorsque les faits ont été commis en utilisant un service de communication au public en ligne.
Lorsque les faits sont commis par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables. »

233 Art. 6-1, alinéa 1er de la LCEN

234 Décret 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique, J.O., 6 février 2015. Ce décret est entré en vigueur le 7 février 2015.

235 Art. 2 Décret 2015-125.

Les fournisseurs ne peuvent **pas modifier la liste** des adresses électroniques concernées, que ce soit par ajout, suppression ou altération et elles sont tenues de préserver la confidentialité des données qui leur sont confiées. Les utilisateurs des services de communication au public en ligne auxquels l'accès est empêché sont dirigés vers une page d'information du ministère de l'intérieur, indiquant pour chacun des deux cas de blocage (sites pédopornographiques et sites provoquant à des actes de terrorisme ou en faisant l'apologie) les motifs de la mesure de protection et les voies de recours.

Certaines personnes conservent un accès aux adresses électroniques des services de communication au public en ligne auxquels l'accès est empêché : il s'agit des agents, individuellement désignés et dûment habilités par l'autorité hiérarchique dont ils relèvent, des services de l'Etat compétents en matière de prévention et de répression du terrorisme ou de lutte contre la pédopornographie, ainsi qu'à une personnalité qualifiée désignée en son sein par la **Commission nationale de l'informatique et des libertés**, dont la mission est de s'assurer de la **régularité des demandes** de retrait et des conditions d'établissement, de mise à jour de communication et d'utilisation de la liste[236].

Si l'autorité administrative est dans l'impossibilité de contacter le fournisseur de contenus ou d'hébergement en vue du retrait du contenu illicite – et ce, alors que leurs données doivent légalement être mises à la disposition du public[237] –, elle est en mesure de requérir directement le blocage du site internet directement auprès du fournisseur d'accès, sans solliciter préalablement le retrait du contenu auprès de l'hébergeur ou de l'éditeur.

L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication **vérifie au moins chaque trimestre** que le contenu du service de communication contrevenant présente **toujours un caractère illicite**. Lorsque ce service a disparu ou que son contenu ne présente plus de caractère illicite, l'office retire de la liste les adresses électroniques correspondantes et notifie sans délai ce retrait à la personnalité qualifiée et aux fournisseurs d'accès à internet. Dans un délai de vingt-quatre heures suivant cette notification, ceux-ci **rétablissent par tout moyen approprié l'accès** aux services fournis par les adresses électroniques retirées de la liste et le transfert vers ces services.

Enfin, toujours en ce qui concerne les contenus d'internet qui constituent des infractions aux dispositions pénales sanctionnant la pédopornographie ou le fait de provoquer à des actes de terrorisme et de faire l'apologie du terrorisme, l'autorité administrative peut également notifier les adresses électroniques des sites concernés aux moteurs de recherche ou aux annuaires, lesquels sont alors tenus de prendre toutes les mesures utiles pour faire **cesser le référencement** du site en cause.

Les personnes morales qui manqueraient aux obligations prévues par la LCEN en ce qui concerne les contenus relatifs à la pédopornographie ou à la provocation ou l'apologie du terrorisme, tels que

---

236 L'al. 3 de l'art. 6-1 LCEN prévoit que cette personnalité de la CNIL peut, si elle constate une irrégularité, à tout moment, recommander à l'autorité administrative d'y mettre fin. Si celle-ci ne suit pas cette recommandation, la personnalité qualifiée peut saisir la juridiction administrative compétente, en référé ou sur requête. En vertu de l'art. 5 du Décret 2015-125, la désignation de la personnalité qualifiée est publiée au Journal officiel de la République française. La personnalité qualifiée dispose pour l'exercice de ses fonctions des services de la Commission nationale de l'informatique et des libertés. Lorsqu'il est nécessaire de traduire en langue française les contenus des services de communication au public en ligne concernés par les mesures de blocage, elle est assistée d'un interprète. L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication met à la disposition de la personnalité qualifiée les demandes de retrait adressées aux hébergeurs et aux éditeurs ainsi que les éléments établissant que les contenus des services de communication au public en ligne concernés constituent des infractions de pédopornographie ou de provocation à des actes de terrorisme ou d'apologie de tels actes.

237 Art. 6.III LCEN, voir aussi supra section 1.2.

présentés ci-dessus, sont punis d'une amende de 375.000 Euros et encourent également l'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ainsi que l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite, soit par tout moyen de communication au public par voie électronique.

Le décret 2015-125 prévoit encore que **les éventuels surcoûts** résultant des obligations mises à la charge des fournisseurs d'accès en matière de blocage administratif de sites internet font l'objet d'une **compensation financière prise en charge par l'Etat**. Le terme de « surcoût » désigne les coûts des investissements et interventions spécifiques supplémentaires résultant de ces obligations. Pour obtenir une compensation, les fournisseurs d'accès adressent à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication un document détaillant le nombre et la nature des interventions nécessaires ainsi que le coût de l'investissement éventuellement réalisé. Le Conseil général de l'économie, de l'industrie, de l'énergie et des technologies analyse le document transmis, notamment au regard des coûts habituellement estimés dans le secteur concerné. L'Etat procède, sur présentation d'une facture, au paiement des compensations correspondant aux surcoûts justifiés au vu de l'analyse du Conseil général de l'économie, de l'industrie, de l'énergie et des technologies.

2.2.1. Actions en réparation

La LCEN ne prévoit **pas de disposition expresse relative à l'octroi de dommages et intérêts** et nos recherches n'ont pas permis d'identifier de la jurisprudence en la matière.

Les juges sont toutefois en mesure de condamner, en application de l'art. 700 du Code de procédure civile, la partie perdante au paiement à l'autre partie de la somme qu'ils déterminent, au titre des **frais exposés** et non compris dans les dépens. Il s'agit, dans ce cas, d'une indemnisation pour le préjudice causé par la **nécessité d'introduire une action en justice** pour obtenir gain de cause. Il en va, par exemple, ainsi dans le cas où, malgré la notification prévue par la LCEN, l'hébergeur n'a pas agi promptement pour retirer le contenu illicite. Ainsi, la société eBay, en tant qu'hébergeur, a été condamnée à payer 1500 euros au titre de frais de justice pour n'avoir pas retiré le contenu illicite su site hébergé malgré la notification de la partie demanderesse, contraignant celle-ci à introduire une action en justice[238]. De même, dans un arrêt du 6 décembre 2009, la Cour d'appel de Paris a condamné Google au paiement d'une somme de 1500 euros en raison des frais exposés par la partie demanderesse qui a souffert de ce que le logiciel *Google Suggest* proposait en premier lieu aux utilisateurs le mot « arnaque » lorsqu'ils saisissaient dans la barre de recherche le nom de la partie demanderesse. Un telle somme est octroyée par le juge en tenant compte de l'équité. L'art. 700 du Code de procédure civile précise qu' « [i]l peut, même d'office, pour des raisons tirées des […] considérations [d'équité], dire qu'il n'y a pas lieu à ces condamnations ».

2.2.2. Actions visant l'obtention d'informations

Si les fournisseurs d'accès à des services de communication au public en ligne ainsi que les fournisseurs d'hébergement n'ont pas d'obligation de surveillance générale, d'une part, ils peuvent être chargés, par les autorités judiciaires, d'une mission de surveillance ciblée et temporaire impliquant qu'elles informent lesdites autorités des résultats obtenus (article 6.I.7 LCEN), et d'autre part, ils ont l'obligation d'informer les **autorités compétentes** de certaines activités illicites particulièrement graves (art. 6.I.7. al. 4 LCEN).

---

238 T. Com. Brest, ord. réf., 6 août 2008: www.legalis.net (27.01.2015) ; voir dans le même sens : CA Paris, Pôle 1, 2ème section, 9 décembre 2009 : www.legalis.net (27.01.2015).

En matière de **protection de la propriété intellectuelle**, la loi 2007-1544 du 29 octobre 2007 de lutte contre la contrefaçon (ci-après la « loi de 2007 ») a eu pour effet d'inclure une disposition octroyant la possibilité aux juridictions saisies au fond ou en référé d'une procédure civile en matière de contrefaçon, d'ordonner à toute personne intervenant notamment dans la distribution de produits argués de contrefaçon de fournir des informations sur l'origine de ces produits, les réseaux de distribution ainsi que tout document qu'elle détiendrait à ce propos. Cette obligation d'information s'applique ainsi à tous les fournisseurs de services liés à internet qui détiendraient de telles informations relativement à des produits argués de contrefaçon et existe pour tous les droits de propriété intellectuelle, en particulier le droit d'auteur, ses droits voisins et les droits du producteur de bases de données[239], les modèles et dessins[240], les brevets d'invention[241], les marques[242], les indications géographiques[243] et les connaissances techniques[244].

2.3. Application du droit commun aux fournisseurs de services liées à internet

Depuis l'entrée en vigueur de la LCEN, le droit commun ne semble intervenir qu'**à titre de complément** des dispositions spécifiques aux fournisseurs de services liées à internet. Ainsi, comme déjà évoqué, la LCEN ne prévoit pas de régime de responsabilité spécifique pour les fournisseurs de contenus sur internet ou éditeurs. Si, selon les circonstances de l'espèce, le régime de responsabilité pénale des éditeurs de presse ne peut être appliqué aux éditeurs dans le domaine d'internet, il reste possible de mettre en cause leur responsabilité civile de droit commun. Il en va ainsi en matière d'atteinte à la vie privée et au droit à l'image protégés par l'art. 9 du Code civil, de dénigrement de produits ainsi qu'en matière d'atteinte aux droits de propriété intellectuelle. On relève ainsi que, dans un jugement du 13 février 2007, le Tribunal de Grande Instance de Paris a condamné Google pour avoir fourni une marque protégée comme mot-clé à un concurrent sans avoir vérifié si les mots-clés proposés par son service étaient ou non réservés au titre d'un droit privatif et, le cas échéant, si l'annonceur, en choisissant ce mot-clé, justifiait de droits sur celui-ci[245].

Comme déjà exposé, les mesures de **retrait ou de blocage des activités** illicites en application de la LCEN constituent l'une des modalités de la réparation intégrale du préjudice subi. Toutefois, l'octroi de **dommages et intérêts** peut constituer, selon les cas, un complément nécessaire. Ainsi, en matière d'atteinte à la propriété intellectuelle, des dispositions d'ordre général au sens qu'elles ne sont pas spécifiques au domaine d'internet, prévoient l'octroi de dommages et intérêts afin de compenser le préjudice subi en raison de l'atteinte portée au droit de propriété intellectuelle. En matière de marques, l'art. L716-4 al. 1er CPI prévoit l'octroi de dommages et intérêts pour les atteintes portées au droit du propriétaire de la marque, en particulier pour des reproductions de la marque sans l'autorisation du propriétaire. La jurisprudence reconnaît toutefois que, même lorsque ces dispositions ne sont pas applicables en raison des circonstances de l'espèce, l'atteinte portée à la marque justifie, en application des règles de responsabilité civile de droit commun, l'octroi d'une indemnisation, aux fins en particulier de réparer le préjudice causé à la fois par le détournement de clientèle résultant de l'atteinte à la marque ainsi que la perte d'image qui en est résultée[246].

---

239 Art. L. 331-1-2 Code de la propriété intellectuelle.

240 Art. L. 521-5 Code de la propriété intellectuelle.

241 Art. L. 615-5-2 Code de la propriété intellectuelle.

242 Art. L. 716-7-1 Code de la propriété intellectuelle.

243 Art. L. 722-5 Code de la propriété intellectuelle.

244 Art. L. 623-27-2 Code de la propriété intellectuelle.

245 TGI Paris, 3ème ch., 1ere section, 13 février 2007 : www.legalis.net (27.01.2015).

246 TGI Paris, 3ème ch., 2ème section, 11 juin 2010 : www.legalis.net (27.01.2015) ; voir dans le même sens : CA Paris, Pôle 5, 2ème ch., 14 janvier 2011, www.legalis.net (27.01.2015).

2.4. Rapport entre les dispositions

Il ressort de nos recherches qu'en droit français, les dispositions spécifiques aux ISP constituent un dispositif relativement complet et précis. Dans les rares cas où les activités des ISP ne sont pas régies par des dispositions spécifiques, il semble que les juridictions aient agi de telle manière à **compléter le dispositif en place en faisant référence aux dispositions d'ordre général**. C'est le cas pour le régime de responsabilité pour les activités des fournisseurs de contenu ou éditeurs dans le domaine d'internet. C'est également le cas pour certaines atteintes telles que les atteintes aux droits de la propriété intellectuelle qui sont régies dans le code de propriété intellectuelle, indépendamment de la question de savoir comment et par qui l'atteinte au droit de propriété intellectuelle a été portée.

3. Implementation / Mise en oeuvre

3.1. Vue d'ensemble

La présente section met en lumière les règles spécifiques de procédure civile internationale en matière de litiges relatifs au réseau Internet.

3.2. Faits nationaux

La LCEN ne contient pas de disposition spécifique en ce qui concerne les règles de procédure civile applicable en matière d'actions en responsabilité des fournisseurs de services liés à internet. Ce sont donc les règles générales de procédure civile qui s'appliquent.

En matière de propriété intellectuelle, le code de propriété intellectuelle prévoit que les actions civiles sont exclusivement portées devant le tribunal de grande instance[247].

3.3. Faits internationaux

S'agissant du réseau Internet, les règles permettant de déterminer les juridictions territorialement compétentes ont évolué. Si, dans un premier temps, les juridictions ont considéré qu'elles étaient compétentes dès que le site était accessible en France[248], elles ont, plus récemment, cherché à établir et caractériser, dans chaque cas, **un lien suffisant, substantiel ou significatif entre les faits ou actes et le dommage allégué**[249]. Ainsi, la Cour de Cassation a confirmé la compétence des juridictions françaises pour statuer sur l'atteinte portée à des marques utilisées par un site à titres de mots-clés, après avoir relevé que la saisie de mots-clés en liaison avec les marques renvoyait les utilisateurs vers des plateformes de commerce en ligne, lesquels visaient des internautes français, et que les produits proposés étaient livrables en France[250].

3.4. Propositions

Eu égard aux modifications récentes apportées dans le dispositif législatif et réglementaire applicable en matière de blocage de sites internet, nos recherches n'ont pas permis d'identifier de nouvelles propositions concrètes dans le domaine.

---

247 Voir par exemple : art. L.331-1 CPI et L615-17 CPI.

248 Cass. 1ère civ., 9 décembre 2003, n° 01-03225: www.legifrance.gouv.fr (27.01.2015).

249 CA Paris, 4ème ch. A, 26 avril 2006 : www.legalis.net (27.01.2015) ; Cass. com., 9 mars 2010, n°08-16752 et : Cass. com., 23 novembre 2010, n° 07-19543 (www.legifrance.gouv.fr (27.01.2015)).

250 Cass. com., 7 décembre 2010, n° 09-16811 : www.legifrance.gouv.fr (27.01.2015).

D. UK (ENGLAND)

1. Transposition of European Law

1.1. Overview

The transposition of relevant European Directives in to UK law is typically by way of secondary legislation in the form of Statutory Instruments but is also achieved through the insertion of new statutory provisions into existing Acts of Parliament, or as was the case for data protection laws, by the creation of a new Statute. Interestingly, the common law in England and Wales, in the form of existing jurisprudence, already catered for the type of court order demanded by Article 8 of Directive 2004/48/EC, and thus, no additional legislation was necessary.

1.2. Transposition of European Directives

Directive 2000/31/EC (the "E-Commerce Directive") was transposed into UK law by secondary legislation, the Electronic Commerce (EC Directive) Regulations 2002 (the "E-Commerce Regulations"), on 21st August 2002.[251]

Regulations 17, 18 and 19 of the E-Commerce Regulations are lifted almost verbatim from, respectively, the Directive Articles 12, 13 and 14. One key difference with the Directive is that the Regulations specify that the qualified immunity regime concerning online intermediaries applies in respect of third party material which is unlawful at both civil and criminal law. A further variation is that Regulation 22 provides some guidance as to what may constitute 'actual knowledge' referred to in Regulations 18 and 19. This is a non-exhaustive list of factors which a court may consider when deciding whether an intermediary has received, via any means of contact that has made available in compliance with Regulation 6(1)(c), actual notice of unlawful third party material present on its servers. Regulation 6(1) makes it obligatory for intermediaries to provide certain information to the end user, "*in a form….which is easily, directly and permanently accessible*." Regulation 6(1)(c) refers to contact details which facilitate rapid and direct communication with the intermediary, such as email addresses, telephone numbers and other contact details.

Regulation 20 states: "*Nothing in regulations 17, 18 and 19 shall ……(b) affect the rights of any party to apply to a court for relief to prevent or stop infringement of any rights.*" The available protections from criminal and pecuniary liability do not therefore affect the possibility of the grant of injunctions.

Regulation 22 also lists several other factors which a court may consider; these are the extent to which any notice includes the full name and address of the sender of the notice, details of the location of the information in question and details of the unlawful nature of the activity or information in question.

Article 8 of **Directive 2004/48/EC** (the "Enforcement Directive") was implemented in to **Scottish law** on 29th April 2006 by secondary legislation, namely Regulation 4 of The Intellectual Property (Enforcement, etc.) Regulations 2006 (the "Intellectual Property Regulations").[252] This created a new type of court order, for disclosure of information about infringing goods and services. In **England & Wales and Northern Ireland**, such a court order was already available under the common law. The Explanatory Notes to the Intellectual Property Regulations explain that by reason of the House of Lords

---

251 Electronic Commerce (EC Directive) Regulations 2002 (Statutory Instrument 2013/2002), available at http://www.legislation.gov.uk/uksi/2002/2013/contents/made (21.01.2015).

252 The Intellectual Property (Enforcement, etc.) Regulations 2006 (SI 1028/2006) available at http://www.legislation.gov.uk/uksi/2006/1028/pdfs/uksi_20061028_en.pdf (21.01.2015).

decision in the 1974 case of *Norwich Pharmacal v Customs and Excise Commissioners*,[253] no provision is necessary to implement in England and Wales or Northern Ireland the obligation set out in Article 8 of the Enforcement Directive. It was ruled in *Norwich Pharmacal* that UK courts may grant orders (known as ***Norwich Pharmacal orders***) against innocent third parties which have been mixed up in wrongdoing. By identifying individuals, the documents and information sought are disclosed in order to assist the applicant for such an order in bringing legal proceedings against individuals who are believed to have wronged the applicant. Although first developed in relation to intellectual property, *Norwich Pharmacal orders* are now granted in relation to other torts, as well as defamation and breach of contract and alleged criminal offences. These have also been used against internet hosting services and internet service providers to identify users which have allegedly engaged in wrongdoing.[254]

Article 8(3) of **Directive 2001/29/EC** which requires that rights owners be able to apply for injunctions against intermediaries whose services are used by third parties to infringe rights is implemented into UK law by way of the Copyright and Related Rights Regulations 2003,[255] which inserts a new **section 97A into the Copyright, Designs and Patents Act 1988**.[256] This introduces a specific power to grant injunctions against service providers, irrespective of the existence or otherwise of any underlying act of infringement by the service provider. All that is required for the power to grant an injunction to be available is actual knowledge on the part of the service provider of another person using the service to infringe copyright. It is not necessary to prove that the service provider was itself directly or indirectly liable for infringement. The notice provisions of section 97A(2) are broadly similar to those of Regulation 22 of the E-Commerce Regulations (discussed above).

With the adoption of **Directive 95/46/EC**, the UK Government chose to enact new primary legislation in the form of the Data Protection Act 1998;[257] this received Royal Assent on 16th July 1998, although it did not come into force until 1st March 2000. Prior to this, the – now repealed - Data Protection Act 1984 was solely concerned with automatically processed personal data. In contrast, the 1994 Directive and the Data Protection Act 1998 extend the scope of protection to manual records as well as computer records, providing they comprise a 'relevant filing system'. To constitute a 'relevant filing system', the set of information must be "*structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily available.*"[258]

1.3. Case-law

There still remains very little UK case law directly addressing the E-Commerce Regulations.

In March 2006, in the case of ***Bunt v Tilley***,[259] an English court for the first time considered the intermediary liability provisions of the E-Commerce Regulations. This concerned Internet Service Providers ("ISPs") which are considered to be a '**mere conduit**', engaged only in the transmission of information or the provision of access to a communication network. The usefulness of the decision in providing guidance for the future is limited by the fact that the claimant acted in person, without the

---

253 *Norwich Pharmacal v Customs and Excise Commissioners* [1974] Appeal Cases 133.

254 Graham J H Smith, *Internet Law and Regulation,* 4th ed., Thomson Sweet & Maxwell, 2007, p.441.

255 The Copyright and Related Rights Regulations 2003 (Statutory Instrument 2498/2003), available at http://www.legislation.gov.uk/uksi/2003/2498/contents/made (21.01.2015).

256 Copyright, Designs and Patents Act 1988, available at http://www.legislation.gov.uk/ukpga/1988/48/contents (21.01.2015).

257 Data Protection Act 1998, available at http://www.legislation.gov.uk/ukpga/1998/29/contents (21.01.2015).

258 Data Protection Act 1998, section 1.

259 *Bunt v Tilley* [2006] England and Wales High Court 407 (Queen's Bench).

benefit either of legal representation or of independent expert evidence, with the result that the factual basis on which the court made its findings is confusing and difficult to discern.[260] The claimant, Bunt, was suing six different parties for defamation of him and his business. Bunt claimed that he had notified the defendants via email of some defamatory allegations, before later bringing an action in respect of both those and further allegations made by the same persons. Three of the six defendants in this case were companies who offered internet services, and at a hearing to consider whether the case against them should be struck out, the Judge said that the question to be considered by the court was whether the ISPs could be liable for material, "*which is simply communicated via the services which they provide.*"[261] Although deciding that, on the basis of defamation law, there was no case for the ISPs to answer, the Judge did consider *obiter* the application of the immunities provided in Regulations 17 and 18 of the E-Commerce Regulations (i.e., those found at **Articles 12 and 13 of the E-Commerce Directive**).

On the facts, it was decided that the ISPs had not received any information in Bunt's emails which should have caused them to believe that they were contributing to or causing the publication of the alleged defamatory statements, and the Judge furthermore rejected the claimant's argument that an ISP, by its very nature as an access provider, can in a sense be said to be in control of the information that the user is able to access online, offering much more than a connection to the internet. There was nothing in the Regulations, said the Judge, to support the claimant's contention that an ISP acts as a 'gatekeeper' to information.

The court furthermore confirmed that the **E-Commerce Regulations would not preclude an injunction** (as permitted under Regulation 20(b)), but only apply to financial and penal sanctions. The Judge found in the present case however that the injunctive relief sought by the claimant against the ISP providers would have been wholly disproportionate to any conceivable legitimate advantage.

As to the protection offered to **ISP *hosts*** which originate from Article 14 of the E-Commerce Directive, the 2009 case of ***L'Oreal v eBay***[262] was referred by the English Courts for clarification of the law on a number points, including the matter of, "***whether the service provided by the operator of an online marketplace is covered by Article 14(1) of Directive 2000/31***." In the judgment of the Grand Chamber: "*…the fact that the service provided by the operator of an online marketplace includes the storage of information transmitted to it by its customer-sellers is not in itself a sufficient ground for concluding that that service falls, in all situations, within the scope of Article 14(1)…"*[263] However, where an operator such as Ebay has provided assistance in the form of optimising presentation of the offers of sale by customer-sellers, or promoting those offers, it cannot then be considered to have taken a neutral position, but instead, to have played an active role of such a kind as giving it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely on the Article 14(1) exemption. The question of whether eBay's use of the relevant data in this case amounted to an active role sufficient to deprive it of the protection of Article 14(1) was referred back to the UK courts to make a decision on the facts of the case.

One further known case in which Article 14 of the E-Commerce Directive featured is that of ***Tamiz v Google***.[264] This partly concerned the 'notice and takedown' provision. Google (which ran the Blogger service at issue) advanced an argument that it did not have sufficient notice for the Article 14 obligation to take down to be triggered. The Judge at the High Court made it clear that a complaint about content is not notice, and that there must be enough evidence of unlawfulness before takedown becomes

---

260 See Graham J H Smith, *Internet Law and Regulation, op. cit.,* p. 373.

261 Justice Eady, *ibid, para. 5.*

262 *L'Oreal v Ebay* [2009] England and Wales High Court 1094 (Chancery Division).

263 Case C-324/09, *L'Oreal v Ebay,* para 106.

264 *Tamiz v Google* [2012] England and Wales High Court 449 (Queen's Bench Division)

necessary. In this case, allegations by the claimant that defamatory statements had been made about him did not, the court said, have to be taken at face value, and would not have amounted to the necessary 'actual knowledge' of illegality which would deprive Google of the possibility to rely on the immunity granted under Article 14 of the E-Commerce Directive or to take action to take down the statements. Although this case subsequently featured in the Court of Appeal, the court did not address Article 14, the matter having already been resolved on other legal grounds.

Useful clarity has been provided in case law dealing with ***Norwich Pharmacal* orders** in the context of copyright and ISPs. As discussed in section 1.2. above, these are the orders for documents and information of the kind envisaged by Article 8 of **Directive 2004/48/EC**.

In the 2012 case of *Golden Eye v Telefonica*,[265] claimants alleged that copyright in various adult films made by them had been infringed by individuals subscribed to O2, the ISP, for example, by copying the films without consent. O2 did not oppose the application in this case, but **required a court order before disclosing information about its subscribers**. In granting the order, the Judge stressed that one of the key factors in deciding whether or not to grant a *Norwich Pharmacal* order in a file-sharing case is how to balance the rights of copyright owners/licensees, and the right of subscribers to an ISP to data protection and privacy.

The new legislative provision allowing for injunctions of the kind demanded by Article 8(3) of **Directive 2001/29/EC** was first successfully secured a group of cases which have come to be known as the *Newzbin cases.*

Section 97A of the Copyright, Designs and Patents Act 1988 ("CDPA") was successfully deployed to force ISP, British Telecom ("BT"), to block its customers' access to an online service used for mass copyright infringement. Website *Newzbin* was turning over £1m a year by charging users for a service which greatly facilitated their downloading of copyright-protected films and other material from Usernet, a bulletin board system predating, but less popular than the World Wide Web. In 2010, the High Court had found that *Newzbin* was committing infringements of Twentieth Century Fox Studio's copyright, and ordered it to be shutdown, which it subsequently was. However, a sequel service was created, *Newzbin2*, which provided exactly the same service. The Studios this time[266] **relied on section 97A of the CDPA to target BT, the largest ISP in the jurisdiction, in order to obtain an injunction** on the basis that BT had actual knowledge of *Newzbin2* using their service to infringe copyright. The Judge rejected BT's arguments that its service was not being used to infringe copyright, that it did not have actual knowledge and that an injunction would be contrary to Articles 12(1) and 15(1) of the E-Commerce Directive. Even if BT was a 'mere conduit' under Article 12(1) of the E-Commerce Directive, Article 12(3) specifically preserves jurisdiction for courts to impose injunctions. Furthermore, a general obligation on ISPs to monitor the information they transmit, prohibited under Article 15(1), would not, said the court, be the effect of the injunction the Studios sought.

1.4. Lacunae and difficulties

The following known lacunae and difficulties related to the transposition of the E-Commerce Directive have been identified by commentators:

- **Linking**: the liability position of an intermediary which hosts a hypertext link to a page stored elsewhere which contains unlawful material is unclear, and has been described as a significant omission in the provisions of both the E-Commerce Directive and the E-Commerce Regulations. Is

---

265 *Golden Eye v Telefonica* [2012] England and Wales High Court 723 (Chancery Division).

266 In the case of *Twentieth Century Fox Film Corp & Others v British Telecommunications Plc* [2011] England and Wales High Court 1981 (Chancery Division).

it the case, for example, that the Article 14/Regulation 19 immunity would apply such that an intermediary which hosts an obvious link that clearly points towards unlawful material is likely to face liability, but if the link is obscure and buried among hundreds of thousands of links on the intermediary's servers, no liability will arise?[267]

- **Territorial scope of the E-Commerce Directive and Regulations**: although the recitals (specifically, Recital 58) of the E-Commerce Directive state that the Directive should not apply to services supplied by service providers established in a third country, this provision is not transposed into the domestic E-Commerce Regulations. The liability of intermediaries provisions of the E-Commerce Regulations are stated to apply to "service providers", defined as any person providing an information society service. The protection provided by the E-Commerce Regulations is, therefore, on the face of it, not restricted to service providers established within the European Economic Area.[268]

- **Scope and degree of protection offered by Article 14**: It is said to be debateable whether Article 14 of the E-Commerce Directive applies only to the purely technical act of hosting, or includes a broader range of those who store, or have caused to be stored, information on behalf of third parties. Recital 42 of the Directive suggests a narrow technical view of the liability exemptions should be adopted, but, despite its opening wording that it applies to, "*the exemptions from liability established in this Directive*," it is concerned only with conditions which have no relevance to hosting. A preferred interpretation of Article 14 is that it therefore applies more broadly to those who, in a general sense, store third party information. This, for example, would then serve to protect a proprietor of a web discussion forum (contributed to by third parties), regardless of whether they have outsourced the technical hosting function.

  A further issue is the reference in Article 14 to "storage"; this provides that service providers are, ""*not liable for the information stored…*" Given that the subject matter of the E-Commerce Directive is the commercial business of making information publicly available through electronic networks and devices, it is said that this reference should be properly understood as providing a host with protection from liability incurred as a result both of storing information and of providing access to the stored information. Unfortunately, the UK E-Commerce Regulations do not use language which make this interpretation clear: an approximation of the Article 14 language is used which focuses on protection from liability arising specifically from the act of storage: "shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that storage…..."[269]

2. National law

2.1. Overview

In the field of civil law, the most significant issues insofar as the liability of ISPs is concerned arise under copyright and defamation laws. This is where recent legislative developments have focused. The success of relevant provisions of the Digital Economy Act 2010 remains to be seen, with the industry-wide Code of Practice yet to be introduced. This will be designed to tackle widespread copyright infringement, applying only to the UK's largest ISPs and allowing copyright owners to make Copyright Infringement Reports to the ISPs who must then notify the subscribers concerned.

---

267 See Chris Reed, *Computer Law*, 7th Ed., Oxford 2011, p.323.

268 See Graham J H Smith, *Internet Law and Regulation, op. cit.,* p. 368.

269 E-Commerce Regulations, Regulation 19, *op. cit.*

Defamation law, historically developed by the common law, has also been adapted to the needs of digital age through recent statutory provisions which offer website operators a defence against potential defamation claims where they have taken prescribed action when notified of potentially defamatory material.

2.2. Provisions specific for ISP

2.2.1. Possibility to request blocking

The Digital Economy Act 2010 was adopted, among other things, to better regulate the online **infringement of copyright**. This inserted a number of new provisions into the existing Communications Act 2003. Although in force, it is understood that these provisions have not yet been implemented in practice due to the absence of an industry-wide code of conduct: something which the provisions themselves require for their proper functioning of these rules. In addition, it seems that this approach has been abandoned in favour of an industry-agreed "memorandum of understanding" establishing a voluntary framework that amounts to little more than a system of sending out "educational notices" to those detected by copyright owners as breaching copyright.[270] It nevertheless seems interesting to briefly explain the approach that would have been followed in the absence of such a Memorandum.

One provision places on internet service providers ("ISPs") an obligation, known as a **'technical obligation'**, to take a technical measure against some or all relevant subscribers to the ISP service for the purpose of preventing or reducing **infringement of copyright** by means of the internet.[271] A 'technical measure' is a measure that (1) **limits the speed or other capacity** of the service provided to the subscriber; (2) **prevents a subscriber from using the service** to gain access to particular material, or **limits such use**; (3) **suspends the service** provided to a subscriber; or (4) **limits the service** provided to a subscriber in another way.[272] Such an obligation may be imposed on an ISP or group of ISPs by an order of the Secretary of State where he/she considers it appropriate to do so, and following an assessment by OFCOM.

Also in the field of **copyright law**, as noted above, **section 97A of the Copyright, Designs and Patents Act 1988** provides the High Court with the **power to grant an injunction** against an ISP to block access to the internet or particular sites where that ISP has actual knowledge of a person using their service to infringe copyright. It is partly because of the availability and successful use of this remedy,[273] that **section 17 of the Digital Economy Act 2010**, which provided for a further power for a blocking injunction, "*in respect of a location on the internet,"* was never implemented through the adoption of secondary legislation and was recently repealed by the Coalition Government.

In the area of **defamation law**,[274] a new piece of primary legislation, the **Defamation Act 2013**, includes a provision, section 13(1), specific to "the operator of a website". This permits successful claimants in defamation cases to apply for **an order compelling the operator of a website to remove a statement posted on the website** (an "Order to remove or cease distribution") that has been found to be

---

270 See Press statement of the UK Government of 19.07.2014, available at https://www.gov.uk/government/news/new-education-programme-launched-to-combat-online-piracy (24.03.2015).

271 Communications Act 2003, section 124G(2), added by the Digital Economy Act 2010. Communications Act 2003 available at http://www.legislation.gov.uk/ukpga/2003/21/contents; Digital Economy Act 2010, available at http://www.legislation.gov.uk/ukpga/2010/24/contents (22.01.2015).

272 Communications Act 2003, section 124G(3).

273 Such as in *Twentieth Century Fox Film Corp & Others v British Telecommunications Plc, op. cit.*

274 For more information on 'defamation' under the English common law, see section 2.3. below.

unlawful, even in cases where the statement was not posted by the operator, and the operator was not a party to the action.[275]

It should be noted that section 5(1) provides a defence to such an operator to a claim of defamation under English common law. Section 5(3), however, enables the defence to be defeated if the author of the alleged defamation is unidentifiable (by the claimant), a notice of complaint was given to the operator, and there was a failure by the operator to respond in accordance with the recently published regulations.[276] These set out tight time periods during which the operator must act in order to continue to be afforded the protection of the statutory provision against any future court action for defamation. In effect however, the operator is (for identifiable authors) not required to take material down and is protected against liability where it passes on a notice of complaint and complies with certain requirements. It is for this reason that section 13(1) was introduced in the course of debates that led to the passage of the 2013 Act, as it ensures that claimants do not experience difficulty in securing the removal of material subsequently found to be defamatory in cases where the author of the material was not in a position to remove it and the section 5 defence, "might prevent the website operator from being required to do so."[277]

2.2.2. Reparation

There are **no known legal provisions unique to ISPs** which provide for compensation or other relief in the case of a breach of legal obligations.

It is however proposed under a forthcoming 'Initial Obligations' Code[278] that an ISP may be required by OFCOM to compensate a copyright owner where it has **contravened a procedure of the Code** itself (rather than having been found to have breached copyright).

Insofar as technical obligations are concerned, ISPs may be subjected to a penalty in accordance with more general provisions contained in the Communications Act 2003 on the enforcement of conditions and penalties for contravention.[279] A contravention by an ISP of a technical obligation can attract a penalty, issued by OFCOM, of **an amount not exceeding £250,000**. In determining the amount, OFCOM must have regard to any representations made to it by the ISP or copyright owner on whom the penalty is imposed, any steps taken by the provider or owner towards complying with the obligations, the contraventions of which have been notified by the provider or owner, and any steps taken by the provider or owner for remedying the consequences of those contraventions.[280]

---

275 Defamation Act 2013, section 13, available at http://www.legislation.gov.uk/ukpga/2013/26/contents/enacted (03.03.2015).

276 The Defamation (Operators of Websites) Regulations 2013, available at http://www.legislation.gov.uk/uksi/2013/3028/contents/made (22.01.2015). See also Ministry of Justice issued guidance "*Complaints about defamatory material posted on websites: Guidance on Section 5 of the Defamation Act 2013 and Regulations*", January 2014, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/269138/defamation-guidance.pdf (22.01.2014).

277 Hansard, House of Commons, 12 September 2012, col 309 in M. Collins, *Collins on Defamation*, Oxford University Press 2014, p. 404.

278 See 2.2.3. below.

279 The Communications Act 2003, sections 94-96.

280 The Communications Act 2003, section 124L(3).

2.2.3. Information Rights

Also under the Communications Act 2003,[281] as amended by the Digital Economy Act 2010, there are what are known as '**initial obligations**' on ISPs, one of which is **a duty to report online copyright infringement**. If it appears to a copyright owner that a subscriber to an internet access service has infringed that owner's copyright by means of the service, the owner may make a copyright infringement report to the ISP who provided the internet access service, and an ISP who receives such a report must then **notify the subscriber of the report**. Such obligations are triggered only where provided for in the '**Initial Obligations Code**'.[282]

A further 'initial obligation' is a duty on ISPs to provide, in accordance with the relevant 'initial obligations code' what are known as a '**copyright infringement list**' to copyright owner for a particular period if the copyright owner asks for one. Such a list sets out in relation to each relevant subscriber to the internet service, which of the copyright infringement reports made by the copyright owner to the ISP (see 2.2.2. above) relate to the subscriber concerned, but does not enable any subscriber to be identified.[283]

If a website operator wishes to avail itself of the defence provided for in section 5 of the Defamation Act 2013[284] against **legal action for defamation**, it is under certain duties to provide and seek information from the complainant and the poster of the alleged defamatory material. In particular, where the operator receives a valid Notice of Complaint, it must – if it wishes to benefit from the statutory defence – provide an anonymised copy of the Notice of Complaint to the poster, where identified, and **indicate that the statement may be removed unless the poster**:[285]

- Informs the operator **whether or not the poster wishes the statement complained of to be removed** from the locations on the website specified in the Notice of Complaint;
- If the poster does not wish the statement to be removed, **provides the operator with the poster's full name and details of the postal address at which the poster resides** or carries on business; and
- Indicates **whether the poster consents to the operator sending these details to the complainant**.

2.3. Application of general provisions / common law to ISP

2.3.1. Injunctions (prohibitions to carry out a certain activity)

Under English law, provisions which serve to prohibit or to require the carrying out of certain activity are usually found in court orders known as 'injunctions'. An injunction is an equitable remedy, being a remedy that originated in the English courts of equity.[286] Injunctions can apply in many cases, and outside the fields of contract law and criminal law, their potential application to ISPs for their own

---

281 The Communications Act 2003, section 124A, 124B and 124C.

282 See section 2.2.1. above.

283 The Communications Act 2003, section 124B(1) and (2).

284 See section 2.2.1. of section D, above.

285 See The Defamation (Operators of Websites) Regulations 2013, *op. cit.*

286 Described in the *Oxford Dictionary of Law* (ed. Jonathan Law, 7th ed., Oxford, 2009, p.204) as, "*that part of English law originally administered by the Lord Chancellor and later by the Court of Chancery, as distinct from that administered by the courts of common law. The common law did not recognise certain concepts and its remedies were limited in scope and flexibility, since it relied primarily on the remedy of damages.*"

actions and those of third parties are most likely to arise in the areas of copyright, defamation and privacy law.

The nature of **copyright** property makes an injunction a suitable remedy where an infringement is proven to have taken place. Since the introduction injunctions against ISPs under section 97A of the Copyright, Designs and Patent Act 1988 however,[287] an **injunction specific to ISPs** has been available, and the wider provisions of the Act providing for injunctive relief are less likely to be used in cases relevant to internet intermediaries. Further specific remedies (known as 'technical measures') will now be available as against ISPs for the purpose of reducing or preventing infringement of copyright on the internet.[288] There are **no other known remedies available under general provisions** applying to copyright law.

Under English law, **protection against defamation** derives from common law,[289] and one of the long-established available remedies is a **permanent injunction** against a defendant to prevent further publication of the defamatory material. Section 10 of the Defamation Act 2013[290] effected a radical change to the orthodox principles of English defamation law by removing the jurisdiction of courts in England and Wales to determine defamation actions against *secondary publishers* of defamatory material (namely, those who are not the author, editor or publisher). It is specifically defined in the Defamation Act 1996 that a person shall not be considered to be an author editor or publisher of a statement if he is only involved, "*in processing, making copies of, distributing or selling any electronic medium in or on which the statement is recorded, or in operating or providing any equipment, system or service by means of which the statement is retrieved, copied, distributed or made available in electronic form"*[291] or is involved only, "*as the operator of or provider of access to a communications system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control.*"[292] The first category will apply, most obviously, to internet intermediaries such as ISPs and internet content hosts; the second will potentially apply to mere conduit ISPs.

A number of cases[293] had previously confirmed the possibility of hosted material being considered as published by the host after the time at which the material has been brought to its attention.

In the 1999 case of ***Godfrey v Demon***,[294] the High Court examined whether a defendant ISP could avail itself of a defence contained in the Defamation Act 1996 (based on similar principles to that contained in the subsequent E-Commerce Regulations, exempting ISPs from liability where they do not know what material contained upon websites within their territory). Defamatory comments about Dr Godfrey had been posted on a website which was hosted by Demon Internet. Dr Godfrey reported these comments to Demon Internet and asked that they be removed. Some weeks later, the comments were still available to read online and so Dr Godfrey brought legal proceedings against Demon Internet. Demon Internet argued that they only had a purely passive role in the publication of the comments. This was rejected by the court, which stated that they held a similar position to that of a library or bookshop, and once they had been advised of the defamatory material, they had a choice to either

---

287 See sections 1.2. and 2.2.1. of section D, above.

288 See section 2.2.1. of section D, above.

289 Through case law such as *Parmiter v Coupland* (184) 6 Meeson & Welsby's Exchequer Reports 105, *Youssoupoff v MGM Studios* (1934) 50 Times Law Reports 581 and *Hebditch v McIlwaine* [1894] 2 Queen's Bench 58.

290 Defamation Act 2013, section 10.

291 Defamation Act 1996, section 1(3)(c).

292 Defamation Act 1996, section 1(3)(e).

293 *Godfrey v Demon* [1999] Entertainment and Media Law Reports 542, *Totalise v Motley Fool* [2002] Entertainment and Media Law Reports 20.

294 *Ibid.*

retain the information or remove it and were **a publisher at common law**. As they knew about the defamatory comments here, they could not rely on the defence that they only had a passive role.

Contrasting this case with **passive internet conduits**, in the 2006 case of ***Bunt v Tilley***,[295] the Judge held that the passive role of affording a connection to the internet did not render the provider a publisher at common law of a statement transmitted across the connection. In order to impose legal responsibility upon anyone under the common law for the publication of the words, it was essential to demonstrate that they had a degree of awareness that such words existed, or at least an assumption of general responsibility. The judge stated that in relation to pure conduits, the practical threshold is likely to be knowledge of the actual postings. When dealing with ISPs who host information, knowledge of "the process of publication" is more likely to be sufficient. Therefore, the ISPs in *Bunt* (who were accused only of providing connections to the internet) could not be held accountable as they had no knowledge of the actual postings on which the claimant was basing his case. This is in contrast to the position of Demon Internet in *Godfrey*, for whom knowing involvement in the hosting of the discussion group was sufficient to found participation in the publication.

More recently, in ***Tamiz v Google Inc***,[296] the Court of Appeal considered whether Google, which hosted a blog, could be liable for defamatory postings. In this case, Tamiz was aggrieved by allegedly **defamatory postings featured on the blog** hosted by Google. He put Google on notice of the offending postings. The postings were ultimately removed voluntarily by the blogger, but Tamiz sued Google in respect of the damage done before the removal of the postings. The principal Court of Appeal judge held that Google was not a primary publisher of the blog and was, "*not in a position comparable to that of the author or editor of a defamatory article*," or, "*the corporate proprietor of a newspaper in which a defamatory article is printed.*"[297] The judges did however disagree with the findings of the judge who heard the case in the first instance and who compared a blogger with being no more responsible than the owner of a wall on which graffiti has been daubed. He held that the position was different in relation to the period after Google had been put on notice of Tamiz's complaint. After Google had had, "*a reasonable time within which to act to remove the defamatory comments*,"[298] it could be, "*inferred to have associated itself with, or to have made itself responsible for, the continued presence of that material on the blog and thereby to have become a publisher of the material.*"[299]

However, in light of those conclusions, it follows that, in respect of causes of action accruing after the commencement of section 10 of the Defamation Act 2013 on 1st January 2014, courts no longer have jurisdiction to hear and determine defamation actions brought against defendants in the position of Google on the facts in *Tamiz v Google Inc*.[300]

Notwithstanding that most online intermediaries will now usually be classified as secondary publishers and no longer exposed to the possibility of being sued for defamation, those which engage in conduct going beyond that set out above (i.e., processing, making copies of, distributing or selling any electronic medium in or on which the statement is recorded), might be treated as 'editors' or 'publishers' of

---

295 *Bunt v Tilley* [2006] England and Wales High Court 407 (Queen's Bench Division).

296 *Tamiz v Google Inc* [2013] England and Wales Court of Appeal Civil Division 68.

297 *Ibid,* para 25.

298 *Ibid*, para 35.

299 *Ibid,* para 34.

300 Except where, as stated by section 10(1), it is not reasonably practicable for an action to be brought against the author of the hosted material. Where it is indeed not reasonably practicable, and an action can be brought against the internet intermediary, it will then be necessary to consider whether the intermediary has a defence, such as the defence for operators of websites in section 5 of the Defamation Act 2013, the defence of innocent dissemination in section 1 of the Defamation Act 1996 or the defences for internet intermediaries in regulations 17-19 of the E-Commerce Regulations.

statements, particularly where it is said that those statements are capable of being retrieved, copied, distributed, or made available via their equipment, systems or services.[301] **Certain intermediaries are still therefore exposed to the possibility of being ordered to take down defamatory material** by way of a permanent injunction granted to a successful claimant in legal proceedings.[302]

Permanent injunctions cannot be granted against those who are not a party to the defamation action. However, successful claimants may, in respect of causes of action accruing after the commencement of section 13 of the Defamation Act 2013 on 1 January 2014, now apply for an order compelling not just, as discussed in section 2.2.1. above, the operator of a website on which a defamatory statement is posted, but also *any person who was not the author, editor or publisher of the defamatory statement*, to stop distributing, selling or exhibiting material contained in the statement (an "Order to remove or cease distribution"). This latter category of **'secondary publishers' may potentially include a broader range of online intermediaries beyond website operators**, and the application of such an order is not dependent on such other person being a party to the original defamation action. No known specific case law is yet available on this point.

Finally, two other kinds of injunction have the potential to require that an ISP take down certain internet content, particularly in the field of privacy law.

The first, granted only on very rare occasions, is known as a '***contra mundum* injunction'**, being an injunction against the world at large, and not merely against the defendants to the proceedings. A famous example is the 2001 case[303] of claimants, Robert Thompson and Jon Venables, convicted, at the age of 11 years old, of killing the toddler, James Bulger. They were granted an injunction restraining the publication of information that would reveal their identity or whereabouts on their release from prison at the age of 18. The injunction, deemed necessary to protect the claimants' right to life and freedom from persecution was issued not just against the newspaper defendants, but against the world at large. There was a clear possibility that an ISP could be in breach of this order if a third party posted material to its servers, even though the ISP did not know it was there. As a result, the order issued was varied by the insertion of a proviso, clarifying that an ISP (and its employees) would not be in breach of the injunction unless:

> "*i. it knew that material had been placed on its servers or could be accessed via its service; or*
>
> *ii. knew that the material was likely to be placed on its servers, or was likely to be accessed via its service; and in either case*
>
> *iii. failed to take all reasonable steps to prevent the publication.*"

This wording was subsequently used on another occasion by the High Court ti protect the new name and whereabouts of Maxine Carr, the former girlfriend of another child killer, on her release from custody in 2004.

---

301 An intermediary that, for example, had in place systems for monitoring, moderating or censoring the content of material hosted on its servers might, depending on the circumstances, have assumed editorial or equivalent responsibility for the content of particular statements or the decision to publish them (see M.Collins, *Collins on Defamation*, *op. cit.*, p. 37.

302 Although it is still too early to tell whether the new prohibition on secondary publishers being responsible for defamatory material will mean it is much less likely that ISPs will be held liable for defamatory material (even where they have actual knowledge of the material itself), it should be noted that an ISP may still nevertheless be ordered to take down defamatory material by way of an Order to remove or cease distribution where a claimant successfully sues the actual author of the material for defamation.

303 *Venables v News Group Newspapers Ltd* [2001] 1 All England Law Reports 908.

The second kind of injunction which can result in an obligation on an ISP to remove material is a temporary remedy, known as an '**interim injunction**'. Although addressed to particular defendants, rather than being an injunction *contra mundo*, third parties, such as ISPs can be in contempt of court[304] if they aid and abet a defendant to breach that order. Under what is known as the *Spycatcher* principle, an interim injunction prevents a person from disclosing private and/or confidential information, but also prevents third parties from disclosing the information, provided they have been given notice of the injunction. The principle is based on the notion of maintaining privacy and preserving the status quo until the conclusion of full court proceedings (in the context of ISPs, most likely to be in cases of defamation and privacy) – often concerning the material in question. Although the *Spycatcher* principle arose in the context of newspapers who had full editorial control over the contents of their publications, claimants may seek to serve such an injunction not just on traditional ISP hosts and access providers, but also on a wide variety of online intermediaries, including search engines.[305]

2.3.2. Possibility to request compensation for damages

General principles of compensation for damages incurred by copyright infringement would apply generally to ISPs found to have breached copyright. According to tort law doctrine, such damages are restricted to those which flow directly and naturally from the tortious act. The normal measure of damage is the amount by the copyright is depreciated, by the infringement as a thing in action.[306]

Compensation is a principal remedy available to successful claimants in **defamation** cases. In the 1999 case of *Godfrey v Demon*,[307] the court decided at a preliminary hearing that the defendant ISP was liable for damages from the moment it had actual knowledge of the apparent defamation and failed to delete or disable the posting. The case later settled out of court for a reported £500,000.

2.3.3. Disclosure of Information

A number of cases have now demonstrated the common and successful use of *Norwich Pharmacal* orders[308] to compel ISPs to disclose information or other personal details of subscribers suspected of unlawful activity.[309]

2.4. Link between different provisions

The E-Commerce Regulations reflect the E-Commerce Directive in clarifying that the provisions (and immunities) contained within **do not affect the grant of injunctions**. Indeed, the Directive specifically permits national courts to require an intermediary to "terminate or prevent" an infringement. In this respect the obligations on ISPs contained in the domestic laws on **copyright law**, considered above, are, in theory, compatible with the E-Commerce Regulations, despite introducing new duties.

With regard to **defamation law** however, both the Regulations and the legislation supporting the common law provide for defences against liability in similar circumstances. The new defence available to a website operator under the Defamation Act 2013 indicates that the Government has expressly sought to protect website operators beyond that offered by the E-Commerce Regulations and is said by one author to, "plot a middle way between blanket immunity and the approach of the E-Commerce

---

304 'Contempt of court' in this context refers to disobedience of a court order or process.

305 See Graham J H Smith, *Internet Law and Regulation, op. cit.* , p. 392.

306 Lord Mackay of Clashfern (ed.), *Halsbury's Laws of England* 23, 5th Ed. Butterworths, 2013, para 966.

307 [1999] Entertainment and Media Law Reports 542.

308 See section 1.2. above.

309 See, for example, *Grant v Google* [2005] England and Wales High Court 3444 (Chancery Division), *Totalise v Motley Fool, op. cit., Golden Eye v Telefonica, op. cit.*

Directive".[310] The result is a number of different legal systems according to whether the ISP is a mere conduit, host or search engine.

Finally, specific provisions on court procedure, costs, remedies or court orders for information have mainly been avoided. Existing common law principles and civil procedure rules continue to apply.

3. Implementation

3.1. Overview

There no known procedural rules specific to the laws concerning the liability of intermediaries which apply to court proceedings.

Certain procedural rules will however apply to new provisions regulating online copyright infringement, according to the Initial Obligations Code, set to govern the functioning of those provisions, introduced by the Digital Economy Act 2010.

3.2. National Facts

Insofar as court proceedings are concerned, we are not aware of any special rules of procedure which apply in the context of ISP liability. Actions for injunctions and damages, whether as part of defamation, copyright or data protection proceedings, for example, are subject to the general Civil Procedure Rules 1998.[311]

It should also be noted that the proposed **Initial Obligations Code**[312] due to be introduced by OFCOM in accordance with the Digital Economy Act 2010 will apply to UK-based ISPs with over 400,000 customers and will provide for **detailed rules on challenging subscribers suspected of copyright infringement**. The procedures envisaged under the Code are intended to resolve online copyright disputes more swiftly than through the courts system; they are overseen by OFCOM, and are intended to be funded jointly by the ISPs and copyright owners. As indicated above (2.2.), the Initial Obligations Code seems to have been abandoned given the Memorandum of Understanding concluded in 2014 between ISP and the entertainment industry. According to the official press statement of several UK governmental institutions, this "new initiative follows a similar partnership between the movie and music industries and ISPs in the United States."[313]

3.3. International facts

Although there is some ambiguity, the definition and use of the territorially unlimited term « service provider » in the **E-Commerce Regulations** lead to the conclusion that the framers of the Regulations

---

310 Daithi Mac Sitigh, *The fragmentation of intermediary liability in the UK,* Journal of Intellectual Property Law & Practice 2013, Vol. 8, No. 7, 521-531 at 527.

311 Civil Procedure Rules 1998, available at http://www.legislation.gov.uk/uksi/1998/3132/article/2.1/made (29.01.2015).

312 Proposed Code available at: Ofcom, *Online Infringement of Copyright and the Digital Economy Act 2010,* Interim statement and notice of a proposal to make an order (June 2012), available at http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf (29.01.2015).

313 Press statement of 19.07.2014 the Department for Business, Innovation & Skills, the Intellectual Property Office, the Department for Culture, Media & Sport, The Rt Hon Dr Vince Cable and The Rt Hon Sajid Javid, available at https://www.gov.uk/government/news/new-education-programme-launched-to-combat-online-piracy (24.03.2015).

intended to include non-EEA service providers as being able to benefit from the protections contained within.[314]

We are not aware of other particular international civil procedure rules that are applicable in this context.

3.4. Propositions

While it seems that the iimplementation of the **Initial Obligations Code** has been abandoned given the Memorandum of Understanding reached in the entertainment industry,[315] there are no other known proposed developments.

---

314 See discussion in Graham J H Smith, *Internet Law and Regulation, op. cit.* , p. 369.

315 See 2.2.1. and 3.2. above.

E. DENMARK

1. Transposition of European Law

1.1. Overview

The transposition of relevant European Directives in to Danish law has either been carried out in the form of new Acts (Danish E- commerce Act and the Danish Act on Processing of Personal Data) or by amending existing laws (the Danish Copyright Act and the Danish Administration of Justice Act). Several provisions in the Directives, such as Article 8(3) of the InfoSoc Directive, did not necessitate any additional legislation since corresponding rights were already provided for under Danish law.

1.2. Transposition of European Directives

The Directive on Electronic Commerce[316] ("E-Commerce Directive") is transposed into the Danish legal system through the **Danish E-commerce Act**[317], which took effect in 2002. The Act, similar to the Directive, contains provisions regulating *inter alia* the liability of intermediary service providers businesses which offer "information society services".

The Danish E-commerce Act, Sections 14-16 is **a near verbatim transposition of Articles 12-15 of the E-Commerce Directive**. Those provisions lay down rules on exception as regards the liability of intermediary service providers and they do not regulate the service providers' responsibility. Instead, such liability are, in Denmark, governed by general tort- and criminal law.[318] The specific sections are related to different types of service providers in the same way as the E-Commerce Directive.[319] The provisions reflect the general rule that the less the information service provider is involved in the information made available, the less is the basis for holding it liable.[320]

The **Danish E-commerce Act section 14** regarding **mere conduit** exempts liability for service providers in so far as they only disseminate illegal content and in no way are involved with the information transmitted. However, section 14, first paragraph p. 2 must be construed so that the service provider can make manipulations of a technical nature which take place in the course of the transmission without being liable.[321]

In Danish doctrine it has been discussed whether liability can be exempted under section 14 even in cases where the service provider has specific knowledge that the transmission contains illegal information. Some legal scholars have referred to recital 44 of the E-Commerce which stipulates that: "*A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of "mere conduit" [...] and as a result cannot benefit from the liability exemptions established for these activities*" and argued that "deliberate

---

316 Directive 2000/31/EC of The European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

317 Lov 2002-04-22 nr. 227 om tjenester i informationssamfundet herunder visse aspekter af elektronisk handel.

318 S. Karstoft, Lov 2002-04-22 nr. 227 om tjenester i informationssamfundet herunder visse aspekter af elektronisk handel, commentary in Karnov, 2015, point 93.

319 The general scope of the Sections follows from the various definitions laid down in the Danish E-commerce Act, § 2, which corresponds to the definitions in the Directive on Electronic Commerce Art. 2.

320 Cf. the E-Commerce Directive, recitals 42-44.

321 Cf. the E-Commerce Directive, recital 43.

collaboration" entails more than (intentional) passivity from the service provider and, thus, that the liability exception in section 14 is absolute and not conditioned on the good faith of the service provider.[322]

Other scholars refer to Article 12 (3) of the E-Commerce Directive which stipulates that the Article shall not affect the possibility of a court or administrative authority of requiring the service provider to terminate or prevent an infringement. They argue that if the service provider's knowledge is specifically qualified, e.g., due to an injunction, it will be liable for the mere transmission of the information.[323]

According to **section 16 in the Danish E-commerce** regarding **hosting**, the rules on exemption of liability are more limited as regards hosting service providers compared to other service providers. To be exempted from liability, it is decisive that it is not the hosting service who chooses to make the information available. Section 16 point 1 makes a distinction between criminal liability, where actual knowledge is required, and civil liability for damages, which only requires awareness of facts or circumstances from which the illegal activity or information is apparent.

The hosting service has to act expeditiously to remove or disable access to the information from the moment he obtains knowledge or awareness. This means, that the obligation to act is connected to knowledge about the illegality of the stored information and, thus, goes further than the obligation to act under Section 14 and 15.

The E-Commerce Directive Art. 12 (3), Art. 13 (2), and Art. 14 (3) stipulate that the rules laid down in those articles shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, to require a service provider to terminate or prevent an infringement. Hence, the measures to terminate or prevent infringement already available under Danish law were not affected by the Directive and, consequently, the Directive did not lead to any amendments to the Danish law in that regard.[324]

It may also be mentioned that Danish law does not impose a general obligation on service providers to monitor the information which is transmitted or stored, nor a general obligation to actively investigate activities or circumstances that may be illegal. Neither is there an obligation for the service provider to report illegal activities. Thus, Danish law was found to be in accordance with Art. 15(1) in the E-Commerce Directive and the provision has therefore not resulted in any amendments of existing laws.

However, Danish law imposes an **obligation to report illegal activities in some specific cases**, e.g., if the service provider has knowledge of crime against national security or where there is a risk for someone's life.[325] These rules comply with Article 15 in the E-Commerce Directive, which entails a prohibition to impose a general obligation on service providers to monitor information.[326]

---

322 C.f. Plesner Mathiasen, J. & Jørgensen, N. B. & Schlüter, J., *E-handelsloven med kommentarer*, 1st ed., Copenhagen 2004, p. 200.

323 C.f. Nielsen, R., *E-handelsret*, 2nd ed., Copenhagen 2004, p. 272.

324 See the preparatory works to the Danish E-commerce Act, LFF 2002-01-29, no. 61, section C.12.2.2.

325 C.f. the Danish Penal Code, Lovbekendtgørelse 2014-07-04 nr. 871 Straffeloven, § 141.

326 C.f. the preparatory works to the Danish E-commerce Act, LFF 2002-01-29, no. 61, section C.12.2.3.

Article 8 of Directive 2004/48/EC ("**Enforcement Directive")**[327] regarding the right of information has been implemented in chapter 29a (sections 306–307) in the Danish Administration of Justice Act (*Retsplejeloven)*[328]. The "right of information" provided for in those provisions are a novelty in Danish law and, similar to the provisions in Chapter 57a of the same Act, apply only in cases of infringement of intellectual property rights.

Directive 2001/29/EC ("**InfoSoc Directive")**[329] was transposed into Danish Law by Act No. 1051 of December 17 2002, amending the Danish Copyright Act (*Ophavsretsloven)*. Fundamentally, Denmark considered the existing Danish Copyright Act to be already in accordance with the Directive. Thus, very few amendments were needed to ensure implementation. Article 8(3) of the InfoSoc Directive provides that the Member States shall ensure that right holders are in position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or a related right. An injunction in Danish law is conditional upon the fulfilment of the provisions in Chapter 40 of the Danish Administration of Justice Act. To our knowledge, Article 8(3) of the InfoSoc Directive did not necessitate any amendments in to the existing Danish law.

Directive 95/46/EC ("**Data Protection Directive")**[330] is primarily implemented in to Danish law by the Danish Act on Processing of Personal Data (*Lov om behandling af personoplysninger*).

1.3. Case-law

The rather limited Danish case law on service providers' responsibility primarily involves the Danish E-commerce Act section 14 and the **possibility to issue injunctions** against a service provider who is otherwise exempted from liability.

One of the most important cases is U.2010.2221H[331] where the Danish Supreme Court confirmed the lower court's injunctive order against the internet service provider ("ISP") Telenor requiring it to disable the access to the web-page www.thepiratebay.org, from which information protected by intellectual property rights was being transmitted.

In case U.2006.1474H[332] the ISP TDC was exempt from liability under the Danish E-commerce Act. As in case U.2010.2221H, the Supreme Court found that the liability exemption did not prevent issuing an injunction ordering the ISP to disable access to illegal information.

In case U.2013.2873Ø[333], the Eastern High Court held that an injunctive order should primarily be directed against the claimed initial infringer and not the ISP. According to the court, the ISP only transmitted the illegal information and it had no obligation or real possibility of obtaining knowledge to assess whether the transmitted information was legal. The court concluded that the injunctive order could be directed against the ISP directly only when the illegality was establish by the courts or the information was manifestly illegal. This was however not the case and the injunctive order was therefore not issued against the ISP.

---

327 DIRECTIVE 2004/48/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2004 on the enforcement of intellectual property rights.

328 Lovbekendtgørelse 2014-12-09 nr. 1308, Retsplejeloven.

329 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society .

330 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

331 Case H.K. 27. maj 2010 i sag 153/2009 (1. afd.).

332 H.K. 10. februar 2006 i sag 49/2005.

333 Ø.L.K. 3. juni 2013 i kære 6. afd. B-3295-12.

The recent case A-0038-14[334] concerned a blocking injunction of a website distributing illegal tangible goods (copyright protected Danish design furniture). In this case, the Danish Maritime and Commercial Court ordered a Danish ISP (Telia Danmark) to block access to the UK based online store Interior Addict. The judgment was based on both Article 8(3) of the InfoSoc Directive and Article 11 of the Enforcement Directive and relied on **copyright infringements** as the central issue. The blocking ruling was also based on the fact that a prior ruling had convicted the owners of the Interior Addict website of illegal distribution and marketing of replica products that infringe the copyrights of Danish right holders.

The cases referred to above show that, under Danish law**, ISPs who are exempt from liability** under the Danish E-commerce Act **nevertheless can be required to take down content they host or transmit by means of injunctive orders**.

1.4. Lacunae and difficulties

Under the notice and takedown-rule in the Danish E-commerce Act section 16 paragraph 1 point 2 (which corresponds to the Directive on Electronic Commerce Art. 14 (1), (b) it is unclear when the service provider has obtained such knowledge or awareness that the provider is obliged to remove or disable access to the information. Furthermore, it is unclear what time period the term “expeditiously” refers to.

It is a risk that service providers, to be sure not to be held liable, take down more information than might be required. This raises concern that the removal of information may have a negative impact on the freedom of speech. It is a matter that merits further examination.

2. National law

2.1. Overview

While there are no specific rules in Danish law on the responsibility of ISPs (2.2.), Denmark has applied general provisions (2.3.), especially relating to civil liability and on injunctions, and encouraged the development of codes of conduct and similar measures (2.4.).

2.2. Provisions specific for ISP

Denmark has not set out special regulations on the responsibility of ISPs apart from the aforementioned EU-related provisions.[335] Thus, the responsibility of the ISPs must be determined on the basis of general provisions.

2.3. Application of general provisions to ISP

2.3.1. Civil Liability

In Danish law, the general rules on **tort liability** are based on the so called *culpa rule* developed in case law. According to this rule liability is incurred for any loss, damage or injury caused by an intentional or negligent individual action or failure to act attributable to the tortfeasor. The assessment to be made here is whether the action deviates from generally accepted behaviour. Besides negligence and a suffered loss it is also a fundamental condition for imposing liability that there is causation between

---

334 Case A-38-14 of Sø- og Handelsretten i Kobenhavn 11 December 2014.

335 The Danish Media Liability Act, Lovbekendtgørelse 2014-08-11 nr. 914 Medieansvarsloven, has not been found to encompass service provider responsibility.

the tortfeasor's act/omission and the resulting damage.[336] In order to impose liability on an ISP, these general requirements for liability under Danish Law must be met.

Strict liability (i.e. liability regardless of negligence) can be imposed in certain limited cases, generally only according to statue but it has also been applied in non-statutory cases. However, none of the examples from case law where the Danish courts have imposed non-statutory strict liability can be applied to the ISP responsibility.

As the main purpose of the ISP is to provide technical assistance for the users, it will mainly be relevant to consider whether the ISP can be held **contributory liable** for illegal activities. General contributory civil liability derives from legal principles developed by case law, however, in some areas such as patent law it is specifically regulated.[337] Typically, contributory liability will be imposed on the basis of an active incitement or action that helps the tortfeasor.

As a general rule, liability cannot be imposed for omissions. However, this position can only be maintained in so far that there is no prior connection to the wrongful act.[338] In cases where there is a **duty to act**, the ISP can be held liable for omissions. To establish a duty to act usually requires a special connection to the tortfeasor, the harmful act or the aggrieved party. The ISP must have actual knowledge or awareness of facts or circumstances from which the activity or information as well as the illegality thereof is apparent. Finally, the ISP must have had opportunity to prevent the wrongful act before an obligation to act can be established.

2.3.2. Injunctions

The national rules allowing for injunctions of different kinds are primarily set forth in the **Danish Administration of Justice Act**[339]. Usually, illegal online activities are prevented by means of DNS- or IP-blockings, i.e., where the internet service access provider blocks the illegal online activity.[340] The Act enables courts to issue **injunctions against the ISP in order to terminate or prevent infringements** in such cases, even though the ISP is not the actual infringing party.[341] Hence, the injunction may be granted irrespective of the intermediary's liability or irrespective of the violation by the intermediary of any kind of duty (such as a general "duty of care").

For an interim injunction to be issued, it must be shown i) that the party seeking the injunction has the right, which is sought to be protected by the injunction, ii) that the conduct of the other party necessitates that an injunction is issued, and iii) that the opportunity of the party seeking the injunction to protect his right will be wasted if the party must await the decision in the underlying legal dispute.[342] Furthermore, if not already initiated, the **party seeking the injunction must initiate court proceedings against the alleged actual infringer** concerning the underlying legal dispute at least two weeks after the injunction has been issued.[343]

---

336 R. Nielsen et al., Kluwerlaw online Cyber Law National Monograph Denmark, 2013, p. 165.

337 Cf. section 3(2) in the Danish Patent Act (Lovbekendtgørelse 2012-01-24 nr. 108 Patentloven).

338 Eyben, B. v. & Isager, H., *Lærebog i erstatningsret*, 6st ed., Copenhagen 2009, p. 45 seq.

339 Lovbekendtgørelse 2014-12-09 nr. 1308, Retsplejeloven.

340 See the memorandum from the Danish Ministry of Business and Growth, Oversigt over juridiske og tekniske håndhævelsesmetoder I Denmark og EU (June 2012), available at http://www.ft.dk/samling/20111/almdel/eru/bilag/300/1138525.pdf (18.02.15), p. 8.

341 C.f. the Administration of Justice Act, Chapter 57 (Sections 641-652).

342 Cf. the Danish Administration of Justice Act, Section 413.

343 Cf. the Danish Administration of Justice Act, Section 425.

Thus, while the issue whether there has been an infringement of for example copyright law is determined in proceedings between the aggrieved party and the alleged infringer (not the ISP), injunctions have been issued against ISPs in accordance with the Danish Administration of Justice Act Chapter 40. The Enforcement Court may provide assistance at the request of the party who have obtained an injunction against the actual infringer to enforce the injunction by preventing an infringement of or by ensuring compliance with the injunction or by destroying what has been made in violation of the injunction.[344] Thus, if the actual infringer does not stop the illegal online activities an injunction ordering the webpage to be blocked is issued against the ISP.

A refusal to respect an injunction may be sanctioned by fines or imprisonment and the party may be ordered to pay damages.[345] Furthermore, moveable property can be seized if it is used, has been used or is likely to be used in violation of the injunction.[346] In the Danish cases where the courts have issued injunctions against ISPs requiring them to take down or block access to specific webpages, the ISPs have complied with the injunctions.[347] In order to facilitate and enhance the efficiency of injunction measures, the professional organization of the Telecom industry has recently adopted a Code of Conduct (see below section 2.4).

The decision on preliminary injunction shall be followed by a final judgment on the merits of the case wherein the **lawfulness of the preliminary injunction is assessed** and it is decided if the **injunction shall be made permanent**.[348]

As for obtainment of **evidence in relation to infringement of intellectual property rights**, the Enforcement Court can under certain circumstances order a search to preserve relevant evidence in respect of an alleged infringement of intellectual property rights. In so far as it is found necessary to preserve the relevant evidence, the object or documents can be seized and copies can be made of documents, information on computers, computer programs or other materials.[349]

Example of other measures which might be relevant in relation to the ISP is intervention in the protection of secrecy of communications and **seizure and disclosure of objects**.[350]

Furthermore, it may be mentioned that injunctions measures are **explicitly provided for in certain laws**, for example in the Danish Marketing Practice Act. It provides that actions in conflict with the Act may be prohibited by judgments and that, concurrently with this or subsequently, such orders may under certain circumstances be imposed by judgments (i.e. injunctions) as may be considered necessary to ensure compliance with the prohibition.[351]

---

344 Cf. the Danish Administration of Justice Act, Section 641 (1).

345 Cf. the Danish Administration of Justice Act, Section 430.

346 Cf. the Danish Administration of Justice Act, Section 641 (2).

347 Se the report from the Danish Ministry of Culture, Rapport fra møderækken om håndhævelse af ophavsretten på internettet (2009), p. 35, available at http://kum.dk/uploads/tx_templavoila/Rapport%20fra%20moderakken%20om%20handhavelse%20af%20ophavsretten%20pa%20internettet.pdf (19.02.15).

348 Cf. the Danish Administration of Justice Act, Section 426. See also R. Nielsen et al., Kluwerlaw online Cyber Law National Monograph Denmark, 2013, p. 172.

349 C.f. the Administration of Justice Act, Chapter 57 a (Sections 653-653 d).

350 See the Administration of Justice Act, Chapters 71 (Sections 780-791 a) and 74 (Sections 801-807 d).

351 See the Danish Marketing Pratice Act, Lovbekendtgørelse 2013-09-25 nr. 1216 om markedsføring, Section 20.

Finally, the Danish Act **relating to domain names**[352] provides for the possibility of third parties to lodge a complaint with the Complaints Board for Domain Names (*Klagenævn*). Also the general terms and conditions of DK Hostmaster, the corporation responsible for the distribution and registration under the .dk-domain provide for the possibility of a third party, especially a rights holder, to require the suspension or blocking and deletion of a domain name if it is identical with or contains the name or trademark rights or other distinctive feature of the party concerned.[353] The suspension can be decided if the domain name is identical to or contains the third party is name or trademark right, if it is used for a website or another service, if the domain name user has no right or faire reason to use the domain name in question and if the Complaints Board has hold on two previous occasions within the 5 previous years that the domain name holder (or a related person) has acted against good practice.

2.4. Codes of Conduct

Article 16 of the E-Commerce Directive encourages the creation of codes of conduct by trade, professional and consumer associations or organizations. For Denmark, the work related to the development of self-regulating instruments exists on several levels; national, Nordic and European. On a regional level, the Nordic countries have jointly set up a working group, which has *inter alia* examined how one can use self-regulation in order to create common rules for the e-commerce industry.[354] As regards the national level, the Danish legislator has in particular specified that guidelines concerning commercial communications and liability exemptions, e.g., regarding the application of a "notice-and-take-down-system" might be relevant.[355]

While there is no specific legislation on when/under what conditions access providers can be asked to block or take down content in Denmark, a **set of voluntary agreements** already exist on this matter. In September 2014, Teleindustrien (TI), which is the professional organization for the Danish telecom industry, entered into a voluntary agreement regarding blocking and take down of internet content in relation to infringements of intellextual property rights etc.[356] The Code of Conduct was established in order to simplify and make more efficient the implementation of decisions on blocking of websites. The agreement ensures that court decisions on blocking of a website against one TI-member must be complied with by the other TI members within 7 days. Moreover, if a blocked website appears on a new domain with the same content, the ISPs will, upon request from the right-holder(s), block that domain without a court order. The advantage for the parties to the Code of Conduct is thus that it limits the number of court proceedings considering that the rights holders (for example to copyright protected material) do not need to bring proceedings against all ISPs separately. The Code of Conduct does not prevent TI-members from reserving the right to try the case independently, if it is necessary with regards to the specific circumstances, and TI cannot be held liable for the member's non-compliance with the agreement.

The Danish Ministry of Culture has recently (8 May 2015) presented a **Memorandum of Understanding concerning a new Code of Conduct;** "Code of Conduct to promote lawful behavior on the internet".[357] The participants to the agreement are inter alia the Ministry of Culture, the Rights Alliance and other

---

352 Lov 2014-02-26 nr. 164 om internetdomæner.

353 According to Section 8.3.4. of the General Terms and Conditions, available at https://www.dk-hostmaster.dk/fileadmin/filer/pdf/generelle_vilkaar/generelle_vilkaar_DK06.pdf (12.02.2015)

354 See the preparatory works to the Danish E-commerce Act, LFF 2002-01-29, no. 61, section 13.

355 See the preparatory works to the Danish E-commerce Act, LFF 2002-01-29, no. 61, section 13.

356 A list of the TI-members is available at; http://www.teleindu.dk/om-ti/medlemmer-af-ti/ (12.02.15). The Code of Conduct is available in Danish at http://www.teleindu.dk/wp-content/uploads/2014/10/TI-code-of-conduct-blokeringer.pdf (24.07.2015).

357 http://kum.dk/nyheder-og-presse/pressemeddelelser/nyheder/bred-opbakning-til-faelles-kamp-for-et-lovligt-og-trygt-internet-paa-ophavsretsomraadet/1/1/ (23.07.2015).

rights holders, ISPs, payment processors (Diners, MasterCard and Nets), advertising companies, web hosting companies, domain registrars, Google and Microsoft. The new agreement builds on the earlier more limited Code of Conduct from 2014 described above. Under the new Code of Conduct, it appears as if an injunction against a specific ISP to block a specific domain name could be **extended with voluntary blocking in other areas than Internet access services**, for example in the area of advertising networks and payment processors.[358] Further, the ISPs will continue their current practice of voluntary blocking once an injunction has been issued against a single ISP. The blocked websites will display a notice which encourages the consumer to search for legal alternative at a website called Share With Care (www.sharewithcare.dk).[359]

3. Implementation

Soweit ersichtlich bestehen im dänischen Recht keine Sonderbestimmungen zur national oder internationalzivilprozessrechtlichen Durchsetzung von Ansprüchen gegenüber ISP.

358 https://edri.org/danish-culture-ministry-danes-regulated-by-google/ (23.07.15).

359 https://edri.org/danish-culture-ministry-danes-regulated-by-google/ (23.07.15).

F. USA

1. Substantive Law

1.1. Overview

A complete and detailed analysis of ISP liability in US law is beyond the scope of this opinion however we will address certain issues relating to liability under the laws of copyright and trademark (in particular as applied to search engines and auction sites), and tort (in particular, defamation and libel). There are no criminal provisions that are particularly aimed at ISPs. Moreover, the safe-harbor rules for ISPs specifically except out criminal liability.[360] This opinion, therefore, will not address issues of criminal law, in particular, computer fraud or hacking.[361]

Notably with respect to copyright and trademark liability, one must distinguish between primary liability, *i.e*. where the ISP has directly engaged in infringing behavior, and **secondary liability**, *i.e*. where the ISP is held liable for the acts of third parties (usually, users) under theories of **contributory liability, vicarious liability or inducement**. It is generally the second type of liability for which U.S. legislative provisions provide certain safe harbors for ISPs.

As a general matter, all three of these theories[362] may be used to hold an ISP liable for acts other than those that directly constitute the violation of another party's rights. In the intellectual property context, under the concept of "**contributory infringement**," a party may be guilty of infringement when it **causes or contributes to the infringing conduct of another with knowledge** of the other party's infringing activities.[363] If the person has the **right and ability to control an infringer's acts and receives a direct financial benefit**, there may be vicarious liability.[364] **Actual knowledge** of the infringer's activity is **not required** for such liability to apply. **Inducement** refers to liability for **acts of the ISP which tend to induce a third party to violate the rights of others.**[365]

---

360 See discussion under 1.2.2, *infra.*

361 See, *e.g.* the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, an amendment made in 1986 to the Counterfeit Access Device and Abuse Act that essentially states that intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining information from any protected computer if the conduct involved an interstate or foreign communication is a punishable act. While the CFAA is primarily a criminal law intended to reduce the instances of malicious interferences with computer systems and to address federal computer offenses, an amendment in 1994 allows civil actions to brought under the statute, as well, See, also, the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510 *et seq*.; and the Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq*.

362 *I.e.* contributory liability, vicarious liability and inducement).

363 *Religious Technology Center v. Netcom*, 907 F. Supp. 1361 (N.D.Cal 1995).

364 *Sony Corp. of America v. Universal City Studios, Inc.,* 464 U.S. 417, 104 S.Ct. 774, (1984) citing the so-called "dance hall cases," F*amous Music Corp. v. Bay State Harness Horse Racing and Breeding Ass'n*, 554 F.2d 1213 (CA1 1977) (racetrack retained infringer to supply music to paying customers); *KECA MUSIC, Inc. v. Dingus McGee's Co.,* 432 F.Supp. 72 (W.D.Mo.1977) (cocktail lounge hired musicians to supply music to paying customers); *Dreamland Ball Room v. Shapiro, Bernstein & Co.*, 36 F.2d 354 (Ct.App. 7th Cir. 1929) (dance hall hired orchestra to supply music to paying customers). These cases are often contrasted with the so-called landlord-tenant cases, in which landlords who leased premises to a direct infringer for a fixed rental and did not participate directly in any infringing activity were found not to be liable for contributory infringement. E.g., *Deutsch v. Arnold*, 98 F.2d 686 (Ct.App. 2nd Cir. 1938).

365 "One infringes contributorily by intentionally inducing or encouraging direct infringement, see *Gershwin Pub. Corp. v. Columbia Artists Management, Inc.*, 443 F.2d 1159, 1162 (Ct.App. 2nd Cir 1971), and infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it, *Shapiro, Bernstein & Co. v. H.L. Green Co.*, 316 F.2d 304, 307 (Ct.App. 2nd Cir 1963). Although

Several specific legislative provisions have, however, been adopted in order to limit the potential liability of ISPs, the most important of which are **Section 230 of the Communications Decency Act of 1996**[366] and the Online Copyright Infringement Liability Limitation Act[367], inserted as **Section 512 of the Digital Millennium Copyright Act of 1998**[368] (DMCA).

1.2. Specific Provisions for ISPs

1.2.1. Section 230 of the Communications Decency Act of 1996[369]

In order to understand the importance of this legislation, it is important to understand the state of the law which preceded its adoption. What follows is a brief description of the major cases that defined the law in this area until 1996.

In the landmark internet case, *Cubby, Inc. v. CompuServe Inc.*[370], internet service provider Compuserve was absolved from liability for content hosted on its servers. Compuserve made available to some of its users a daily newsletter called "Rumorville". The company Cubby, Inc. developed a competing news source called "Skuttlebut." Cubby sued CompuServe itself, in addition to the authors, alleging CompuServe was liable for the statements of its authors.[371]

Under the **common law of defamation**, if Compuserve were considered a publisher, it could be held liable for the statements appearing in Rumorville. Conversely, if it were found to be merely a "distributor," it could not be held liable unless it knew or had reason to know about the allegedly defamatory statements. The Southern District of New York dismissed all claims against CompuServe, ruling that CompuServe **should not be deemed a publisher, but only a distributor** who had no first-hand knowledge of the contents of the publication and therefore, **no liability** could be imposed. Compuserve, the court found, had **no knowledge and wielded no control** over Rumorville's publications, nor did it have the "**opportunity to review** Rumorville's contents before being uploaded onto CompuServe's computer banks, from which it is immediately available to approved [CompuServe] subscribers."[372]

Several years later, in *Stratton Oakmont v. Prodigy Services*[373] the court held that Prodigy, another online service provider, **was responsible** for user-uploaded content **because it exercised more editorial control** over its articles than did CompuServe. In that case, an unknown user posted statements on Prodigy's "Money Talk" bulletin board indicating that Stratton Oakmont, Inc., a Long Island securities brokerage firm, and its president, Daniel Porush, had committed criminal and

---

'[t]he Copyright Act does not expressly render anyone liable for infringement committed by another, '*Sony Corp. v. Universal City Studios*, 464 U.S., at 434, 104 S.Ct. 774, these doctrines of secondary liability emerged from common law principles and are well established in the law, *id.*, at 486, 104 S.Ct. 774 (Blackmun, J., dissenting); *Kalem Co. v. Harper Brothers*, 222 U.S. 55, 62–63, 32 S.Ct. 20, 56 L.Ed. 92 (1911); Gershwin Pub. Corp. v. Columbia Artists Management, supra, at 1162; 3 M. Nimmer & D. Nimmer, Copyright § 12.04[A] (2005)." *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.,* 545 U.S. 913, 930-31, 125 S.Ct. 2764, 2776 (2005).

366 47 U.S. Code §§ 230 *et seq*.

367 17 U.S. Code § 512.

368 17 U.S. Code §§ 501 *et seq*.

369 47 U.S. Code §§ 230 *et seq*. The provisions of this law are often referred to simply as "Section 230".

370 776 F. Supp. 135 (S.D.N.Y. 1991).

371 Digital Media Law Project available at: http://www.dmlp.org/threats/stratton-oakmont-v-prodigy (Apr. 16, 2015)

372 *Id.*

373 1995 WL 323710 (N.Y. Sup. Ct. 1995).

fraudulent acts in connection with the initial public offering of Solomon-Page, Ltd. As a result, Stratton and Porush sued Prodigy and anonymous defendants in New York state court for defamation. "Money Talk" was, at the time, a widely read forum covering stocks, investments, and other business matters. Prodigy contracted with Charles Epstein to act as "Board Leader," a position entailing, in part, participation in board discussions, board promotional efforts, and board supervision. In its argument that Prodigy was a publisher of the defamatory statements, the plaintiffs pointed to representations Prodigy had made in various newspaper articles representing itself as an organization that exercised editorial control over the content on its servers.

In making their case, the plaintiffs also pointed to Prodigy's "content guidelines," which stated rules that users were expected to abide by, a software screening program which filtered out offensive language, and the employment of moderators or "Board Leaders" who were responsible for enforcing the content guidelines.

This was the state of the law until 1996.

Although initially enacted to regulate (and restrict) speech on the Internet[374], the Communications Decency Act of 1996 ("CDA") contains provisions that specifically protect ISPs from potential liability. Much of the CDA was subsequently struck down by the U.S. Supreme Court as unconstitutional, however, Section 230(c) which provides as follows, remains. "**No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider**."[375] In passing the CDA the House of Representatives explicitly stated its intent to overturn the result reached in the Prodigy case.[376] As a result, online intermediaries – which include not only ISPs but also a range of "interactive computer service providers," including bloggers (even in some cases where they edit content appearing on their blog)[377] - that host or republish speech are protected against numerous laws[378] that might otherwise be used to hold them liable for content posted by others. It does not, however, cover liability for violation of federal criminal law (although it does cover some state criminal law and civil law claims based on federal criminal statutes), intellectual property law, and electronic communications privacy law.[379] [380]

---

374 See the website of the Electronic Frontier Foundation article on Section 230 available at: https://www.eff.org/fr/issues/cda230 (Apr. 13, 2015)

375 47 U.S.C. § 230(c) available at: https://www.law.cornell.edu/uscode/text/47/230 (Apr. 13, 2015).

376 See H.R. Conf. Rep. 104-458, at 194. See also, *Zeran v. America Online,* 129 F.2d 327 (U.S Court of Appeals, 4th Circuit, 1997 (negligence action against commercial interactive computer service provider alleging that provider unreasonably delayed in removing defamatory messages posted by unidentified third party, refused to post retractions of those messages, and failed to screen for similar postings thereafter barred by CDA).

377 See: https://www.eff.org/issues/bloggers/legal/liability/230 (Apr. 13, 2015).

378 These may include claims of **negligent misrepresentation**, **interference with business expectancy**, **breach of contract**, **intentional nuisance**, **violations of federal civil rights**, and **emotional distress**. The protection has also been acknowledged against a state cause of action for violating a statute that forbids dealers in autographed sports items from misrepresenting those items as authentically autographed, as well as unfair competition laws. In addition, it has protected a library from being held liable for misuse of public funds, nuisance, and premises liability for providing computers allowing access to pornography. See https://www.eff.org/issues/bloggers/legal/liability/230 (Apr. 13, 2015).

379 *Id.*

380 For a more extensive discussion of some of the major cases interpreting Section 230, see Electronic Frontier Foundation website at: https://ilt.eff.org/index.php/Defamation:_CDA_Cases (Apr. 13, 2015).

It should also be noted that there is considerable case law concerning the line between internet service providers (who are protected) and internet content providers (who are not).[381] *Carafano v. Metrosplash*[382] is one such case. Matchmaker.com was a commercial Internet dating service where individuals, for a fee, could post anonymous profiles and view profiles of other members in the area, with the ability to contact such members via email sent through the website server. There was also a questionnaire section with multiple choice and essay answers where members could provide additional detail; some answers were innocuous while others were sexually suggestive. Matchmaker reviewed photos for impropriety before posting but did not review the profiles themselves, relying instead on participants to adhere to service guidelines. Such guidelines prohibited members from posting last names, addresses, phone numbers or email addresses within a profile.

On October 23, 1999, an unknown person posted a "trial" profile of Plaintiff Carafano, an actress, without her permission or knowledge, in the Los Angeles section of the site. This profile included sexually related commentary and contained photos of the actress and listed her movies. It also provided a fictional email address for contact, and upon sending an email to this address, the sender would receive an automatic response stating "You think you are the right one? Prove it!!", and provided Plaintiff's home address and telephone number. As a result of the profile, Plaintiff received numerous threats and sexually explicit messages via email and voicemail. After contacting the website and having the profile removed, Carafano filed suit against Metrosplash in California, alleging **invasion of privacy, misappropriation of the right of publicity, defamation, and negligence.** The Court of Appeals held that (1) the fact that **provider's questionnaire facilitated expression of information by individual users did not make provider an "information content provider"** within the meaning of the CDA, and thus provider was entitled to statutory immunity from liability in tort, and (2) **even if provider could be considered an "information content provider," it was still entitled to statutory immunity**. An "'interactive computer service" qualifies for immunity so long as it does not also function as an "information content provider" for the portion of the statement or publication claimed to be false, misleading or defamatory. "Accordingly, courts have interpreted Section 230 protection to be 'quite robust, adopting a relatively expansive definition of 'interactive computer service[.]'"[383]

---

381 See, *e.g., Carafano v. Metropsplash*, 339 F.3d 1119 (online matchmaking service is an interactive computer service (ICS)); *PatentWizard, Inc. v. Kinko's, Inc*., 163 F. Supp. 2d 1069, 1071 (Dist. S. Dakota. 2001) (photocopy shop not contested as ICS provider under § 230); *Schneider v. Amazon.com, Inc*., 31 P.3d 37, 39 (Wash. Ct. App. 2001) (online bookseller providing forum for others to submit book reviews is an ICS provider); *Marczeski v. Law*, 122 F. Supp. 2d 315, 327 (D. Conn. 2000) (organizer of chat room for discussion of dispute about plaintiff held to be ICS provider); *Batzel v. Smith,* 333 F.3d 1018, 1031, Ct.App.9th Cir. (Cal.)2003 (website and listserv operator held to be interactive computer services provider and user, not content provider); *Smith v. Intercosmos Media Group, Inc*., 2002 WL 31844907 (E.D.La. 2002) (domain name registrar is an ICS provider). *Parker v. Google, Inc*., 422 F. Supp. 2d 492 (E.D.Pa. 2006), *affirmed* 242 Fed. Appx. 833 (3rd Cir. 2007)(unpublished) (search engine Google immune for archiving of, caching of, or providing access to allegedly defamatory, unauthorized, or threatening usenet postings); *DiMeo v. Max*, 433 F. Supp. 2d 523 (E.Dist. Pa. May 26, 2006) (online message board is covered by section 230 despite editorial review by message board operator), *affirmed* 248 Fed. Appx. 280 (3rd Cir. 2007)(unpublished); *Prickett v. infoUSA, Inc*., 561 F. Supp. 2d 646 (E.Dist. Tex. 2006) (database publisher retains section 230 immunity for content furnished to it by third parties even if the database publisher later licenses the database content to third parties); *D'Alonzo v. Truscello*, 2006 WL 1768091 (Court of Common Pleas Pa. 2006)(unpublished)(website was "interactive computer service," and not "internet content provider," within meaning section 230 immunity provision); *Delfino v. Agilent Technologies, Inc*., 52 Cal. Rptr. 3d 376, 145 Cal. App. 4th 790 (Cal. App. Ct. 6th Dist. 2006) (employer that provided its employees with Internet access through employer's internal computer system was "provider or user of an interactive computer service" within meaning of section 230 immunity provision). https://ilt.eff.org/index.php/Defamation:_CDA_Cases (Apr. 13, 2015).

382 339 F.3d 1119 (2003).

383 339 F. 3d at 1123.

1.2.2. Online Copyright Infringement Liability Limitation Act: Section 512 of the Digital Millennium Copyright Act[384]

The Online Copyright Infringement Liability Limitation Act was adopted as Title II (§§ 201-203) of the DMCA (Public Law 105-304), and was codified at 17 U.S.C. § 512. For this reason, this opinion will refer to this law as "section 512."

Section 512 of the DMCA provides certain specific **limitations on liability for copyright infringement by online service providers**. The limitations are in connection with 4 categories of conduct:

1. Transitory communications;
2. System caching;
3. Storage of information on systems or networks at the direction of users; and
4. Information location tools.[385]

These limitations constitute **complete bars to monetary damages** and, in many situations, **restrict the availability of injunctive relief.**[386] The determination of whether a provider qualifies for any of the limitations is made for each such limitation: eligibility for one has no bearing on the eligibility for any other.

With respect to the first category, a "service provider" is defined as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."[387] For the other three limitations, the definition of a "service provider" is broader: "a provider of online services or network access, or the operator of facilities therefor."

Even in the absence of a limitation, the provider will only be liable for copyright infringement if the owner can demonstrate the infringement and if none of the defenses, such as fair use[388], are available.[389]

In addition, in order to be eligible for any of these limitations on liability, a **service provider must "(1) adopt and reasonably implement a policy of terminating in appropriate circumstances the accounts of subscribers who are repeat infringers; and (2) it must accommodate and not interfere with 'standard technical measures.'"**[390] "Standard technical measures" are defined as "**measures that copyright owners use to identify or protect copyrighted works, that have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair and voluntary multi-industry process, are available to anyone on reasonable non-discriminatory terms, and do not impose substantial costs or burdens on service providers.**"[391]

---

384 In US law, when a summary of legislation is published by the government authority charged with enforcement and/or interpretation of the law in a specific area, such a summary has particular weight in the eyes of a court. As a result, since the U.S. Copyright Office has published an official summary of the DMCA, this opinion is based primarily on that publication.

385 The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary, December 1998, p. 8, available at: http://www.copyright.gov/legislation/dmca.pdf (Mar. 31, 2015).

386 17 U.S.C. § 512(j).

387 17 U.S.C. § 512(k)(1)(A).

388 See discussion of "fair use" under section 3.4, *infra.*

389 17 U.S.C. § 512(l).

390 The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary, *op.cit.*, p. 9).

391 *Id.* at 9-10, available at: http://www.copyright.gov/legislation/dmca.pdf (Mar. 31, 2015).

1.2.2.1. Limitations for Transitory Communications

Where a provider acts **only as a data conduit**, transmitting digital information from one point on a network to another at the request of a third party, under Section 512(a), **ISPs will not be liable** for acts of **transmission, routing, or providing connections for the information, or for the intermediate and transient copies that are made automatically in the operation of a network**. [392]

This limitation is subject to the following conditions:

- "The transmission must be **initiated by a person other than the provider**.
- The transmission, routing, provision of connections, or copying **must be carried out by an automatic technical process without selection of material by the service provider**.
- The service **provider must not determine the recipients** of the material.
- Any intermediate copies must not ordinarily be accessible to anyone other than anticipated recipients, and must not be retained for longer than reasonably necessary.
- The material must be **transmitted with no modification to its content**."[393]

1.2.2.2. Limitations for System Caching

Section 512(b) limits ISP liability for the practice of retaining copies, for a limited time, of material that has been posted online by a third party, and then transmitted to a subscriber at his or her request. The ISP in these cases retains the material in order that they may respond to any subsequent requests for the same material by transmitting the saved copy rather than retrieving the material from the original source on the network a second time, thereby reducing the ISP's bandwidth requirements as well as the waiting time necessary to obtain the information. The limitation applies only to **acts of intermediate and temporary storage, when achieved through an automatic technical process in order to make the material available to subscribers if subsequently requested**. [394] The following conditions apply:

- "The **content** of the retained material **must not be modified**.
- The provider must **comply with any rules concerning "refreshing" material** – replacing retained copies with material from the original location – established in accordance with a **generally accepted industry standard data communication protocol**.
- The provider **must not interfere with technology that returns information concerning "hits"** to the person who posted the material where such technology meets certain requirements.
- The provider must **limit users' access to the material in accordance with conditions on access, such as password protection, imposed by the person posting the material**.
- Any **material posted without the copyrights owner's authorization must be removed or blocked promptly once the service provider has received notification that it has been removed, blocked, or ordered to be removed or blocked, at the originating site**." [395]

1.2.2.3. Limitation Regarding Information Residing on Systems or Networks at the Direction of Users

Pursuant to § 512(c), ISP liability is limited for infringing material on websites (or other repositories) hosted or stored on their systems at the direction of a user. The limitation is subject to the following conditions:

---

392 *Id.* at 10.

393 *Id.*

394 *Id.*

395 *Id.* at 11.

- "The provider **must have filed with the Copyright Office, a designation of an agent to receive notifications of claims of infringement**.[396]
- The provider **must not have actual knowledge of the infringement, be aware of facts or circumstances from which infringing activity is apparent, or upon gaining such knowledge or awareness, or fail to respond expeditiously to take the material down or block access to it.**
- If the provider has the right and ability to control the infringing activity, it must **receive no financial benefit directly attributable to the infringing activity**.
- Upon receiving proper notification of claimed infringement, the provider must **expeditiously take down or block access to the material**."[397]

Notification here refers to a written and signed notification of the designated agent of a service provider identifying a copyrighted work that has allegedly been infringed, the allegedly infringing material (providing sufficient information to allow the ISP to find it), contact information of the complainant, and an affirmation of the complainant that s/he has a good faith belief that the use of the material is unauthorized, the notification is accurate and the complaining party is authorized to act on behalf of the owner of the exclusive right being infringed. [398]

---

396 The Copyright Office provides a suggested form for Interim Designation of Agent to Receive Notification of Claimed Infringement (available at: http://copyright.gov/onlinesp/agent.pdf (Apr. 2, 2015)) or Amended Interim Designation of Agent to Receive Notification of Claimed Infringement (available at: http://copyright.gov/mwg-internal/de5fs23hu73ds/progress?id=cc18xMLY19jA92q824AI2SUZ6gTUK3ke-vm2d09p1ek, (Apr. 2, 2015)).

397 The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary, *op.cit at*. 11-12.

398 See §512(c)(3) which provides:
(3) Elements of notification.—
(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:
(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
(B)
(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.
(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to

If, upon receiving a proper notification, the service provider promptly removes or blocks access to the material identified in the notification, the provider is **exempt from monetary liability and is protected from any liability to third parties for claims based on its having taken down the material**.[399] The U.S. Copyright Office has published the following information concerning designated agents:

> "The Copyright Office has created a directory of designated agents[400] from the designations filed with the Office for those service providers seeking the limitations on liability contained § 512(c). A copyright owner of an exclusive right, or authorized agent of a copyright owner, may use the Office's directory of designated agents to find the designated agent of a service provider that is hosting claimed infringing material, and may use that information to send a notification of claimed infringement to the service provider's designated agent.[401] Upon receipt of a compliant notification of claimed infringement, a service provider must respond expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of the infringing activity, if the service provider seeks to receive the benefits of the limitations of liability contained in § 512(c). A service provider is not required by law to remove the allegedly infringing material, but upon receipt of a compliant notification will be deemed to have been placed on notice of the allegedly infringing activity, and without the benefit of the limitations on liability contained in § 512, may face secondary liability for continuing to host the allegedly infringing material.
>
> The Copyright Office published interim regulations[402] specifying the procedure by which a service provider may designate an agent to receive notifications of claimed infringement. The Copyright Office does not provide printed forms for designating an agent, but makes available on this website suggested formats for filing an Interim Designation or an Amended Designation. An Amended Designation will replace in its entirety (not supplement) an Interim Designation or a prior Amended Designation for the same service provider. The Office has provided an Interim Designation template that may be used to designate an agent. Persons using this template have the option of filling in the blanks while viewing the form online and then printing out and signing the completed form, downloading the form for later use, or printing the blank form and completing it offline. Regardless of the method of completing the form, a printed copy of the completed form, together with the appropriate fee, must then be mailed or hand-delivered to the Copyright Office.
>
> Although the Copyright Office encourages the use of the Office's interim designation template (in part, because Copyright Office staff are familiar with this format and therefore the use of this form will simplify processing), service providers may prepare their own form, but should ensure that it includes all the information required in section 201.38 (c) or (f), as appropriate, of the interim regulations. Please note that the entire Interim Designation or Amended Designation that is submitted will be posted on the Copyright Office's website. Only include information in the designation submission that is intended to be publicly posted. If extraneous information is included in the submission that is not required by the interim regulations, that information will

---

assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

399 512(c)(3); 512(g)(1). *C.f.* discussion of the *Lenz* case under Section 2.3.1, *infra.*

400 Available at: http://copyright.gov/onlinesp/list/a_agents.html (Apr. 2, 2015).

401 See § 512(c)(3) for the required elements of notification.

402 Designation of Agent to Receive Notification of Claimed Infringement, 37 CFR, Part 201, available at: http://copyright.gov/fedreg/1998/63fr59233.html (Apr. 2, 2015).

also be scanned and posted on the website. If a service provider is paying the appropriate fee from a Copyright Office deposit account, a cover letter with the deposit account information should be submitted together with the designated agent form, not contained on the form itself."[403]

1.2.2.4. Limitation Regarding Information Location Tools

Section 512(d) limits liability for **referring or linking users to a website that contains infringing material** by using information location tools such as **hyperlinks, online directories, search engines** and the like, under the following conditions:

- The provider **must not have actual knowledge of the infringement**, or **be aware of facts or circumstances from which infringing activity is apparent.**
- If the provider has the right and ability to control the infringing activity, the provider **must not receive a financial benefit directly attributable to the activity**.
- Upon receiving notification of alleged infringement, the provider **must respond expeditiously to take the material down or block access to it.**

With the exception of some differences in the notification requirements, these conditions, as well as the provisions protecting against the possibility of mistaken or fraudulent notifications and those protecting the provider against claims based on having taken down material are very similar to those applicable to information stored at the direction of users.[404]

1.2.2.5. Special Rules Regarding Liability of Nonprofit Education Institutions

The actions or knowledge of a **faculty member or graduate student employee** of a nonprofit educational institution who is **performing a teaching or research function** may affect the institution's eligibility for one of the above four limitations on liability. In the context of transitory communications or system caching, the faculty member or student is **deemed a "person other than the provider**," such that the **institution is not disqualified from eligibility for the limitation**. With respect to the other limitations, the **knowledge or awareness of the faculty member or student will not be attributed to the institution**. The following conditions must, nonetheless, be fulfilled:

- The faculty member or graduate **student's infringing activities do not involve providing online access to course materials that were required or recommended during the past three years**;
- The institution has **not received more than two notifications over the past three years** that the faculty member or graduate student was infringing; and
- The institution provides all of its users with **informational materials describing and promoting compliance with copyright law**.[405]

Each law providing a cause of action which may be brought against an ISP provides for specific remedies available in connection with each type of cause of action; the availability of any specific type of remedy, then, will depend on whether the type of cause of action may be brought against an ISP. As a result, a breakdown of the law by remedy is not appropriate and would make any discussion difficult to follow.

---

403 See "Online Service Providers" on the website of the U.S. Copyright Office, available at: http://copyright.gov/onlinesp/ (Apr. 2, 2015.)

404 512(f)-(g); The Digital Millennium copyright Act of 1998: U.S. Copyright Office Summary, *op. cit*. at 12-13.

405 *Id.* at 13.

1.2.3. Remedies

There are no rules concerning specific types of actions which may be filed specifically against ISPs; the general rules concerning remedies (*e.g.* a strong preference for awarding money damages as a primary remedy) will apply. It should be noted that, although there may be instances in which it might be possible to obtain an injunction, these are the exception rather than the norm (and usually require proof of imminent irreparable harm in the sense that money damages can never compensate the loss). This is particularly true in the Internet context because of the extremely broad interpretation given in U.S. law to the freedom of speech protections of the First Amendment. Since Section 512 provides for certain specific remedies, it is unlikely that, as a litigation tactic, a plaintiff would not prefer to request one of these remedies rather than taking the riskier position of requesting an injunction.

Pursuant to section 512(c)(3) of the DMCA, where a copyright owner submits a notification of infringement under penalty of perjury to the service provider's designated agent, and the provider promptly **removes or blocks access** to the material identified in the notification, the provider is exempt from monetary liability as well as being protected from any liability to a third party for claims based on its having taken down the material.[406]

In order to provide some **protection against mistaken or fraudulent notifications**, the subscriber has the possibility of responding to an infringement notice and takedown by filing a **counter notification**, and the provider's limitation of liability for takedown is dependent upon the provider promptly notifying the subscriber that it has removed or disabled access to the material. If such a counter notification is filed (which requires the subscriber to state under penalty of perjury that the material was removed or disabled through mistake or misidentification, unless the copyright owner files an action seeking a court order against the subscriber) the provider must put the material back online within 10-14 business days after receipt of the counter notification. Knowing material misrepresentation in a notice or counter notice is subject to penalties as well as liability for any resulting damages (including costs and attorneys' fees) incurred by the alleged infringer, the copyright owner or its licensee, or the service provider.[407]

At least one such case has been filed. In 2007, Stephanie Lenz posted a video to YouTube of her children dancing and running around in her kitchen with Prince's "Let's Go Crazy" playing in the background. A few months later, Universal Music Corp. had the video removed for copyright infringement by using the take-down provisions of the DMCA. Lenz then filed a lawsuit in federal court[408], requesting Universal be held accountable for misrepresenting that her video violated copyright law when, instead, it represented fair use of the Prince song. In dismissing the parties' respective motions for summary judgment, the court ruled[409] that the DMCA does not give copyright owners the right to simply take down content without first not only considering some facts that might be relevant to a fair use analysis but also " evaluat[ing] the significance of such facts."

The opinion of the Ninth Circuit Court of Appeals in this case was published on September 14, 2015.[410] The Court confirmed that a copyright owner must consider the existence of fair use before sending a DMCA takedown notice and, **if the online content uses the copyright owner's material in a manner that qualifies as a fair use**, the copyright owner **may not send a DMCA takedown notice**. The copyright

---

406 §512(g)(1)

407 §512(f); The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary *op,cit.* at 12.

408 *Lenz v. Universal Music Corp*., Not Reported in F.Supp.2d, 2008 West Law 962102, 2008.

409 *Lenz v. Universal Music Corp*., Order Denying Cross-Motions for Summary Judgment, available at: https://www.eff.org/node/73102 (Apr. 14, 2014).

410 Available at: http://cdn.ca9.uscourts.gov/datastore/opinions/2015/09/14/13-16106.pdf (Sept. 21, 2015).

owner who sends a DMCA takedown notice need only have a **subjective good faith belief that fair use does not apply in order to avoid liability** for any DMCA misrepresentation – even if a court subsequently reaches the opposite conclusion and decides that fair use does indeed apply. An **intensive, in-depth analysis is not required** – in fact, the majority held that a computer algorithm might be sufficient. On the other hand, where a copyright owner subjectively believes that there is a significant probability that a particular use qualifies as a fair use and takes deliberate action to avoiding acquiring knowledge of the fair use, sending a takedown notice is likely to be a DMCA misrepresentation under the willful blindness doctrine. The court's opinion gives little guidance on what will adequately support a good faith belief on what type of family video posting will constitute fair use, however, it would appear that no actual monetary loss need be demonstrated to recover at least nominal damages.

Section 512(h) establishes a procedure pursuant to which a copyright owner can obtain a **subpoena from a federal court ordering a service provider to disclose the identity of a subscriber who is allegedly engaging in infringing activities**.

Subsection (m) specifically provides that the section **does not require a service provider to monitor** its service or access material in violation of law (*e.g.* the Electronic Communications Privacy Act) as a condition for eligibility for one of the liability limitations of Section 512.

1.3. Application of General Provisions / Common Law to ISPs

There is extensive (and not always consistent) case law concerning issues relating to ISP liability and the Internet. A complete analysis of this case law goes well beyond the scope of this opinion. We will therefore limit our discussion to some of the more important and/or interesting recent cases on these issues, all of which concern trademark liability.

The Lanham Act, enacted by Congress in 1946, provides for a national system of trademark registration and protects the owner of a federally registered mark against the use of similar marks if such use is likely to result in consumer confusion, or if the dilution of a famous mark is likely to occur. The Lanham Act was codified in U.S. law at 15 U.S.C. §§ 1051 *et seq.* One of its sections, 15 U.S. Code § 1114[411], on the one hand, provides for civil liability for trademark infringement but, on the other hand, specifically provides for a safe harbor from liability for damages in the case of "innocent infringement by printers and publishers."

Primary liability of an ISP is analyzed in the same fashion as any other primary liability case. The seminal case on **secondary participant-based trademark infringement**, however, remains ***Inwood*** *Laboratories, Inc. v. Ives Laboratories, Inc.*[412] That case concerned a trademark infringement claim under 15 U.S. Code § 1114 made against manufacturers of generic versions of a brand-name drug on the grounds that, by manufacturing the generics in identically colored capsules and using catalog entries comparing prices and revealing the colors of the generic capsules, they induced pharmacists illegally to substitute a generic drug for the brand-name drug and to mislabel the substitute drug.[413] While finding no vicarious liability of the generic manufacturer for the pharmacists' infringement, the U.S. Supreme Court held:

> Thus, if a manufacturer or distributor **intentionally induces** another to infringe a trademark, or if it **continues to supply** its product to one whom it **knows or has**

---

411 ("Remedies; infringement; innocent infringement by printers and publishers"), available at: https://www.law.cornell.edu/uscode/text/15/1114 (Apr. 16, 2015).

412 456 U.S. 844, 102 S.Ct. 2182 (U.S. 1982).

413 456 U.S. at 849-50.

> **reason to know is engaging in trademark infringement**, the manufacturer or distributor is contributorily responsible for any harm done as a result of the deceit. [emphasis added][414]

1.3.1. As Applied to Auction Sites

The *Inwood* test, then, offers **two ways for a plaintiff to establish secondary liability: (1) intentional inducement of a third party** or **(2) continued supply to a third party with actual or constructive knowledge of such party's infringement**.[415] *Inwood* has notably been applied to the online environment in the context of secondary liability of auction sites, such as eBay, for listing infringing items for sale on their websites.[416] In one such case[417], the jeweler Tiffany unsuccessfully sued the online auctioneer, who knew that some of the jewelry appearing for sale on their website might be counterfeit. The background for that case was as follows: eBay had voluntarily implemented several measures to help ensure the authenticity of goods advertised on its websites.[418] For example eBay (at a cost of $20 million per year): (1) developed a "fraud engine" software to identify illegal listings; (2) maintained and managed the Verified Rights Owner (VeRO) Program, a notice and takedown system allowing trademark owners to submit a Notice of Claimed Infringement (NOCI) to eBay identifying listings offering items that infringed owners' rights, thereby allowing eBay to remove them, which eBay did promptly upon receiving an NOCI; (3) provided a space for trademark owners on its site (an "About Me" page) to warn users about suspected fakes and (4) suspended hundreds of thousands of sellers that eBay suspected were engaged in infringing conduct.[419] These actions did not suffice to prevent Tiffany from bringing an action against eBay for contributory infringement. On appeal, the Second Circuit court held:

> For contributory trademark infringement liability to lie, a service provider mush have **more than a general knowledge or reason to know that its service is being used to sell counterfeit goods**. Some **contemporary knowledge of which particular listings are infringing** or will infringe in the future is **necessary**.[420]

The Second Circuit appears to have left an opening for trademark owners who have not given notice of a specific infringing listing by suggesting that "**willful blindness might satisfy the knowledge standard,**" however the court did not find willful blindness in *Tiffany* because, although eBay knew there were infringing postings on their site, they did not ignore the information they received concerning infringements.[421]

1.3.2. As Applied to Search Engines

The issue of potential secondary liability of search engines for infringements committed by advertisers to whom they have sold keywords tied to the trademarks of third parties has been treated less extensively in U.S. case law. According to Prof. Dinwoodie[422], this is because the liability of search

---

414 *Id.* at 854.

415 G. Dinwoodie, *International Landscape of Secondary Liability,* 37 Columbia Journal of Law & Arts ("Colum.J.L. & Arts") 463, 472 (2014).

416 *Id.*

417 *Tiffany (NJ) Inc. v. eBay Inc.,* 600 F.3d 93 (2d Cir. 2010) ("Tiffany").

418 Dinwoodie, 37 Colum.J.L. & Arts at 472.

419 *Id.,* citing *Tiffany*.

420 *Tiffany,* 600 F. 3d at 107.

421 Dinwoodie, *op. cit.* at. 475.

422 *Id.*

engines has usually been analyzed as a matter of primary trademark infringement. It may also be because parties prefer to settle these cases rather than litigate them until judgment.

For example, in 2007, Viacom filed a $1 billion lawsuit against YouTube, accusing the Google unit of illegally broadcasting 79,000 copyrighted videos on its website between 2005 and 2008.[423] The suit was eventually settled in March, 2014, although the details of that settlement have not been released. Google and Viacom issued the following joint statement at the time: "This settlement reflects the growing collaborative dialogue between our two companies on important opportunities, and we look forward to working more closely together."[424] Articles in the press have nonetheless intimated that "Google, which acquired YouTube in 2006, has more or less made peace with most big content companies, in part via a 'ContentID' system that allows copyright owners to track their stuff on the world's largest video site. The system also gives content owners the ability to demand "takedowns" of their stuff — or the option to run ads against it."[425]

2. Implementation

2.1. Overview

With the exception of the civil procedure aspects of the laws discussed under Section 1.2, *supra.,* we are unaware of any provisions or measures concerning civil procedure in matters relating to the liability of ISPs. The rules concerning jurisdiction (and, in particular, the Constitutional limitations on the exercise by a court of jurisdiction over a defendant not physically located within the jurisdiction, be it in another state or another country) would apply in this context. There is fairly abundant case law concerning the extent to which an internet presence, as well as the nature of the website in question, may justify such extra-territorial exercise of jurisdiction. An in-depth discussion of this body of case law is nonetheless beyond the scope of this opinion.[426]

2.2. National Facts

There are no civil procedure rules specific to ISPs; the ordinary rules apply.

2.3. International facts

There are no private international law rules specific to ISPs; the ordinary rules apply.

---

423 See: *Viacom Intern. Inc. v. YouTube, Inc.,* 718 F.Supp.2d 514, Southern District of New York (Manhattan) 2010; *Viacom International v. YouTube*, 676 F.3d 19, U.S. Court of Appeals for the Second Circuit (Manhattan) 2012; *Viacom Intern. Inc. v. YouTube, Inc*., 940 F.Supp.2d 110, Southern District of New York, 2013.

424 J. Stempel, "Google, Viacom settle landmark YouTube lawsuit, " Reuters, Mar. 18, 2014, available at: http://www.reuters.com/article/2014/03/18/us-google-viacom-lawsuit-idUSBREA2H11220140318 (Apr. 14, 2014).

425 P. Kafka, "It's Over! Viacom and Google Settle YouTube Lawsuit," Tech News, Reviews & Analysis, Mar. 18, 2014, available at: http://recode.net/2014/03/18/its-over-viacom-and-google-settle-youtube-lawsuit/ (Apr. 14, 2014).

426 For an in-depth discussion of these issues, see, *e.g.,* G. Dinwoodie *et al,* The Law Applicable to Secondary Liability in Intellectual Property Cases, 42 New York University Journal of International Law and Politics, last revised January 20, 2011, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1502244 (Apr. 13, 2015).

2.4. Memorandum of Understanding

Although not, technically, a proposition for the future, the Memorandum of Understanding (MOU) concerning the Center for Copyright Information of 2011[427] signed by various content owner representatives, certain participating ISPs and participating content owner groups bears mention. The MOU provided, among other things, for the creation of the **Copyright Alert System** ("CAS")[428]. The CAS was developed to help consumers understand the importance of respecting copyright and to alert them of possible infringing activity that has taken place using their Internet connection. Through the CAS, copyright owners send notices of alleged copyright infringement to participating ISPs, who then forward these notices to their Subscribers in the form of Copyright Alerts. The Alerts include the date, time, time zone and title of the copyrighted content alleged to have been unlawfully distributed through a peer-to-peer or file sharing system on a Subscriber's account. Under the CAS, **users will be sent a maximum of six Alerts** with an increasing degree of seriousness. In general, there are two Educational Alerts, two "Acknowledgement" Alerts that require a response from the Subscriber, and two "Mitigation" Alerts that impose minor consequences to emphasize the seriousness of the problem.[429]

Mitigation Measures are intended to further emphasize the need to cease infringing activity of Subscribers. The measures differ for each Internet Service Provider ("ISP") but may, for example, take one of the following forms:

- A temporary reduction of Internet speed;
- Redirection to a landing page until the primary account holder of your account contacts your ISP;
- Redirection to a landing page where the primary account holder must review and respond to educational information.

While the ISPs can modify the Mitigation Measures in a manner consistent with their own policies, ISPs will not use account termination as a Mitigation Measure.[430]

A Subscriber can request a review of a Copyright Alert when s/he receives a "Mitigation Alert" (after three or four Alerts, depending on the Subscriber's ISP). Administered by the American Arbitration Association ("AAA"), the Independent Review Program is an inexpensive way to challenge the validity of some or all of the Copyright Alerts (on one of the grounds specified below) through an electronic process conducted by trained examiners. To file for an Independent Review a Subscriber must complete the application steps on the AAA website within fourteen calendar days of receiving a Mitigation Alert. If the Subscriber's challenge is successful, no Mitigation Measure will be applied and record of the Copyright Alerts will be removed from the Subscriber's account. If the challenge is not successful, the ISP will implement the Mitigation Measure.[431]

If a Subscriber used the file at issue but his or her use would be deemed "fair use" under the law, the Subscriber's use will not constitute copyright infringement. U.S. Copyright law specifies four factors to consider in determining whether an otherwise infringing use of a work is "**fair use**" and asks courts to

---

427 Available at: http://www.copyrightinformation.org/wp-content/uploads/2013/02/Memorandum-of-Understanding.pdf (April 14, 2015). Since all of the provisions discussed in this section are a matter of contract law, based on this MOU, this section cites almost exclusively to the website of the organization which implements this agreement.

428 For additional information see the website of the Center for Copyright Information website at: http://www.copyrightinformation.org/the-copyright-alert-system/ (April 15, 2015).

429 See: http://www.copyrightinformation.org/resources-faq/independent-review-faqs/ (April 16, 2015).

430 *Id.*

431 *Id.*

look at the specific facts presented to determine whether "fair use" applies in a particular case. The four factors are: **(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.**

In order to prove "fair use", the Subscriber would need to show that his or her use was for commentary, criticism, news reporting, teaching, or research; or that s/he changed the work and the new version does not harm the market for the original. A number of courts have considered whether downloading and distributing ("sharing") digital files that are identical to the original through P2P systems is fair use. Thus far, all of these courts have held that this behavior is not fair use.[432] [433]

---

432 See *A & M Records, Inc. v. Napster, Inc.,* 239 F.3d 1004, 1015 (9th Cir. 2001) (even where the works are not offered for sale, exchanging them for others as a barter is commercial and not fair use); *Sony BMG Music Entm't v. Tenenbaum*, 672 F. Supp. 2d 217, 232–37 (D. Mass. 2009) (downloading and "sharing" files has an effect on the market for the original work even if the user would not have purchased every one of the files traded).

433 See: http://www.copyrightinformation.org/resources-faq/independent-review-faqs/what-are-the-grounds-for-requesting-a-review/ (April 23, 2015).

IV. SCHLUSSFOLGERUNGEN

1. Auslegung der EU-Richtlinien durch den EuGH

Der EuGH hat die verschiedenen Richtlinien in teilweise weitreichenden Entscheidungen angewendet. Auch wenn die Entscheide keine ausdrücklichen Anweisungen für den Gesetzgeber enthalten, prägen diese die weitere Entwicklung des Rechts durchaus.

Zu erwähnen sind in diesem Zusammenhang insbesondere der Entscheid Promusicae (keine Überwachungspflicht), SABAM (keine allgemeine Filter- und Blockierungspflicht) und UPC Telekabel (zu den Voraussetzungen einer zulässigen Blockierung) im Bereich des Copyrights, L'Oréal v. Ebay (keine Haftungsfreistellung der Online-Geschäftsplattform, die eine aktive Rolle spielt), Hyperlinks (Svensson, BestWater und C-More Entertainment: Haftungsfreistellung für Hyperlinks und für „Framing", aber Möglichkeit nationaler Massnahmen, die Broadcasting schützen) sowie im Bereich des Datenschutzes Google v. Spain (Recht auf Vergessen).

2. Evaluationen der EU-Richtlinien und Revisionspläne:

- Die Strategie zum digitalen Binnenmarkt von Mai 2015 stellt eine umfassende Überarbeitung der Bestimmungen zur Verantwortlichkeit von Internetmittlern in Aussicht, wobei insbesondere die Möglichkeit der Regelung eines Melde- und Abhilfeverfahrens sowie allfällige Sorgfaltspflichten von Internetdienstleistern geprüft werden sollen, gerade (aber nicht nur) im Zusammenhang mit Urheberrechtsverletzungen. Die Strategie sieht auch eine Neuregelung des Urherberrechts insgesamt in Aussicht, so dass in der Tat der gesamte Rechtsrahmen zur Verantwortlichkeit von Providern sich in kurzer Zeit umfassend ändern könnte.
- Die E-Commerce-Richtlinie 2000/31/EG wurde in verschiedenen Analysen und Studien evaluiert. Für die Verantwortlichkeit von Internetdienstleistern wurden dabei insbesondere Unklarheiten im Anwendungsbereich (insbesondere angesichts der Entwicklung neuer Angebote, z.B. Hyperlinks, Video-Streaming, etc.), Unterschiede in der Umsetzung (insbesondere zu den Voraussetzungen der Haftungsfreistellung von Hosting- und Access-Providern) und die Vielzahl verschiedener Melde- und Abhilfeverfahren (Notice and Take-Down-Procedures) als schwierig hervorgehoben.
- Die Durchsetzungsrichtlinie 2004/48/EG wird zwar als ungenügend empfunden und 2014 wurde ein Aktionsplan für einen neuen Konsens über die Durchführung der Immaterialgüterrechte angenommen. Die Rolle der Internetdienstleister soll dabei spezifisch berücksichtigt werden.
- Die Urheberrechts- oder Informationsrichtlinie 2001/29/EG wurde in verschiedenen Berichten und Konsultationen beurteilt. Dabei sind die Meinungen zu einer allfälligen Weiterentwicklung der Verantwortlichkeit von Internetdienstleistern geteilt. Eine entsprechende Neuregelung wird in der Strategie zum digitalen Binnenmarkt in Aussicht gestellt.
- Im Bereich der Datenschutzrichtlinie 95/46/EG ist eine umfassende Revision per Ende 2015 in Aussicht gestellt. Dabei sind zwar keine Sonderregeln für Internetdienstleister vorgesehen, aber gewisse Vorschriften betreffen sie durchaus, soweit sie als für die Datenbearbeitung verantwortliche Person gelten (z.B. die Pflicht, nach einer Veröffentlichung von Daten alle Schritte zur Information von Dritten über ein Löschungsgesuch zu treffen). Gerade diesbezüglich sind die Differenzen zwischen dem Europäischen Rat und dem Europäischen Parlament allerdings noch beträchtlich, so dass sich das Resultat der aktuellen Verhandlungen nicht voraussagen lässt.

3. Die verschiedenen Richtlinien wurden in folgenden Rechtsakten umgesetzt:

- E-Commerce-Richtlinie

D	Telemediengesetz
F	Loi du 21 juin 2004 n° 2004-575 pour la confiance dans l'économie numérique
UK	Electronic Commerce (EC Directive) Regulations 2002
DK	Danish E-Commerce Act

- Art. 8 Durchsetzungsrichtlinie

D	§ 19 Markengesetz; § 101 Urhebergesetz
F	Loi 2007-1544 du 29 octobre 2007 (Code de la propriété intellectuelle)
UK	England: Common Law Schottland: Intellectual Property (Enfocement, etc.) Regulations 2006
DK	Retsplejeloven (Zivilprozessrecht) Kapitel 29a

- Art. 8 (3) Urheberrechts- oder Informationsrichtlinie

D	Vorbestehende Störerhaftung
F	Loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information (Code de la propriété intellectuelle)
UK	Section 97 A Copyright Designs and Patents Act 1988
DK	Keine Änderungen im bestehenden Datenschutzrecht (Ophavsretsloven*) &* Retsplejeloven (Zivilprozessrecht) Kapitel 40

- Datenschutzrichtlinie

D	Bundesdatenschutzgesetz
F	Loi 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel
UK	Data Protection Act 1998
DK	Lov om behandling af personoplysninger

In den verschiedenen Staaten werden insbesondere bei der Umsetzung der E-Commerce-Richtlinie folgende Lücken und Schwierigkeiten angemerkt:

D	Anwendung auf Hyperlinks, Suchmaschinen sowie WLAN Anbieter
F	Anforderung an die Kenntnis des Internetdienstleisters, Frage der offensichtlichen Rechtswidrigkeit des Inhalts
UK	Anwendung auf Hyperlinks, Drittstaaten, Auslegung des Begriffs Hosting (und Anwendung der entsprechenden Ausnahme z.B. auf Blogs)
DK	Anforderung an die Kenntnis des Internetdienstleisters; Zeitrahmen für Herunternahme von rechtswidrigem Inhalt

4. Spezielle zivilrechtliche Verantwortlichkeitsbestimmungen ausserhalb des EU-Rechts wurden insbesondere im Rahmen des Defamation Act 2013 sowie des Digital Economy Act 2010 im Vereinigten Königreich eingeführt, wobei es sich im ersten Fall um eine Möglichkeit der gerichtlichen Anordnung der Entfernung von Inhalten handelt, im zweiten Fall um die Möglichkeit der Verpflichtung von Internetdienstleistern zum Ergreifen von „technischen Massnahmen" gegenüber Klienten sowie um Informationspflichten. Die im Digital Economy Act 2010 in Aussicht gestellten Regelungen werden allerdings vorerst nicht angewendet, da sich die grösseren Dienstleister und Unternehmen der Unterhaltungsindustrie auf eine Vereinbarung diesbezüglich geeinigt haben.

5. Im Bundesrecht der Vereinigten Staaten von Amerika scheinen zwei spezielle zivilrechtliche Verantwortlichkeitsbestimmungen gegenüber Providern relevant, die beide Haftungserleichterungen zum Gegenstand haben; der eine im Copyright, der andere zum *Defamation Act*. Im Bereich des Copyrights führt die Haftungserleichterung in der Regel zu einem Wegfall der Schadenersatzpflicht und teilweise auch der Möglichkeit gerichtlicher (Unterlassungs-)Anordnungen (*injunctions*). Für verschiedene Providerarten bestehen dabei unterschiedliche Voraussetzungen. Soweit ein Provider Information speichert, setzt die Haftungsfreistellung insbesondere voraus, dass das entsprechende Material auf entsprechenden Hinweis des Rechteinhabers entfernt worden ist. Allgemeine (auf alle Rechtsverletzer anwendbare) Verantwortlichkeitsbestimmungen sind im Bereich des Markenrechts relevant. Hier führt die Rechtsprechung zu Suchmaschinen und Auktions-Seiten insbesondere aus, wann ein Service Provider von einer Rechtsverletzung spezifisches Wissen hat, um dafür zur Verantwortung gezogen zu werden. Nach der Lehre besteht eine gewisse (wenn auch nicht umfassende) Tendenz dazu, dem Internetdienstleister eine Pflicht zum Ergreifen gewisser Schritte zur Verhinderung von (weiteren) Verletzungen aufzuerlegen. Angesichts des sektorspezifischen Ansatzes der US-Amerikanischen Regelung scheint die Abstimmung zwischen den verschiedenen Regelungen kaum zu Schwierigkeiten zu führen.

6. Soweit ersichtlich bestehen in den USA, der EU oder den ausgewählten EU-Mitgliedstaaten keine (über die obigen Regelungen hinausgehenden) besonderen Regelungen zur Rechtsdurchsetzung gegenüber Providern.

7. Soweit ersichtlich bestehen in den USA, der EU oder den ausgewählten EU-Mitgliedstaaten keine Bestrebungen, verbindliche Regelungen zur rascheren oder besseren Rechtsdurchsetzung gegenüber Providern zu schaffen. Die Rechtsdurchsetzung wird allerdings in der EU, im Vereinigten Königreich und in den USA teilweise durch Vereinbarungen (*Memoranda of Understanding*) der grösseren in den jeweiligen Bereichen aktiven Unternehmen mit den grösseren Internetdienstleistern erleichtert, wobei der Staat diese insbesondere in Europa unterstützt und prüft.

SCHWEIZERISCHES INSTITUT FÜR RECHTSVERGLEICHUNG

Dr. Lukas Heckendorn Urscheler
Vize-Direktor

Dänemark: Signe Vest & Henrik Westermark, Referent für skandniavisches Recht
Deutschland: Dr. Johanna Fournier, Referentin für deutsches Recht
Europäische Union: Henrik Westermark & Lukas Heckendorn Urscheler
Frankreich: Stephanie De Dycker, Referentin für französischsprachige Rechtsordnungen
USA: Karen T. Druckman, Referentin für US-Amerikanisches Recht
Vereinigtes Königreich: John Curran, Referent für englisches Recht