FORSCHUNGSSTELLE FÜR
VERBRAUCHERRECHT (FFV)

Prof. Dr. Martin Schmidt-Kessel
Direktor

Universität Bayreuth • 95440 Bayreuth

Postanschrift:
Universität Bayreuth
95440 Bayreuth

Gebäude: RW I
Universitätsstraße 30
95447 Bayreuth

Telefon: 0921 / 55 - 6126
Telefax: 0921 / 55 - 6122

Internet: www.verbraucherrecht.uni-bayreuth.de
E-Mail: verbraucherrecht@uni-bayreuth.de

Die Regulierung des Datenschutzes und des Urheberrechts in der digitalen Welt

Eine vergleichende Untersuchung zu den USA, Großbritannien, Frankreich und Schweden

Gutachten im Auftrag des Verbraucherzentrale Bundesverbands

von

Prof. Dr. Martin Schmidt-Kessel

unter Mitarbeit von Prof. Dr. Claas Christian Germelmann**,** Johanna Held, Hannah Katrin Herden, Christine Kirchberger, Shane McNamee**,** Pam Storr, Sonja Wichmann

Inhalt

– Zusammenfassung der Ergebnisse –

1. Die Marktanalyse zeigt bei allen untersuchten Rechtsordnungen eine starke Differenzierung zwischen zentralen großen Akteuren (Global Player und nationale Anbieter) und einer großen Zahl kleinerer Anbieter.

   a. Die besondere Stärke einer relativ kleinen Zahl von Großanbietern in der digitalen Welt ist ordnungspolitisch problematisch und zeigt Handlungsbedarfe. Das gilt erst recht angesichts des Umstandes, dass gegen die betreffenden Akteure die Standards des Datenschutz- und Verbraucherrechts schlecht durchgesetzt werden können.

   b. Für die Entwicklung einer Aufsichtsstruktur für die digitale Welt ist an einen differenzierten Zugriff in Abhängigkeit von Marktmacht und Systemrelevanz zu denken. Dies könnte – nach dem Vorbild der neuen Architektur der europäischen Bankenaufsicht – auch unterschiedliche Zuständigkeitsebenen einschließen.

2. Die untersuchten Rechtsordnungen verfügen über keine besonderen Behörden zum Schutz des Verbrauchers in der digitalen Welt.

   a. Eine eigenständige, administrative Durchsetzung oder Marktaufsicht für den digitalen Markt durch eine einzige Aufsichts- oder Regulierungsbehörde unter verbraucherspezifischen Aspekten besteht nicht.

   b. Die beiden Schutzfunktionen – Handeln einer Administrativbehörde zum repressiven Schutz der Verbraucher sowie eine administrative Aufsicht zur präventiven Vermeidung von verbraucherspezifischen Gefahren – sind in keiner der untersuchten Rechtsordnungen für die digitale Welt in einer verwaltungsrechtlichen Einheit zusammengefasst.

3. Das Verhältnis zwischen Verbraucherschutz und den Sonderregeln des Datenschutzrechts und des Urheberrechts ist für beide Gebiete sehr verschieden.

   a. Datenschutz gegenüber Unternehmen ist zwar historisch ein gesondertes Rechtsgebiet, wird aber heute politisch und zunehmend auch rechtlich als Verbraucherschutz eingeordnet.

   b. Urheberrecht dient – trotz gegenteiliger rechtspolitischer Forderungen – nach wie vor dem Urheberschutz. Verbraucher- oder Nutzerinteressen fließen nur beim Interessenausgleich ein, der für die Feinjustierung der auf Privatpersonen bezogenen materiellen Ausnahmen vom Urheberrecht sowie der Durchsetzungsinstrumente erforderlich ist. Anhaltspunkte für eine abweichende Entwicklung bestehen bislang allein für Schweden.

4. Allgemeine Konzepte und Institutionen zum Schutz von Verbrauchern oder der öffentlichen Sicherheit und Ordnung lassen sich auch für die digitale Welt nutzbar machen.

   a. Das gilt insbesondere für die marktbezogenen Konzepte administrativen Vorgehens gegen unfaire oder unseriöse Geschäftspraktiken in den USA („*unfair and deceptive trade practice*“) und den untersuchten EU-Mitgliedstaaten. Aus deutscher Perspektive lassen sich diese als „öffentlich-rechtliches (Un-)Lauterkeitsrecht“ einordnen, wie sie Art. 11 I UGP-Richtlinie 2005/29/EG den Mitgliedstaaten als (von deren Mehrzahl genutzter) Alternative zum deutschen zivilrechtlichen Modell einräumt.

   b. Das Ausscheiden von Unternehmen aus dem Markt insgesamt können allgemeine Verbraucherschutzbehörden wie auch die besonderen Datenschutzbehörden kaum einmal anordnen. Die Befugnis beschränkt sich in aller Regel auf die Untersagung bestimmter Produkte oder Verhaltensweisen und auf Sanktionen (Bußgelder).

5. Administrativ organisierter Verbraucherschutz erfolgt in der digitalen Welt in höchst unterschiedlichem Maße.

a. Datenschutz wird – mit deutlichen Abstichen für die USA – in den untersuchten Rechtsordnungen auch durch starke Sonderbehörden betrieben. Eine Zusammenfassung beider Aspekte in einer Behördenzuständigkeit findet sich – abgesehen von den allgemeinen Ordnungsbehörden – nur ausnahmsweise statt, etwa unter dem US-Konzept der *unfair and deceptive trade practice*. Es ist freilich auch für die Europäische Union vorstellbar, die Bekämpfung unfairer Geschäftspraktiken im Sinne der UGP-Richtlinie 2005/29/EG für den Datenschutz fruchtbar zu machen.

b. Öffentliche Verwaltung im Bereich des Urheberrechts findet bislang nur begrenzt und dann zum Zwecke der Durchsetzung des Urheberrechts statt, wie etwa bei der durch die *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* (HADOPI) und dem *Office of Communications* (OFCOM) administrierten *three strikes policy* Frankreichs und Großbritanniens. Diese dienen freilich nur mittelbar –durch die Definition begrenzter Sanktionen, ein rechtsstaatliches Verfahren sowie insgesamt die Kanalisierung der Rechtsdurchsetzung – dem Verbraucherschutz.

6. Die einschlägigen Behörden der untersuchten Rechtsordnungen dienen grundsätzlich nicht der Durchsetzung individueller Rechte oder der Beratung einzelnen Verbraucher.

a. Vorrangiger Zweck der behördlichen Rechtsdurchsetzung ist die Durchsetzung und Sicherung der einschlägigen Standards am Markt. Pflichten oder Ansprüche auf Eingreifen bestehen in aller Regel nicht.

b. Die Verknüpfung der Behördentätigkeit mit der Trägerschaft einer Einrichtung für die außergerichtliche Streitschlichtung verbessert die Informationsgewinnung der Behörde und stärkt ihre Stellung auch im Hinblick auf die administrative Durchsetzung.

7. Die einschlägigen Behörden verfügen in ihren – beschränkten und das Urheberrecht regelmäßig nicht betreffenden – Aufgabenbereichen über weitreichende Befugnisse.

a. Befugnisse zur Tatsachenermittlung, zur Annahme von Verbraucherbeschwerden, sowie in Schweden die Befugnis des KO neben dem *Allmänna reklamationsnämnden* auch individuellen Verbraucherbeschwerden regelnd nachzugehen bilden enorm wichtige Instrumente der Erkenntnis über die Einhaltung verbraucher- und datenschutzrechtlicher Standards allgemein und in der digitalen Welt. Ein weiterer Ausbau von ADR-Trägerschaften – etwa in Umsetzujng der ADR-Richtlinie – würde diesen kognitiven Teil der Marktüberwachung erheblich stärken.

b. Eine wesentliche weitere Funktion der einschlägigen Behörden ist die Information von Verbrauchern und Unternehmen aber auch der Öffentlichkeit und damit auch der Politik. Diese kommunikative Aufgabe macht regelmäßig einen großen Anteil der behördlichen Aktivität aus und erfolgt sowohl im Einzelfall als auch durch Berichte.

c. Den berufenen Verwaltungsbehörden stehen – in den begrenzten, das Urheberrecht regelmäßig nicht erfassenden Zuständigkeiten – Befugnisse sowohl von Anordnungen im Einzelfall (etwa Untersagungsverfügungen) als vielfach auch zu administrativer Normsetzung zu. Darüber hinaus ergibt sich die Stärke der betreffenden Behörden teilweise auch aus der Möglichkeit zur Verhängung von Bußgeldern. Den meisten einschlägigen Behörden der untersuchten Rechtsordnungen fehlt hingegen die Möglichkeit, „schwarze Schafe“ nach Art der deutschen Gewerbeuntersagung vom Markt zu verbannen. Wobei öffentliches „naming and shaming“ teilweise eine ähnliche Funktion erfüllt, gegen die effektive Rechtsbehelfe des Unternehmers – auch im Falle eines falschen Verdachts – kaum zur Verfügung stehen.

8. Hinsichtlich der Einbindung der einschlägigen Behörden in den Staatsaufbau finden sich ganz erhebliche Unterschiede. Insgesamt ist aber die Tendenz zu weisungsunabhängigen Agenturen erkennbar denen sowohl eine Regelungsbefugnis für den Einzelfall als auch eine Normsetzungsbefugnis zukommt.

a. Für den Datenschutz ergibt sich dies im Bereich der Europäischen Union bereits aus der Datenschutzrichtlinie. Von politischer Steuerung (ganz oder teilweise) unabhängige Agenturen finden sich aber auch für den allgemeinen Verbraucherschutz (etwa die *Federal Trade Commission* [FTC]) oder der *Konsumentombudsmannen* [KO]).

b. Den betreffenden Behörden steht regelmäßig auch eine (abgeleitete) Rechtssetzungskompetenz zu. Für die US-amerikanische FTC ergibt sich diese sogar durch die Möglichkeit zur Herbeiführung der Allgemeinverbindlichkeit von Einzelfallentscheidungen.

9. In Deutschland findet sich – abgesehen von den allgemeinen Ordnungs- und Sonderordnungsbehörden – nur eine sehr begrenzte behördliche Aufsichtsstruktur für die digitale Welt, wie beispielsweise in Ansätzen bei der Bundesnetzagentur für den Bereich der Telekommunikation sowie bei den Landesdatenschutzbehörden. Bei Überlegungen zur Etablierung ähnlicher Strukturen und Handlungsbefugnisse und -mittel wie in den untersuchten Rechtsordnungen, sind verschiedene Aspekte zu bedenken:

a. Die öffentlich-rechtliche Durchsetzung verbraucherschützender Standards für die digitale Welt steckt in Deutschland – abgesehen vom Datenschutz – noch in den Kinderschuhen. Die Befugnisse des BVL für den grenzüberschreitenden Rechtsverkehr werden nur eingeschränkt zur Kenntnis genommen.

b. Als allgemeines marktbezogenes Aufsichtsinstrument käme in Deutschland insbesondere eine (auch!) öffentlich-rechtliche Umsetzung von Art. 11 UGP-Richtlinie 2005/29/EG in Betracht, die aber durch Landesbehörden vollzogen werden müßte.

c. Verbunden werden könnte dieses Aufsichtsinstrument auch mit der Trägerschaft für Streitschlichtungsstellen nach der ADR-Richtlinie 2013/11/EU.

d. Die Empfehlung der Europäischen Kommission zum *colletive redress* sieht ausdrücklich behördliche Möglichkeiten zur Koordinierung von Verbraucherklagen unter Einbezug datenschutzrechtliche Ansprüche vor.

A. Einleitung

Die traditionelle Wahrnehmung des Verbraucherrechts in Deutschland und insbesondere in der deutschen Rechtswissenschaft ist nicht selten merkwürdig einseitig: Verbraucherrecht gilt verbreitet als Sonderprivatrecht. Dabei ist der Instrumentenmix, welcher Standardsetzung und Durchsetzung mit allen zur Verfügung stehenden Instrumenten also insbesondere auch mit den Mitteln des Straf- und Ordnugnswidrigkeitenrechts betreibt, politisch eine Selbstverständlichkeit. Immerhin finden sich für einzelne Sektoren zunehmend Betrachtungen des Verbraucherrechts, welche ausgehend von Sachfragen und Schutzbedarfen des jeweiligen Sektors mit einem umfassenden Ansatz die Rolle des gesamten (potentiellen) Instrumentariums des Verbraucherrechts in den Blick nehmen; besonders wichtige Beispiele sind insoweit die Lebensmittelsicherheit[1] und der Anlegerschutz[2]. Eine übergreifende, systematische Aufarbeitung der mit diesem Mix verbundenen Sach- und Rechtsfragen steht freilich bislang aus.

Eine wesentliche Gruppe von Instrumenten des Verbraucherrechts läßt sich unter der Überschrift „Schutz des Verbrauchers durch die öffentliche Verwaltung“ zusammenfassen. Sie entspricht der gesamtstaatlichen Verantwortung für den Verbraucherschutz und ist Ausdruck zweier spezifischer Aufgaben, welche die öffentliche Verwaltung und das Verwaltungsrecht für den Schutz des Verbrauchers wahrnehmen: Dabei geht es einerseits um spezifisch hoheitliche Schutzinstrumente wie präventive und repressive Marktzugangsbeschränkungen für Unternehmer und für deren Leistungen, die Markt-, Unternehmer- und Produktüberwachung oder die Information oder Warnung der Öffentlichkeit – im Mittelpunkt steht hier die präventive Funktion der betreffenden Regelungen und Handlungen. Andererseits fällt der öffentlichen Verwaltung die Aufgabe zu, materielle Standards des Verbraucherrechts und des Verbraucherschutzes durchzusetzen und damit deren Einhaltung zu erzwingen; dieser Erzwingungsfunktion sind etwa die Untersagung verbraucherrechtswidriger Leistungsgegenstände, Vertriebsmethoden und sonstiger Verhaltensweisen oder die Sanktionierung von Unternehmerverhalten durch Bußgelder zuzurechnen. Bei der zu Durchsetzungszwecken vorgenommenen Herausnahme des Unternehmers aus dem Markt, etwa durch Gewerbeuntersagung, verbinden sich beide Aufgabenstellungen der Prävention und der Durchsetzung; überhaupt finden sie sich vielfältig vermischt. Am deutlichsten wird ihre Verschiedenheit einerseits dort, wo auch ordnungsgemäß handelnde Unternehmer präventiven Maßnahmen (Zulassungserfordernissen, Überwachung etc.) unterworfen werden, und andererseits bei Maßnahmen der Erzwingung von konformem Verhalten in Bereichen, wo eine hoheitliche Marktüberwachung oder andere präventive Maßnahmen nicht vorgesehen sind. Übergreifende Zusammenschauen eines solchen Verbraucherverwaltungsrechts finden sich bislang nicht, auch wenn die Aufgabenstellung als solche dem deutschen öffentlichen Recht inzwischen präsent ist.[3]

---

[1] Siehe etwa *Leibe* (Hrsg.), Verbraucherschutz durch Information im Lebensmittelrecht (2010); *Leible/Meyer* (Hrsg.), Risiko als Thema des Lebensmittelrechts: *Risikobewertung *Risikomanagement *Risikokommunikation (2008).

[2] Etwa *Koschyk/Leible/Schäfer* (Hrsg.), Anlegerschutz und Stabilität der Finanzmärkte (2012).

[3] Das zeigen insbesondere die Vorträge von *Hellermann* und *Durner* bei der Jahrestagung 2010 der Vereinigung der deutschen Staatsrechtslehrer, VVDStRL 70 (2011) 366 ff. und 398 ff.

Erst recht hat sich die – gerade in jüngster Zeit sehr aktive[4] – Verwaltungsrechtsvergleichung bislang nicht übergreifend mit Fragen des Verbraucherschutzes durch die öffentliche Verwaltung beschäftigt. Studien finden sich insoweit vor allem für einzelne Sektoren[5] und betreffen – mit Ausnahme der Fragen nach einer verbraucherschützenden Finanzmarktaufsicht – vorwiegend Bereiche der Privatisierungsfolgenregulierung. Studien zu besonderen Instrumenten (wie die von *Pfeiffer* herausgegebene Studie zum Verbraucherinformationsrecht[6] oder den Band der Common Core Gruppe zu The Enforcement of Competition Law in Europe[7]) oder zu Institutionen (darunter insbesondere das skandinavische Modell des Ombudmanns[8]) beginnen gerade erst, sich allmählich zu ersten Zügen eines Gesamtbilds zu verdichten.

In jüngerer Zeit hat die politische Diskussion in Deutschland um die Wahrnehmung der gesamtstaatlichen Verantwortung für den Verbraucherschutz neue Fahrt aufgenommen, indem verschiedene Akteure die Einrichtung von sog. Marktwächtern vorgeschlagen haben.[9] Ziel ist dabei nicht die Einrichtung zusätzlicher Verwaltungsbehörden, vielmehr geht es – ursprünglich vor allem für den Finanzsektor – in erster Linie um eine Ergänzung des hoheitlichen Verbraucherschutzes nach dem Vorbild der sog. Watchdogs in den USA und dem Vereinigten Königreich: „Dazu sollen die Verbraucherorganisationen als zivilgesellschaftliche Marktwächter die Märkte aus Verbrauchersicht beobachten, unlautere Praktiken aufspüren, Hinweise systematisch erfassen und Missstände an die Aufsicht weitergeben. Mit Hilfe von Abmahnungen und Klagen setzen sie Verbraucherinteressen kollektiv durch.“[10] Verbunden ist das Marktwächterkonzept dann aber in zweiter

---

[4] Zu den Leitwerken zählen insbesondere die von *von Bogdandy/Cassese/Huber* herausgegebenen Bände III und IV des Handbuchs Ius Publicum Europaeum (2010, 2011); siehe ferner *Schneider* (Hrsg.), Verwaltungsrecht in Europa 1 und 2 (2007, 2009).

[5] Insbesondere die von *Keßler* und *Micklitz* herausgegebenen Bände zu Kundenschutz auf liberalisierten Märkten: Telekommunikation (2008), Kundenschutz auf liberalisierten Märkten – Personenverkehr, Eisenbahn (2008), Kundenschutz auf liberalisierten Märkten – Energie (2008) und Institutionelle Finanzmarktaufsicht und Verbraucherschutz (2010).

[6] *Pfeiffer* (Hrsg.), Rechtsvergleichende Untersuchung des Verbraucherinformationsrechts (2013).

[7] *Möllers/Heinemann* (Hrsg.), The Enforcement of Competition Law in Europe (2007).

[8] Siehe etwa *Kucsko-Stadlmayer* (Hrsg.), Europäische Ombudsmann-Institutionen – eine rechtsvergleichende Untersuchung zur vielfältigen Umsetzung einer Idee (2008) und *Haas*, Der Ombudsmann als Institution des Europäischen Verwaltungsrechts – zur Neubestimmung der Rolle des Ombudsmanns als Organ der Verwaltungskontrolle auf der Grundlage europäischer Ombudsmann-Einrichtungen (2012). In beiden Publikationen wird interessanterweise die Institution derart in den Mittelpunkt der Betrachung gerückt, daß die verbraucherschützende Funktion völlig zurücktritt. Anders hingegen bereits die knappen Bemerkungen in der Studie von *Schulze/Schulte-Nölke*, Rechtsvergleichende Untersuchung des verbraucherschützenden Lauterkeitsrechts der Mitgliedstaaten (2003), 86 f.

[9] Insbesondere die Konferenzdokumentation SPD-Bundestagsfraktion (Hrsg.), Verbraucherinteressen stärken – Marktwächter einführen, Konferenz der SPD-Bundestagsfraktion (2013) sowie schon zuvor den Entschließungsantrag der Fraktion BÜNDNIS 90/DIE GRÜNEN Finanzmarktwächter im Verbraucherinteresse einrichten, BT-Drs 17/6503 aus dem Jahre 2011. Chronologisch dazwischen die Publikation Verbraucherzentrale Bundesverband e.V. – vzbv, Finanzmarktwächter: Verbraucherbezogene Fehlentwicklungen und Missstände am Finanzmarkt systematisch und frühzeitig erkennen (2012).

[10] SPD-Bundestagsfraktion (Hrsg.), Verbraucherinteressen stärken – Marktwächter einführen, Konferenz der SPD-Bundestagsfraktion (2013), 5. Ähnliche Formuierungen finden sich in den übrigen in Fn. 9 genannten Quellen.

Linie mit verwaltungsrechtlichen Konsequenzen, nämlich der breiten Ausstattung staatlicher Behörden mit einem Mandat für den Verbraucherschutz durch dessen gesetzlicher Verankerung als Zweck der Verwaltungstätigkeit[11] und der Etablierung eines Anrufungsrechts des Marktwächters nach dem Vorbild der britischen *super-complaints* mit entsprechenden reaktionspflichten der angerufenen Behörde.[12]

Zu den Bereichen, welche für die Einführung von Marktwächtern in der politischen Diskussion genannt werden, zählt die sogenannte digitale Welt.[13] Unter diesem – nicht konturenscharfen und partiell metaphorischen – Begriff wird politisch primär der durch das Internet und die darauf aufsetzenden Anwendungen bis hin zu Web 2.0 und Web 3.0 gespannte Raum verstanden. Dieser Raum begründet nicht nur zahlreiche neue Chancen und Risiken für Verbraucher, sondern ändert – zumindest teilweise – auch dessen Rolle, weil er als Nutzer selbst Inhalte zur Verfügung stellt und damit kein reiner Abnehmer von Leistungen mehr ist.[14] Diese Rollenänderung hat sich etwa im Bereich des Urheberrechtsschutzes auch in neuen Schutzbedarfen niedergeschlagen, welche den Verbraucher sogar als Rechtsbrecher gegen als überzogen angesehenes Vorgehen der Rechteinhaber erfassen sollen.[15] Aus persönlichkeits- und datenschutzrechtlicher Sicht stellt der Verbraucher als Folge dieses Rollenwandels mit seinen Inhalten auch „sich selbst“ zur Verfügung, woraus sich für den Verbraucherschutz eine neue Variante des – im Ansatz wohlbekannten – Dilemmas eines Schutzes vor sich selbst ergibt.[16]

Aus verwaltungsrechtlicher Sicht hat auch die digitale Welt Anteil an der grundrechtlich abgesicherten Gewerbe- und Berufsfreiheit. Eine generelle Marktüberwachung findet daher – wie in der

---

[11] Entschließungsantrag der Fraktion BÜNDNIS 90/DIE GRÜNEN Finanzmarktwächter im Verbraucherinteresse einrichten, BT-Drs 17/6503, 3; SPD-Bundestagsfraktion (Hrsg.), Verbraucherinteressen stärken – Marktwächter einführen, Konferenz der SPD-Bundestagsfraktion (2013), 8 (Grußwort *Kelber*), 15 (Bericht über den Vortrag von *Thorun*). Vgl. auch Verbraucherzentrale Bundesverband e.V. – vzbv, Finanzmarktwächter: Verbraucherbezogene Fehlentwicklungen und Missstände am Finanzmarkt systematisch und frühzeitig erkennen (2012), 4.

[12] Entschließungsantrag der Fraktion BÜNDNIS 90/DIE GRÜNEN Finanzmarktwächter im Verbraucherinteresse einrichten, BT-Drs 17/6503, 4; Verbraucherzentrale Bundesverband e.V. – vzbv, Finanzmarktwächter: Verbraucherbezogene Fehlentwicklungen und Missstände am Finanzmarkt systematisch und frühzeitig erkennen (2012), 4 f.; SPD-Bundestagsfraktion (Hrsg.), Verbraucherinteressen stärken – Marktwächter einführen, Konferenz der SPD-Bundestagsfraktion (2013), 19 (Schlußwort Drobinski-Weiß). Zur Funktionsweise der *super-complaints* im Vereinigten Königreich siehe Office of Fair Trading (Hrsg.), Super-complaints – Guidance for designated consumer bodies (2003) sowie die kurzen Hinweise bei *Möllers/Heinemann* (Hrsg.), The Enforcement of Competition Law in Europe (2007) 460.

[13] Insbesondere SPD-Bundestagsfraktion (Hrsg.), Verbraucherinteressen stärken – Marktwächter einführen, Konferenz der SPD-Bundestagsfraktion (2013), 5.

[14] Die auf *Toffler* zurückgehenden Begrifflichkeiten *prosumer*, *produser* oder deren Übertragungsversuch ins Deutsche (Prosument) schillern teilweise, weil Sie auch als Kombination aus *professionel* und *consumer* gedeutet werden können. Darüber hinaus sind auch Konzepte zur (politisch verstandenen) Verbraucherpartizipation entwickelt worden, dazu etwa die Stellungnahme des Wissenschaftlichen Beirats Verbraucher- und Ernährungspolitik beim BMELV, Verbraucheröffentlichkeit im Netz – Möglichkeiten und Grenzen politischer Gestaltung (2013).

[15] Dazu etwa *Schmidt-Kessel*, Urheberrecht und Verbraucherschutz im Internet, in: *Leible/Ohly* (Hrsg.), Der Schutz des geistigen Eigentums im Internet, Mohr: Tübingen 2013, 223 ff.

[16] Für einen jüngeren Vorschlag etwa *Benninghoff*, Brauchen wir eine "Button"-Lösung für das Datenschutzrecht?, VuR 2013, 361 f.

analogen Welt – selbstverständlich nicht statt; § 4 TMG stellt dies für Deutschland mit klar. Das heißt freilich nicht, daß verwaltungsrechtliche Zuständigkeiten und Befugnisse in diesem Bereich nicht bestünden:[17] Zuständig und auch mit Eingriffsbefugnissen versehen sind vielmehr in Deutschland die Gewerbebehörden (als Sonderordnungsbehörden) und – für die nichtgewerblichen Unternehmen – die allgemeinen Ordnungsbehörden, soweit nicht Sonderzuständigkeiten für einzelne Sektoren und Berufsgruppen bestehen. Aufgabe dieser Behörden ist keine allgemeine Marktüberwachung, sondern die vielfach auf Information durch Dritte angewiesene Gewährleistung von Sicherheit und Ordnung; das schließt spezifisch verbraucherrechtliche Standards grundsätzlich mit ein.[18] Insoweit gilt wiederum für die digitale Welt nichts anderes als für die analoge. Auch die Ergänzung dieses klassichen Zuschnitts durch die Tätigkeit des Bundeskartellamts entspricht – trotz ordnungspolitischer Sonderfragen der digitalen Welt – dem Basisstandard administrativen Verbraucherschutzes in Deutschland.

Sonderstellungen beim administrativen Verbraucherschutz in der digitalen Welt nehmen in Deutschland die BNetzA und die Datenschutzbehörden ein. Bei der BNetzA wird in der digitalen Welt freilich die recht großzügig verstandene Befugnisnorm aus der Nummernverwaltung, § 67 I 1 TKG,[19] kaum einmal anwendbar sein, während die allgemeine Befugnisnorm des § 126 TKG trotz ihres Charakters als gewerbepolizeiliche Generalermächtigung[20] in ihrem Anwendungsbereich weitgehend auf Verstöße gegen das TKG beschänkt ist. Aus der digitalen Welt erfaßt dies im Wesentlichen den Ausschnitt des Verhältnisses zwischen dem Verbraucher und seinem Internetprovider sowie der weiteren in §§ 43a ff. TKG adressierten Akteure, nicht jedoch generell das Verhältnis zu anderen Unternehmern. Diese Beschränkung auf die Infrastrukturfragen der digitalen Welt entspringt der – partiell verfassungrechtlich vorgegebenen für die hier interessanten Fragestellungen aber unerheblichen – Trennung zwischen Telekommunikation und deren Inhalten. Hingegen erfaßt das Telemediengesetz in Umsetzung der e-commerce-Richtlinie 2000/31/EG zwar weite Teile der geschäftlichen Vorgänge in der digitalen Welt, es begründet jedoch keine Sonderzuständigkeiten und insbesondere keine zugunsten der BNetzA.[21]

Die Landesdatenschutzbehörden[22] stehen mit ihren vor allem in § 38 BDSG beschriebenen Aufgaben und Befugnissen im Mittelpunkt der rechtlichen Erfassung der digitalen Welt, indem sie die Datenverarbeitung, -nutzung und -erhebung durch nicht-öffentliche Stellen (und diesen gleichgestellte öffentliche Stellen), also gleichsam die zweite Währung und das Schmiermittel der digitalen

---

[17] Leicht mißverständlich daher SPD-Bundestagsfraktion (Hrsg.), Verbraucherinteressen stärken – Marktwächter einführen, Konferenz der SPD-Bundestagsfraktion (2013), 8 (Bericht Beitrag *Billen*).

[18] Einer Sanktionierung dieser Standards durch einen Straf- oder Ordnungswidrigkeitentatbestand bedarf es dazu nicht; jedoch ist nach klassischer Lesart nicht jede verbraucherschützende Norm auch zugleich Teil der öffentlichen Sicherheit; es bedarf danach vielmehr zumindest auch eines öffentlichen Interesses an polizeilichem oder ordnungsbehördlichem Schutz. Ob diese Einschränkung für verbraucherschützende Normen angesichts von § 2 UKlaG heute noch zutrifft, darf man bezweifeln.

[19] Dazu etwa OVG Münster MMR 2009, 286 und OVG Münster NJW 2008, 3656 (jeweils unerlaubte Telephonwerbung).

[20] OVG Münster, Urt. v. 30. 6. 2009 – 13 A 2069/07, Rn. 81; Geppert/Schütz/Meyer-Sebastian § 126 TKG Rn. 4.

[21] Vgl. §§ 4 ff. TMG. Vgl. etwa die bayerische Zuständigkeitszuweisung in § 4 III Verordnung über Zuständigkeiten im Ordnungswidrigkeitenrecht (Verordnung nach § 36 II 1 OWiG).

[22] In Bayern zusätzlich der TÜV für Aspekte der technischen Datensicherheit.

Welt kontrollieren. Ihre Unabhängigkeit von der hierarchisierten Staatsverwaltung ist europarechtlich vorgeschrieben.[23] Die Befugnisse der Landesdatenschutzbehörden sind freilich weitgehend auf die Durchsetzung der materiellen Standards des BDSG und anderer Datenschutzvorschriften beschränkt,[24] so daß auch hier keine Überwachung unternehmerischer Aktivitäten in der digitalen Welt insgesamt stattfindet. Daneben bleiben die Gewerbebehörden oder – wie § 38 VI BDSG nur unzureichend deutlich macht – die Sonderordnungsbehörden des betreffenden Sektors zuständig und befugt. Hinzu kommt, daß die Befugnisse der Landesdatenschutzbehörden praktisch mit der Untersagungsvefügung und der Verhängung von Bußgeldern enden, während die hoheitliche Anordnung des Ausscheidens aus dem Markt weiterhin Sache der (Sonder-)Ordnungsbehörden ist.[25]

Zu den Kernfragen der digitalen Welt gehören – das wurde oben schon angedeutet – der Umgang mit Urheberrecht und Datenschutz.[26] Beide Bereiche bilden Referenzgebiete der digitalen Welt, wie sie – jedenfalls aus deutscher Perspektive – hinsichtlich der Zwecksetzungen und der Verwaltungsstrukturen kaum unterschiedlicher sein könnten: Das Urheberrecht ist als Schutzinstrument zugunsten der Urheber (auch gegen Intermediäre wie Verlage) entstanden und hat verbraucherrechtliche Relevanz in der digitalen Welt vor allem dadurch erlangt, daß sich aus der Verfolgung von durch Privatleute im Internet begangenen Rechtsverletzungen ein teilweise als „Abzocke“ stigmatisiertes Geschäftsmodell entwickelt hat.[27] Unterhalb der Schwelle des Straf- und Ordnungswidrigkeitenrechts sind in Deutschland jedoch keine gesonderten Behörden allgemein für diesen Bereich und Fragenkreis zuständig und zwar weder zur Durchsetzung des Urheberrechts[28]

---

[23] EuGH, Urt. v. 9. 3. 2010, C-518/07, Rn. 31 ff.

[24] Vgl. § 38 V BDSG

[25] Das wird bereits aus der Unterrichtungsbefugnis nach § 38 I 6 BDSG deutlich. Damit hat das Datenschutzrecht teil an der allgemeinen Problematik des Vollzugs verbraucherschützenden Ordnungsrechts durch die unteren Verwaltungsbehörden, deren Spitzen als Wahlbeamte sich nicht selten in Situationen institutioneller Befangenheit (als Wirtschaftsförderer und Rechtsdurchsetzer gelichermaßen) befinden. Anders läßt es sich kaum erklären, daß die Städte Hamburg und Berlin bislang gegen die deutschen Tochterunternehmen großer internationaler Akteure des Web 2.0 nicht mit den Mitteln des § 35 GewO vorgegangen sind, obwohl deren Unterstützung für die datenschutzrechtswidrigen Praktiken der jeweiligen Mutterunternehmen offensichtlich ist.

[26] In diesem Sinne auch SPD-Bundestagsfraktion (Hrsg.), Verbraucherinteressen stärken – Marktwächter einführen, Konferenz der SPD-Bundestagsfraktion (2013), 8 (Grußwort *Kelber*) sowie 22 (Vortrag *Tack*).

[27] Siehe nochmals *Schmidt-Kessel*, Urheberrecht und Verbraucherschutz im Internet, in: *Leible/Ohly* (Hrsg.), Der Schutz des geistigen Eigentums im Internet, Mohr: Tübingen 2013, 223 ff. m.w.N. Die vom Ministerium für den Ländlichem Raum und Verbraucherschutz Baden-Württemberg sowie vom vzbv erhobene Forderung, die Nutzerinteressen als schutzwürdiges Ziel im Urheberrechtsgesetz zu erfassen (s. vzbv, Verbraucherschutz im Urheberrecht – Positionspapier des Verbraucherzentrale Bundesverbandes [2011] sowie Ministerium für den Ländlichem Raum und Verbraucherschutz Baden-Württemberg/vzbv, Urheberrecht 2.0 – Wo bleiben die Verbraucher. Positionspapier zur Reform des Urheberrechts), hat sich bislang nicht realisieren lassen. Der Gesetzgeber ist stattdessen im Gesetz gegen unseriöse Geschäftspraktiken (BGBl. 2013 I 3714) den Weg gegangen, das Geschäftsmodell und dessen Funktionsbedingungen direkt anzugehen (Begrenzung des Abmahnungsstreitwerts und Begründung eines Sondergerichtsstands für Klagen gegen Verbraucher durch §§ 97a, 104a UrhG und § 51 GKG).

[28] Immerhin ergeben sich aus §§ 111b, 111c UrhG und Artt. 4 ff. Verordnung (EG) Nr. 1383/2003 des Rates vom 22. Juli 2003 über das Vorgehen der Zollbehörden gegen Waren, die im Verdacht stehen, bestimmte Rechte geistigen

noch zum Schutze von Verbrauchern gegen überzogene Durchsetzungsmaßnahmen.[29] Ohne Verletzung von Rechtsnormen im öffentlichen Interesse kommt auch ein Einschreiten der allgemeinen Ordnungsbehörden auf der Basis der polizeilichen Generalklauseln regelmäßig nicht in Betracht. Hingegen ist das Datenschutzrecht in Deutschland gerade als Schutzinstrument zugunsten Privater entstanden und dazu auch mit wirkmächtigen Datenschutzbehörden ausgestattet worden. Die Schwächen des Datenschutzes liegen – außer in der unglücklichen Verknüpfung von Kundendatenschutz und Schutz vor dem Staat – in seiner Begrenzung auf den Bereich der Datenverarbeitung selbst, welcher bei den kombinierten Geschäftsmodellen der digitalen Welt zu kurz greift, und in seiner begrenzten internationalen Durchsetzbarkeit. Beide Referenzgebiete zusammengenommen ergibt sich ein gutes Bild von Möglichkeiten und Grenzen von Verbraucherschutz durch die öffentliche Verwaltung in der digitalen Welt.

Die im folgenden zunächst unternommene Marktanalyse[30] deutet einen zusätzlichen Zusammenhang zwischen den beiden hier gewählten Ausschnitten der digitalen Welt an: Datenverwertung und Verwertung von Urheberrechten sind Geschäftsmodelle, die gerade bei den großen Akteuren im Markt zusammentreffen und immer stärker zusammenwachsen. Wollte man bestimmte Akteure aus der digitalen Welt etwa einem allgemeinen Zulassungserfordernis unterwerfen, müßte dieses wohl sinnvollerweise beide Felder umfassen. Zugleich hat die Marktanalyse damit ordnungspolitischen Handlungsbedarf ergeben. Verbraucherpolitisch muß die Marktanalyse hingegen viele Schutzbedarfe offen lassen, die sich nicht aus dem Verhalten der großen Akteure am Markt ergeben. Gerade die problematischen Geschäftsmodelle welche sich der Mittel der Urheberrechtsdurchsetzung bedienen, werden nicht von den großen Playern betrieben.

Die nachfolgende rechtsvergleichende Untersuchung nimmt vier Rechtsordnungen in den Blick, welche durch ihre Marktsituation und durch ihre Verwaltungsstrukturen besondere Erkenntnisse zur Fortentwicklung administrativen Verbraucherschutzes für die digitale Welt in Deutschland erwarten lassen. Das gilt zunächst für die USA, deren Verbraucherschutzrecht ohnehin primär durch hoheitlich handelnde Akteure geprägt ist; das Land verfügt über eine starke Tradition des *copyright* und über eine deutlich weniger ausgeprägte *privacy policy*. Großbritannien, Frankreich und Schweden sind hingegen Mitglieder der europäischen Union, was verbraucher- datenschutz- und urheberrechtlich gewisse Gleichläufe erwarten läßt. Administrativ sind die Traditionen jedoch höchst unterschiedlich, weil die französische Verwaltungstradition die Mutter der klassisch-kontinentalen und hoheitlich orientierten Strukturen ist, während englische Behörden bisweilen ohne Mitwirkung der Gerichte nichteinmal vollstreckbare Titel kreieren können und die Emanzipation des englischen Verwaltungsrechts vom Privatrecht insoweit nach wie vor nicht völlig abgeschlossen ist.[31] Das schwedische Recht verfügt mit der Verbraucherschutzagentur (*Konsumentverket*)

Eigentums zu verletzen, und die Maßnahmen gegenüber Waren, die erkanntermaßen derartige Rechte verletzen Zurückhaltungs-, Beschlagnahme-, Einziehungs- und Vernichtungsbefugnisse der Zollbehörden hinsichtlich urheberrechtswidriger Vervielfältigungsstücke, denen freilich vor allem die Funktion einer vorbeugenden Sicherung der Zwangsvollstreckung der zivilen Ansprüche zukommt. Rechtsmittel gegen die Anordnung richten sich in Deutschland nach den Regeln des Verfahrens in Ordnungswidrigkeitssachen, s. § 111b VII UrhG.

[29] In der Vergangenheit sind Versuche, die Gewerbebehörden und – für die anwaltlichen Abmahnungen – die Rechtsanwaltskammern zum Schutz von verbrauchern zu aktivieren gescheitert.

[30] Siehe unten *Held/Germelmann*, Marktanalyse.

[31] Siehe *Kleve/Schirmer*, England und Wales, in: Schneider (Hrsg.), Verwaltungsrecht in Europa (2007), 35, 63 ff.

und ihrem Direktor, dem Verbraucherombudsmann (*Konsumentombudsmannen, KO*) eine für die nordischen Staaten charakteristische Verwaltungs- und Befugnisstruktur, welche eine sehr starke Position des Ombudmanns mit einer konsensorientierten Lösungssuche verbindet.

Eine rechtsvergleichende Untersuchung des administrativ organisierten Verbraucherschutzes für die Bereiche Datenschutz und Urheberrecht setzt zunächst ein gewisses Grundverständnis der Regelungsstrukturen der materiellen Standards im Datenschutz- und Urheberrecht voraus. Maßgebende Gesichtspunkte zu dieser Frage sind etwa die grundrechtliche Verankerung des Datenschutzrechts, der Bestand und die Grundstruktur seiner allgemeinen Regeln sowie die Sonderregeln für die digitale Welt. Für das Urheberrecht zentral ist die Frage nach der grundsätzlichen Einordnung der Rechtsposition selbst: Folgt die Rechtsordnung dem Copyright-System oder der Idee eines Urheberpersönlichkeitsrechts? Zudem auf nach Sonderregeln für die digitale Welt und den Instrumenten ihrer Durchsetzung zu schauen.

Die hier gebotene Untersuchung von Behördenstrukturen und Behördenaktivitäten läßt sich gut in einer Matrixstruktur fassen: Die eine Dimension dieser Matrix, die der Behördenstruktur, fragt nach dem Verbraucherschutz durch öffentliche Verwaltung im Allgemeinen, dem Vorhandensein einer allgemeinen Administration für die digitale Welt sowie nach Sonderbehörden für den Datenschutz und dem behördlichen Schutz des Urheberrechts respective dem behördlichen Eingreifen zum Schutz vor übermäßiger Urheberrechtsdurchsetzung. Für die andere Dimension ist zunächst nach dem jeweiligen behördlichen Grundverständnis und sodann nach der Behördenstruktur und den Zuständigkeiten sowie nach Befugnissen und informellen Verfahrensweisen zu fragen; weitere Punkte sind die Möglichkeiten der Sanktionierung von Fehlverhalten, die Frage nach Spielräumen für eine eigene Politik der Behörde sowie Besonderheiten grenzüberschreitender Durchsetzung.

B. Analyse des digitalen Medienmarkts in Frankreich, Schweden, Großbritannien und den USA

I. Einleitung

Um zu verstehen, wie die digitalen Märkte in verschiedenen Referenzländern strukturiert sind, sollen diese Märkte im Folgenden analysiert werden. Der Schwerpunkt liegt hierbei auf digitalen Angeboten, deren Geschäftsmodell auf der Weitergabe von Daten ihrer Nutzer liegen, und Angeboten, die auf der Verwertung von Urheberrechten beruhen. Die Analyse dieser Angebote gibt einen Überblick über mögliche Problemfelder in der digitalen Welt, die Gegenstand der Beobachtung und Analyse durch Marktwächter sein können.

1. Die Internetpenetration in den Vergleichsländern als Referenzgröße

Die Internetverbreitung ist in den Ländern Frankreich (69%), Großbritannien (68%) und Deutschland (65%) ähnlich hoch (hier Referenzjahr 2011). Eine Ausnahme stellt Schweden dar, wo die Internetverbreitung 2011 bereits bei 90% lag[1]. Betrachtet man die monatliche Nutzungszeit im Internet, sticht vor allem Großbritannien hervor, wo die Nutzer monatlich 34,7 Stunden im Internet verbrachten. Deutsche, schwedische und französische Nutzer kommen dagegen nur auf 24 Stunden pro Monat.[2]

Unter den fünf am meisten genutzten Seiten befinden sich in allen vier Ländern die Suchmaschine Google, das soziale Netzwerk Facebook und die Videoplattform YouTube. Ferner ist in allen Ländern mindestens eine, meist länderspezifische, Kleinanzeigenseite unter den Top 15 zu finden. Neben diesen globalen Playern sind in jedem Land lokale Nischenanbieter zu finden, deren Einfluss im Vergleich zu den großen Anbietern jedoch eher als gering einzuschätzen ist.

2. Methodik und Datenbasis zur Internetnutzung generell

Zur Analyse der in den einzelnen Ländern am häufigsten genutzten Internetseiten wurde die Webanalytics Seite Alexa.com verwendet. Diese zieht ihre Rankings aus einem globalen Traffic Panel bestehend aus allen Internetnutzern. Die ausgegebenen Ranks stellen einen Verhältniswert zu anderen Seiten in Relation zur durchschnittlichen Anzahl täglicher Nutzer und der Anzahl der Pageviews des letzten Monats dar.[3] Für jedes Land sind ergänzende Rankings verfügbar, die an den entsprechenden Stellen mit aufgenommen wurden. Zur besseren Vergleichbarkeit der Länder wurde jedoch vorwiegend das alexa.com Ranking als Datenbasis verwendet. Da auf alexa.com allerdings immer nur Werte für Gesamtseiten ausgegeben sind, können bei Unternehmen teilweise keine nach Unterseiten aufgeschlüsselten Informationen bekannt gegeben werden. So sind für google.com beispielsweise keine Rankingwerte von google+ und google books verfügbar. Außerdem erhebt die folgende Darstellung keinen Anspruch auf Vergleichbarkeit der Daten der einzelnen Unteraspekte zwischen den Ländern, da die meisten Daten aus länderspezifischen und

[1] Europäische Kommission 2011, S. 51

[2] comScore (2011).

[3] Alexa Internet (2013c).

nicht europaweit vergleichenden Studien stammen und die Untersuchungszeiträume voneinander abweichen.

II. Frankreich

1. Mediensystem und Bevölkerung

Nach Schätzungen des IMF leben in Frankreich im Jahr 2013 63,704 Mio. Menschen.[4] Davon nutzen 79,6 % das Internet.[5] In 2013 wurden 25,1 Mio. ***mobile Internetnutzer*** verzeichnet. Besonders mobile Fotodatenbanken erfreuen sich zunehmender Beliebtheit (2,5 Mio Nutzer im Juli 2013, davon 1,8 Mio. Instagram-Nutzer)[6]. Mit dem Apple iPad gingen 2012 2,3 Mio. Franzosen online.[7]

2. Generell genutzte Webseiten und mobil genutzte online Angebote

Die fünf von den französischen Internetnutzern am häufigsten besuchten Seiten ähneln den weltweiten Gewohnheiten. Mit google.fr (Platz 1, global Platz 28), google.com (Platz 2, global Platz 1), facebook.com (Platz 3, global Platz 2), youtube.com (Platz 4, global Platz 3) und wikipedia.org (Platz 5, gobal Platz 6) sind die beliebtesten globalen Seiten auch in Frankreich auf den vorderen Rängen. Eine Ausnahme stellt naturgemäß die länderspezifische Google Seite dar. Mit yahoo.com (Platz 8) und live.com (Platz 11) finden sich zwei weitere ***Suchmaschinen*** unter den fünfzehn beliebtesten Seiten. Der Suchdienst commentcamarche.fr, auf dem technische Fragen beantwortet werden, hat seinen Unternehmenssitz in Frankreich und rangiert auf Platz 15. Facebook auf Platz drei ist als einziges ***soziales Netzwerk*** unter den Top 10 der beliebtesten Internetseiten vertreten, linkedin.com und twitter.com folgen erst auf Platz 12 und 14. Unternehmen, deren Geschäftsmodell zumindest zum Teil auf der ***Onlineverwertung von Urheberrechten*** basiert, sind youtube.com (Platz 4) und amazon.fr (Platz 7). Die beliebtesten Seiten mit einem ***Unternehmenssitz in Frankreich*** finden sich mit leboncoin.fr (Onlineportal für Privatanzeigen), orange.fr (Telekommunikationsanbieter) und free.de (Telekommunikationsanbieter) auf Platz 6, 9 und 10.[8] Seit 2008 hat sich insbesondere die Stellung von Facebook (2008 nicht unter den Top 10) und YouTube (2008 auf Platz 10) verbessert.[9] Dies ist durch die steigende Beliebtheit sozialer Netzwerke und Internetvideos zu erklären.

Siehe Anhang 1: Generell genutzte Seiten Frankreich

Bei den ***mobil genutzten Seiten*** sieht die Lage in Frankreich ähnlich wie bei der stationären Nutzung aus, auch hier rangieren Google (1), YouTube (2) und Facebook (3) ganz vorne. Mit der Marke iTunes (4) von Apple und Apple selbst (10) auf den vorderen Plätzen des Rankings der

[4] International Monetary Fund (2013).

[5] Internet World Stats (2013a).

[6] Mediametrie (07.08.2013), S. 1.

[7] eMarketer (März 2013).

[8] Alexa Internet (2013c).

[9] Hans-Bredow-Institut für Medienforschung an der Universität Hamburg (2009), S. 317.

mobil genutzten Seiten wird jedoch ersichtlich, dass es auch spezifische Dienste gibt, die vorwiegend mobil genutzt werden.[10]

3. Nutzung von Online-Angeboten, die Daten verwerten

80% der französischen Internetnutzer sind in einem sozialen Netzwerk angemeldet,[11] 25.6 Mio. bei facebook.com,[12] womit Facebook in Frankreich mit Abstand der Marktführer im Bereich sozialer Netzwerke ist. Der zweitbeliebteste Anbieter der privaten sozialen Netzwerke Skyrock kommt nur auf ein Viertel der Nutzerzahlen von Facebook. Skyrock ist ein französisches Netzwerk, das hauptsächlich in 10 Ländern aktiv ist; 34,6% seiner monatlichen Seitenaufrufe stammen aus Frankreich, 21,1 % aus Indien. Das Netzwerk hat im letzten Jahr jedoch stark an Seitenaufrufen verloren.[13] Nach Skyrock sind Twitter, Linkedin, Viadeo (professionelles Netzwerk aus Frankreich), Trombi.com (französische Suchmaschine für Schulfreunde), Trumblr.com (Bloggingplattform), Copain d´avant (französische Suchmaschine für Schulfreunde) und Badoo (soziales Netzwerk) die am häufigsten genutzten sozialen Netzwerke in Frankreich.[14] Nach Alexa.com rangieren auch noch die französische Bloggingplattform over-blog.com unter den beliebtesten Seiten der Kategorie soziale Netzwerke.[15] Twitter erhielt in Frankreich in den letzten Jahren einen erstaunlichen Nutzerzuwachs (Nov. 2012, 5,5 Mio. Besucher) und ist bei der Nutzung vom stationären PC/Laptop insbesondere in der Altersgruppe über 55 Jahren sehr stark vertreten. Im Vergleich zu anderen europäischen Ländern kommt der Nutzung von sozialen Netzwerken über den mobilen Zugang in Frankreich eine hohe Bedeutung zu. Vor allem jüngere Nutzer besuchen soziale Netzwerke mit ihrem Mobiltelefon. Facebook ist das beliebteste mobil genutzte Netzwerk (11.2 Mio. Nutzer), gefolgt von Twitter (1.5 Mio) und Myspace (0,7 Mio).[16]

4. Nutzung von Online-Angeboten, die Urheberrechte verwerten

33,9 Mio. der Internetnutzer in Frankreich haben im Juni 2013 mindestens ein Video online angeschaut, mit einer durchschnittlichen Dauer eines Videos von 3 Minuten und 45 Sekunden. Bei den 15-24-Jährigen ist die Situation noch verstärkt, sie schauen 10 Stunden im Monat Onlinevideos. Die fünf am häufigsten genutzten Videoseiten in Frankreich sind: Youtube, Dailymotion, TF1/Wat, Google und France Television. Wobei YouTube in diesem Zusammenhang eine herausragende Stellung einnimmt. Die Seite erzielt monatlich 25,6 Mio. Unique Visitors (Dailymotion auf Platz 2 nur 8,5Mio.), es werden 1,5 Mrd. Videos gesehen (bei Dailymotion nur 127,2 Mio.) und die gesamte auf dieser Seite verbrachte Zeit beträgt 69,4 Mio. Stunden (bei TF1/ Wat, die auf Platz zwei der verbrachten Zeit liegt lediglich 12 Mio. Stunden).[17] Unter den Musikdiensten hat neben Ama-

[10] Mediametrie (07.08.2013), S. 3.

[11] Mediametrie (04.07.2013).

[12] Internet World Stats (2013a).

[13] Alexa Internet

[14] eMarketer (April 2013).

[15] Alexa Internet (2013c).

[16] eMarketer (Jan. 2013).

[17] Mediametrie (14.08.2013).

zon.fr (Platz 7) und apple.com (Platz 48) vor allem der französische Musikstreaminganbieter deezer.com (Platz 54) mit einer langen Verweildauer von 6,09 Minuten pro Tag (Amazon und Apple haben nur 3,40 Minuten) eine relevante Stellung.

5. Zusammenfassung und Diskussion der digitalen Welt in Frankreich

Die untersuchten Online-Angebote machen deutlich, dass der digitale Markt in Frankreich durch US-amerikanische Anbieter dominiert wird. Insbesondere Facebook und YouTube haben eine herausragende Stellung inne, während lokale Wettbewerber wie Skyrock an Bedeutung verlieren. Besonders auffällig ist, dass französische Anbieter, deren Geschäftsmodell auf der Weitergabe von persönlichen Daten basiert, eine zu vernachlässigende Stellung im Markt einnehmen.[18] Neben diesem – für Netzwerke allerdings typischen – Konzentrationseffekt fällt die starke und zunehmende Bedeutung der mobilen Zugänge zur digitalen Welt auf, was wegen des hohen Personalisierungsgrades von mit mobilen Endgeräten abgerufenen Daten nach neuen Problemlösungen verlangen kann. Hier ist beispielsweise an Themen wie Datensicherheit und Datenschutz zu denken.

Mit Fragen der Urheberrechtsverletzung beschäftigt sich in Frankreich die Behörde HADOPI (Haute Autorité pour la diffusion des oeuvres et la protection des droits sur l´internet). Sie überwacht die Einhaltung von Urheberrechten im Internet und versendet Mahnungen an Internetnutzer bei Verletzung der entsprechenden Rechte. Die Anwendung des „three strikes and you´re out" Prinzips, das Personen den Zugang zum Internet sperrt, sofern diese dreimal das Urheberrecht verletzt haben, steht jedoch stark in der Kritik.[19]

III. Schweden

1. Mediensystem und Bevölkerung

Von den zu untersuchenden Ländern ist Schweden mit einer Bevölkerung von 9,597 Mio. Personen das bevölkerungskleinste Land.[20] Allerdings ist die Internetpenetration in Schweden mit 92,7% im Jahr 2013 am höchsten.[21] Die Zahlen zur mobilen Nutzung des Internets in Schweden variieren je nach Quelle erheblich. Nach einer Erhebung des Münchner Kreises, lag 2011 die Nutzung des ***mobilen Internets*** bei 58%.[22] 2013 liegt die Rate wesentlich höher. Nach IAB Schweden und SWEDMA bei 79%, nach eMarketer bei 61%. Nichtsdestotrotz sind die Quellen sich einig, dass Schweden als führendes Land bei der Smartphone-Adaption gesehen werden kann.[23] Trotz der enormen Internetverbreitung in Schweden ist es bemerkenswert, dass 2009 die Zeitung immer noch das am häufigsten genutzte Medium der Schweden war.[24] Das traditionelle

[18] Lediglich overblog.com, viadeo.com und skyrock.com rangieren als soziale Netzwerke unter den acht beliebtesten ihrer Kategorie und bei Suchmaschinen nimmt nur commentcamarche.net eine bedeutende Position ein.

[19] Reporters without Borders (März 2012). Dazu noch unten *Wichmann,* Länderbericht Frankreich, 1.a.bb) 4) (b).

[20] International Monetary Fund (2013).

[21] Internet World Stats (2013a).

[22] Münchner Kreis (2011).

[23] Zitiert nach NewMedia TrendWatch (2013).

[24] Nord (2011), S. 16.

Mediensystem in Schweden wird von der Bonnier-Gruppe dominiert. Einem Unternehmen, das in allen klassischen Medien in Schweden und dem Ausland aktiv ist und derzeit auch versucht, sein online Geschäft auszubauen.[25]

2. Generell genutzte Webseiten und mobil genutzte online Angebote

Das stark ***nachrichtenorientierte Mediennutzungsverhalten*** der Schweden spiegelt sich auch in den von ihnen am häufigsten besuchten Seiten wieder. Drei der fünf am meisten besuchten Anbieter gleichen der globalen Nutzung (facebook.com (3), google.com (2) und youtube.com (4)), hinzu kommt google.se auf Platz 1, was den Nutzungsmerkmalen der anderen untersuchten Ländern entspricht. Auf Platz 5 rangiert allerdings ein rein schwedischer Anbieter, die Internetseite des Abendblatts, aftonbladet.se. Mit expressen.se (12) findet sich ein weiterer rein schwedischer Nachrichtenanbieter unter den Top 15 Seiten. ***Suchmaschinen***, die sich durch die Weitergabe von personenbezogenen Daten finanzieren, sind neben Google die Folgenden: yahoo.com (8), live.com (10).[26]

Auf Platz 13 ist mit piratbay.sx ein ***Filesharing (BitTorrent-)Netzwerk***, das von der schwedischen Piratenpartei gegründet wurde, aufzufinden und auf Platz 14 befindet sich mit imdb.com (The Internet Movie Database von Amazon) ein Informationssuchdienst für Filme. Mit blocket.se schafft es eine schwedische Kleinanzeigenseite auf Platz 7.

Die in 2012 am meisten über ***mobiles Internet*** durchgeführten Aktivitäten sind das Versenden von Emails, das Lesen auf Nachrichtenseiten, das Besuchen von sozialen Netzwerken, die Nutzung von GPS Apps und auf Platz fünf das Anhören oder Downloaden von Spielen, Bildern, Filmen oder Musik. [27] Anhand dieser Daten wird deutlich, dass die Aktivitäten aus dem stationären Internet auch im mobilen Internet durchgeführt werden, jedoch zusätzlich ein Fokus auf dem Versenden von Emails und der Nutzung von GPS basierten Services liegt.

3. Nutzung von Online-Angeboten, die Daten verwerten

54% der Personen zwischen 16-74 Jahren nutzten 2011 soziale Netzwerke. In der Altersgruppe der Schweden zwischen 16-24 Jahren sind es 90%. Professionelle soziale Netzwerke werden von 10% der Bevölkerung genutzt.[28] Zu ihnen gehören unter den Top 15 Seiten neben Facebook, das von 4,95 Mio. Personen genutzt wird[29], linkedin.com (9) und twitter.com (15). Google+ wird von 0,5 Mio. Schweden genutzt.[30] Weitere häufig genutzte soziale Netzwerke sind folgende US-Amerikanischen Seiten: die Blogingplattform tumblr.com, die Pinnwandseite printrest.com und der soziale Nachrichtenaggregator reddit.com, bei dem registrierte Nutzer Nachrichtenlinks oder Textbeiträge einstellen können, welche dann von anderen Benutzern bewertet werden. 40% der

[25] Hans-Bredow-Institut für Medienforschung an der Universität Hamburg (2009), S. 581 f. ff.

[26] Alexa Internet (2013c).

[27] Statistics Sweden (16.01.2013).

[28] Statistic Sweden zitiert nach NewMedia TrendWatch (2013).

[29] Internet World Stats (2013a).

[30] Plus Demographics (2013).

schwedischen Bevölkerung nutzt soziale Netzwerke vom Mobiltelefon aus und über 40% der Männer und 30% der Frauen verwenden dabei auch GPS Anwendungen. Der Anteil der Nutzer von sozialen Netzwerken bei den 16-24-Jährigen liegt wesentlich höher (79%) und bei den 65-74-Jährigen wesentlich niedriger (7%).[31] Unter den Suchmaschinen sind in Schweden die üblichen internationalen Anbieter vertreten, ergänzend bieten die werbefinanzierten schwedischen Seiten hitta.se (Platz 18) und eniro.se (Platz 24) Adressen, Wegbeschreibungen und Telefonnummern.[32]

4. Nutzung von Online-Angeboten, die Urheberrechte verwerten

2013 wurden täglich 25 Mio. Videos über YouTube angeschaut. Das enorme Wachstum des Videokanals lässt sich unter anderen daran beziffern, dass es in 2008 nur 1,2 Mio. waren, was einem Wachstum von 1983,3% entspricht.[33] Der aus Schweden stammende Musikstreamingdienst Spotify erfreut sich starker Beliebtheit unter den Schweden. So handelt es sich bei Spotify um die Marke mit den meisten Facebook-Fans in Schweden[34]. Unter den 100 beliebtesten Seiten in Schweden befinden sich 12 Videoanbieter, was die hohe Relevanz von online Videos bei den Schweden untermauert. Besonders beliebte Bilderplattformen sind instagram.com (27), imgur.com (32) und flickr.com (65).

5. Zusammenfassung und Diskussion der digitalen Welt in Schweden

Die Bonnier-Gruppe ist ein gutes Beispiel dafür, dass die klassischen Anbieterstrukturen im Mediensystem nicht auf den digitalen Bereich übertragbar sind und somit auch erhebliche Anpassungen in den für den Umgang mit Medien relevanten Gesetzen notwendig sind. Mit einem Umsatz in Höhe von 2,5 Mio. USD im Jahr 2005 (der zweitgrößte Medienanbieter MTG/Viaset lag lediglich bei 1,2 Mio Euro) hält die Bonnier-Gruppe eine marktbeherrschende Stellung in Schweden[35]. Allerdings ist unter den 25 in Schweden am meisten genutzten Internetseiten nur expressen.se als Seite der Bonnier-Gruppe zu finden[36]. Besonders auffällig bei der schwedischen Internetnutzung ist die Tatsache, dass sich zwei Nachrichtenseiten und drei Videoplattformen unter den Top 15 befinden, was darauf hindeutet, dass die Adaption von Inhalten, die traditionell über andere Medienkanäle genutzt wurden, in Schweden schon weit fortgeschritten ist. In Bezug auf die Internetnutzung muss Schweden deshalb eine besondere Rolle zugewiesen werden, das Land kann als Early Adopter für Trends in der Mediennutzung gesehen werden. Bereits seit 2003 sind Dienstleitungen des Staates (Steuererklärung etc.) online verfügbar.[37] Die schwedischen E-Government Services sind auf Platz 7 weltweit.[38] Auffällig ist auch, dass es unter den 100 meist genutzten Seiten nicht ein einziges genuin schwedisches soziales Netzwerk gibt. Auch bei der

[31] Statistics Sweden (16.01.2013).

[32] Alexa Internet (2013c).

[33] eMarketer (Feb. 2013).

[34] Socialbakers (2013).

[35] Hans-Bredow-Institut für Medienforschung an der Universität Hamburg (2009), S. 581 f. ff.

[36] Alexa Internet (2013c).

[37] Geens (April 2013).

[38] UN Public Administration Programme (2012).

Einschätzung dieses Befunds muss der inhärente Vorteil großer internationaler Netzwerke berücksichtigt werden. Ähnlich wie in anderen Ländern dominieren auch in Schweden Google (google.se, google.com und google.uk, Plätze 1, 2, 94), Yahoo (yahoo.com) und Microsoft (live.com und bing.com, Platz 9 und 16) den Markt der Suchmaschinen und somit den Markt der Weitergabe von personenbezogenen Daten, die wiederrum ein zielgruppengerechtes Werben ermöglichen. Da diese Dienste ihren Sitz im Ausland haben, unterliegen sie nicht der schwedischen Jurisdiktion.[39] Hervorzuheben ist die Tatsache, dass im Bereich sozialer Netzwerke und Suchmaschinen internationale US-amerikanische Unternehmen den schwedischen Internetmarkt dominieren. Bei den Videoplattformen wird in Teilen und bei Kleinanzeigen vorwiegend auf nationale Anbieter zurückgegriffen. Blocket.se (7) als Kleinanzeigenportal ist Ebay mit seiner schwedischen Seite tradera.com auf Platz 25 stark überlegen. Auch die geringe Beliebtheit von amazon.com (Platz 21) im Gegensatz zu den anderen Ländern ist bemerkenswert.
In Schweden ist Filesharing sehr beliebt und in kleineren Maßen wird es nicht bestraft, da die schwedische Rechtsprechung davon ausgeht, dass die Privatsphäre von Personen schützenswerter als das Urheberrecht von Personen ist.[40] Der hohe Stellenwert der Privatsphäre in Schweden wird auch daran deutlich, dass die schwedische Datenschutzbehörde im Juni 2013 die Verwendung aller Google Cloud Services (z.B. Google Kalender, Email etc) für schwedische Regierungseinrichtungen untersagt hat, da Google bei diesen Diensten ein zu weites Nutzungsrecht von Daten einräumt und die Weitergabe der Daten an Subunternehmer nicht klar ersichtlich ist.[41]

IV. Großbritannien

1. Mediensystem und Bevölkerung

Nach Schätzungen des IMF leben in Großbritannien 63,758 Mio. Personen.[42] Die Internetverbreitung liegt mit 83,6% in 2013 auf einem hohen und mit Deutschland vergleichbaren Level (83%).[43] Internetnutzer in Großbritannien verbringen täglich 1,75 Stunden im Internet; TV ist mit 4 Stunden täglich immer noch das am häufigsten genutzte Medium.[44] 2012 gaben ***53%*** der 1805 befragten Personen ab 16 Jahren an, sie würden das ***Smartphone*** als Zugangsweg zum Internet nutzen.[45]

2. Generell genutzte Webseiten und mobil genutzte online Angebote

Die vier meist besuchten Webseiten in Großbritannien spiegeln das Bild der anderen Länder wieder (google.co.uk (1), google.com (2), facebook.com (3), youtube.com (4)). Die hohe Präsenz von ***Nachrichtenseiten*** unter den beliebtesten Seiten deutet auf ein starkes Informationsinteresse der Bevölkerung hin, das gezielt über Online-Medien gedeckt wird (bbc.co.uk (5), dailymail.co.uk (13)). Beliebte ***Suchmaschinen*** sind neben den beiden Google Seiten yahoo.com (7) und

[39] Geens (April 2013).
[40] Geens (April 2013).
[41] Wauters (Juni 2013).
[42] International Monetary Fund (2013).
[43] Internet World Stats (2013a).
[44] eMarketer (Juli 2013a).
[45] eMarketer (Juli 2013a).

live.com (11). ***Soziale Netzwerke*** sind bei den Briten besonders beliebt, es rangieren neben Facebook drei weitere auf den Top 15 Plätzen: linkedin.com (10), twitter.com (12) und wordpress.com (15). Neben YouTube befindet sich dagegen kein weiterer ***Musik- oder Videoanbieter*** unter den Top 15 beliebtesten Seiten, erst auf Platz 20 erscheint mit imdb.com die Filmsuchdatenbank von Amazon. Auf Platz sechs befindet sich mit Ebay ein Online-Marktplatz und mit amazon.co.uk auf Platz acht und amazon.com auf Platz 16 ein klassischer Onlinehändler, was auf die Beliebtheit von E-Commerce in Großbritannien hindeutet.[46]

3. Nutzung von Online-Angeboten, die Daten verwerten

EMarketer zu Folge nutzen in 2013 32,1 Mio. Briten (50,2% der Bevölkerung) soziale Netzwerke. Dabei sind unter den Internetnutzern Frauen häufiger in sozialen Netzwerken (72,5% der Internetnutzerinnen) aktiv als Männer mit 61,7% aller Internetnutzer.[47] Alle Nutzer verbringen täglich 1,18 Stunden in sozialen Netzwerken, womit diese die beliebteste Onlinetätigkeit der Briten darstellen. Hinzu kommen noch einmal 0,54 Stunden für Mikroblogging und 0,34 Stunden für Bloggen.[48] Auch die Nutzung von ***sozialen Netzwerken über das Mobiltelefon***, die momentan bei ***20,8 Mio. Personen*** liegt, wird bis 2017 stark ansteigen (31,1 Mio.).[49] Im Dezember 2012 waren 33 Mio. Nutzer aus Großbritannien bei Facebook registriert. Prozentual auf alle Internetnutzer sind dies 13,5% mehr als in Deutschland.[50] Google+ wird von 3,5 Mio. Briten genutzt.[51] Weitere beliebte Plattformen sind linkedin.com, twitter.com, trumblr.com, printerest.com und reddit.com.[52]

4. Nutzung von Online-Angeboten, die Urheberrechte verwerten

Im Vergleich zu den anderen Onlineaktivitäten ist die Nutzung von online TV in UK nicht so stark verbreitet. Täglich verbringen Konsumenten nur 0,47 Stunden mit dem Anschauen von Online Fernsehen.[53] Nach einer Studie von Eye for Travel entfallen 70% der Besuche von online Videoseiten auf YouTube, gefolgt von den Video-on-Demand Seiten iPlayer von BBC und ITV Player.[54] Trotz der geringen Videonutzungszeiten sind unter den 100 beliebtesten Seiten 12 Videoanbieter zu finden. Neben den bereits erwähnten (youtube.com und imdb.com) sind auch Seiten von britischen Telekommunikationsanbietern zu finden, deren primärer Traffic auch aus UK stammt: die Seite von British Sky Broadcasting (sky.com (32)) und von Virgin Media (virginmedia.com (49)).[55] Fernsehsendungen werden in Großbritannien schon von 60% der Smartphonenutzer auf dem

[46] Alexa Internet (2013c).
[47] eMarketer (Juli 2013b).
[48] eMarketer (Juli 2013a).
[49] eMarketer (Juli 2013b).
[50] Internet World Stats (2013a).
[51] Plus Demographics (2013).
[52] Alexa Internet (2013c).
[53] eMarketer (Juli 2013a).
[54] Eye for travel (2011).
[55] Alexa Internet (2013c).

Handy angeschaut, 38% der Befragten gaben an pro Tag mehr als eine Stunde Fernsehen über das Handy zu schauen.[56]
Bei den Anbietern von Onlinemusik gibt es neben amazon.co.uk (8), amazon.com (16) und apple.com (27) einen weiteren interessanten Anbieter: Auf der in Israel ansässigen Seite fiverr.com (61) können Internetnutzer ihre eignen Musikinhalte verkaufen.[57]

5. Zusammenfassung und Diskussion der digitalen Welt in Großbritannien

Auf Grund der hohen Nutzungszeiten nehmen soziale Netzwerke in Großbritannien eine herausragende Stellung ein. Umso bemerkenswerter ist es, dass es in Großbritannien ähnlich wie in Schweden unter den 100 beliebtesten Seiten kein heimat-ansässiges soziales Netzwerk gibt. Gleiches gilt für Suchmaschinen. Die Bevölkerung hat die sozialen Netzwerke und Suchmaschinen aus den USA in großer Breite adaptiert. Daraus entsteht auch für Großbritannien das Problem, dass die primären Anbieter, deren Geschäftsmodell auf der Weitergabe von personenbezogenen Daten beruht, ihren Unternehmenssitz nicht im britischen Rechtsraum haben. Bei den Onlinevideos sieht die Situation ähnlich aus, auch wenn die Seiten der Broadcaster Sky und Virgin Media bei den Briten beliebt sind, nimmt YouTube nichts destotrotz eine marktbeherrschende Stellung ein.
Um die Urheberrechte von Filmen zu schützen, blockieren die meisten Internetserviceprovider in Großbritannien ihren Nutzern den Zugang zum ursprünglich in Schweden gegründeten Internetvideo Portal „The Pirate Bay".[58] Als Maßnahme zur Bestrafung von Urheberrechtsverletzungen ist es der Regierung in Großbritannien möglich, den entsprechende Internetnutzer den Zugang zum Internet zu verlangsamen oder ganz zu sperren. Damit gibt die Regierung den Internetserviceprovidern das Recht, technische Ausstattungen zum Monitoring der Seitenbesuche von ihren Kunden einzusetzen.[59]

V. USA

1. Mediensystem und Bevölkerung

Der US-Amerikanische Medienmarkt ist aus einer Reihe von Gründen besonders bedeutsam: zu allererst wegen seiner Größe. Mit einer Bevölkerung von 316,854 Mio. Amerikanern, haben die in den USA großen Medienkonzerne wesentlich stärkeren Einfluss, als die dominierenden Anbieter in Europa. Beispielsweise ist google.com in Schweden, Frankreich und Großbritannien unter den fünf beliebtesten Seiten, nichtsdestotrotz kommen 30,4% des weltweiten Datenverkehrs aus den USA.[60] Die Internetpenetration in Amerika liegt 2013 bei 78,1 %[61]. Das PEW Research Center ermittelte eine Rate von 85% unter den Personen über 18 Jahren und eine Penetration von 95%

[56] eMarketer (Juli 2013d).
[57] Alexa Internet (2013c).
[58] BBC (Juni 2012).
[59] Freedom House (September 2012), S. 7.
[60] Alexa Internet (2013b).
[61] Internet World Stats (2013b).

unter den 12-17***-Jährigen***.[62] Ferner liegt die Nutzung des mobilen Internets (Smartphone, Tablet) dieser Zielgruppe bei 74%.[63] 56% der Amerikaner über 18 Jahren besaßen im Mai 2013 ein Smartphone und 34% ein Tablet. Das Marktforschungsunternehmen eMarketer erwartet für 2013 das erste Mal, dass der Teil der Onlinezeit, der über mobile Endgeräte erfolgt (19,4 % der Medienzeit), die Zeit, in der das stationäre Internet genutzt wird (19,2% der Medienzeit), übersteigt.[64] 28% aller Smartphones laufen unter dem Android Betriebssystem und 25% unter dem Apple iOS System[65]. Mit 26% der Amerikaner, die einen E-Reader besitzen, liegt die Rate in den USA für elektronisch gelesene Bücher sehr hoch.[66] Diese Tatsache weist auf ein weiteres Merkmal der Bedeutsamkeit des US Medienmarkts hin: seine Innovationskraft. Die meisten digitalen Innovationen (Internet), die großen digitalen Unternehmen und Trends (Paywall) stammen aus den USA (insb. Silicon Valley in Palo Alto (CA)).

2. Generell genutzte Webseiten und mobil genutzte online Angebote

Die ersten vier am häufigsten besuchten Seiten der Amerikaner stimmen mit dem weltweiten Ranking überein: google.com, facebook.com, youtube.com und yahoo.com. Amazon.com nimmt auf Platz 5 eine prominente Stellung ein. Insbesondere ***soziale Netzwerke*** sind in der amerikanischen Bevölkerung sehr beliebt, so finden sich unter den 15 meist besuchten Seiten neben Facebook noch vier weitere: linkedin.com (6, Soziales Netzwerk für professionellen Austausch), twitter.com (11), blogspot.com (12, Bloggingwebsite von google) und pinterest.com (13, online Pinwand). Neben den aus anderen Ländern bekannten ***Suchmaschinen*** google.com (1), yahoo.com (4) und live.com (14), befindet sich noch die Microsoft Suchmaschine bing.com (10) unter den Top 15 Seiten. Die Suchmaschine ask.com (Platz 32) ist in Amerika ebenso weit verbreitet. ***Online-Marktplätze*** sind durch ebay.com (9) und craigslist.org (8) vertreten. Ergänzend zu YouTube findet sich unter der Kategorie Verwertung von Urheberrechten noch die Landingpage für Disney-Inhalte (go.com, Platz 15) unter den 15 meist besuchten Seiten. ***Nachrichtenseiten*** sind erst ab dem 16. Platz durch cnn.com vertreten.[67]

3. Nutzung von Online-Angeboten, die Daten verwerten

Facebook wird zum Kommunizieren mit anderen mittlerweile genauso häufig genutzt wie das Schreiben einer Email.[68] In Amerika gibt es 166 Mio. Facebooknutzer (in Europa 251 Mio.) Prozentual auf die Internetnutzer des jeweiligen Landes bezogen, sind jedoch mehr Internetnutzer in Amerika bei Facebook angemeldet (68%) als in Europa (48% der Internetnutzer).[69] In der Woche verbringen amerikanische Facebooknutzer 6,8 Stunden auf Facebook, YouTube Nutzer kommen

[62] Pew Research Center (Mai 2013a).

[63] Pew Research Center (September 2012).

[64] eMarketer (August 2013).

[65] eMarketer (Juni 2013).

[66] Pew Research Center (Mai 2013b).

[67] Alexa Internet (2013c).

[68] eMarketer (Juli 2013c).

[69] Internet World Stats (2013b).

auf 5 Stunden. Google+ wird von 28,3 Mio. US-Amerikanern genutzt.[70] Die Zeiten für Google+ und Twitter bei den jeweiligen Nutzern sind mit 4,3 und 4,2 Stunden etwas geringer.[71] Allerdings wird an diesen sehr hohen Zahlen deutlich, welchen Einfluss soziale Netzwerke in Amerika haben. Die meist genutzten sozialen Netzwerke in den USA sind nach einer Umfrage aus 2013 Facebook, Twitter, Google +, LinkedIn, Printerest, MySpace, Instagram, Tumblr und Foursqure.[72] Auch reddit.com (38) als sozialer Nachrichtenaggregator ist in Amerika sehr beliebt. Unter den mobil genutzten Anwendungen verzeichnen soziale Netzwerke als auch Videoplattformen die stärksten Zuwachsraten.[73] 28 Mio. Amerikaner nutzen Twitter und 100 Mio. Facebook mindestens einmal im Monat per Smartphone.[74] ***Fotowebseiten*** wie Instagram und Snapchat werden besonders häufig vom Smartphone aus genutzt. [75]

4. Nutzung von Online-Angeboten, die Urheberrechte verwerten

Die beliebtesten Videoseiten in den USA sind neben youtube.com das Video on Demand und Filmverleihportal netflix.com (25) und die Informationsdatenbank über Filme imdb.com (26). Auch pornographische Filmdatenbanken werden mit xvideos.com (51), xhamster.com (54) und pornhub.com (57) häufig genutzt. Das Videoportal für nichtkommerzielle Videos vimeo.com (75) und das kostenlose Videostreamingportal hulu.com (83) von NBC, FOX und ABC sind in anderen Ländern nicht weit verbreitet oder zugriffsbeschränkt.[76]

Neben Amazon und Apple (30) werden als Musikseiten noch pandora.com (50), fiverr.com (69) und thepiratebay.sx (73) genutzt. Die beiden letzten Seiten werden auch für Videos verwendet. Der Musikstreamingdienst pandora.com wird zu 94,7% aus den USA genutzt, da er in allen anderen Ländern außer Australien und Neuseeland nicht verwendet werden darf.

5. Zusammenfassung und Diskussion der digitalen Welt in den USA

Wie eingangs erläutert, ist dem USA Amerikanischen Medienmarkt auf Grund seiner Größe, der vielen dort ansässigen digitalen Unternehmen und seiner Innovationskraft eine herausragende Bedeutung zuzuweisen. Besonders auffällig bei der Betrachtung des US-amerikanischen Medienmarktes ist, dass alle dominanten Anbieter aus den Bereichen Weitergabe von personenbezogenen Daten ihren Unternehmenssitz in den USA haben. Außerdem verbringen die USA Amerikaner bedeutend mehr Zeit in sozialen Netzwerken als die Einwohner der europäischen Länder, die in dieser Studie analysiert werden. Zudem ist die Vielfalt der genutzten sozialen Netzwerke auffällig.

[70] Plus Demographics (2013).

[71] eMarketer (Juli 2013c).

[72] Meeker, Mary und Liang Wu (KPCB) (Mai 2013), S. 27.

[73] eMarketer (August 2013).

[74] eMarketer (August 2013).

[75] eMarketer (Juli 2013c).

[76] Alexa Internet (2013c).

Den folgenden Ausführungen zur rechtlichen Situation ist vorwegzunehmen, dass in den USA Anbieter mobiler Plattformen nicht für Gesetzesverstöße von Drittanbietern von Apps verantwortlich sind.[77] In den USA baut die GPS basierte Datenapp Foursquare sein bisheriges Geschäftsmodell weiter aus. Bisher erzielte Foursquare durch die Übermittlung von geographischen Daten von Unternehmen an Konsumenten seine Erlöse. Neuerdings verkauft Foursquare zudem die GPS Daten der Nutzer an seine Werbekunden, wobei durch die Aggregation mit weiteren Konsumentendaten Datenschutzaspekte noch stärker berührt werden [78] Auf Seiten der Nutzer ist durch das Bekanntwerden des NSA Spähprogramms Prism, das durch einen Direktzugriff auf Server von diversen Onlineanbietern wie Google, Apple und Facebook personenbezogene Daten und Kommunikationsdaten sammelt, eine neue Datenschutzdiskussion entbrannt.[79]

VI. Relevante Unternehmen

1. Google Inc.

Die Haupteinnahmequelle des in Kalifornien ansässigen Unternehmens Google Inc. ist mit 96,4% aller Umsätze der Bereich der Werbung.[80] Weitere Geschäftsbereiche sind im Feld Suche, Anwendungssysteme (Android, Google Chrome) und Plattformen (Google+, Google TV und Google Books) einzuordnen. Auch für Unternehmen bietet Google diverse Produkte an. Zu seinen Webbasierten Applikationen zählen Gmail. Google Docs, Google Calendar und die Google Seiten. Außerdem gibt es spezielle Google Maps Anwendungen für Unternehmen.[81] Auch im immer weiter wachsenden Markt des mobilen Internets ist Google mit dem am häufigsten genutzten Betriebssystem aus Smartphones, Android, gut positioniert. Google sorgt dafür, dass einige seiner Apps (Google Maps, Google Earth, YouTube, Gmail and Google Search) auf allen Android Handys vorinstalliert sind.[82] Die meisten Umsätze und Seitenaufrufe von Google stammen aus den USA (46,3% und 30,1%). 8,8% kommen aus Indien und 2,8 % aus Großbritannien. [83] Googles Hauptkonkurrenten sind Microsoft Corporation, Yahoo! Inc und eBay Inc.[84]

Googles soziales Netzwerk Google+ registrierte im August 2013 weltweit 90 Mrd. Nutzer,[85] bei Facebook waren es im Dezember 2012 976 Mrd.[86] Google+ wird vorwiegend von männlichen Usern genutzt (70,38%), zudem stammt der Großteil der Benutzer aus den USA.

Im Jahr 2006 hat Google für 1,6 Mrd USD die Videoplattform ***Youtube LLC*** gekauft. Neben seiner Videofunktion stellt YouTube noch ein Analysetool bereit, das es ermöglicht, Daten über Nutzer

[77] Center for Democracy and Technology (CDT) (September 2012), S. 1.

[78] MCDermott (Juli 2013).

79 The Guardian (Juni 2013).

[80] MarketLine (2012b), S. 20.

[81] MarketLine (2012b), S. 3ff. ff.

[82] MarketLine (2012b), S. 23.

[83] Alexa Internet (2013b).

[84] MarketLine (2012b), S. 29.

[85] Plus Demographics (2013).

[86] Internet World Stats (2013a).

zu sammeln und seine Inhalte an die individuellen Bedürfnisse der Zuschauer anzupassen.[87] Die in der Minute hochgeladenen Stunden von Videos auf YouTube haben sich von Mai 2011 bis Mai 2013 von 50 Stunden Videomaterial, auf 100 Stunden verdoppelt.[88] Die Reichweite von YouTube ist stärker über mehrere Länder verteilt als die von google.com. So stammen 19,8% der Seitenabrufe von YouTube aus den USA, 8,2% aus Indien und 4,5% aus Japan. Die meisten europäischen Aufrufe sind aus Deutschland (3,6%), Großbritannien (3,3%) und Frankreich (2,8%) zu verzeichnen.[89] Es ist anzumerken, dass YouTube in den jeweiligen Ländern unterschiedliche Funktionen anbietet. So sind in Deutschland die Musikfunktion, die TV-Show-, Film-, und Nachrichtenfunktion sowie viele weitere nicht aktiviert. [90]

2. Facebook Inc.

Das 2004 gegründete US-Amerikanische Unternehmen mit Sitz in Kaliforniern ist der Marktführer im Bereich sozialer Netzwerke. Das Geschäftsmodell von Facebook beruht auf zwei Einnahmequellen: Werbung und Gebühren für die digitale Währung, die es Nutzern ermöglicht virtuelle Güter in Spielen und Apps zu kaufen. Die Hauptprodukte von Facebook sind (Desktop-) Anwendungen, mobile Applikationen, Plattformen, Profilseiten und Display Werbung.[91]

Facebook hatte im März 2013 1.11 Mrd. monatlich aktive Nutzer und 751 Mio. aktive mobile Nutzer. Die mobile Nutzung von Facebook ist seit 2006 möglich. Schätzungen zufolge landen 57,1% der Traffics für soziale Netzwerke auf der Facebookseite, gefolgt von YouTube mit einem Marktanteil von 24,7% und Twitter mit 1,7%.[92] Die meisten Besucher von Facebook kommen aus den USA (22,3%), Indien (7,8%), Brasilien (4,7%), Deutschland (3,4%) und Großbritannien (3,2%).[93] Im September 2012 verbrachte jeder Facebooknutzer im Monat durchschnittlich 6.40 Stunden auf Facebook, bei Yahoo, Google und YouTube war es nur die Hälfte der Zeit. [94] Die Hauptkonkurrenten von Facebook sind derzeit Google Inc. mit google+, die japanische Community mixi Inc., vKontakte, das beliebteste Netzwerk in Russland und die chinesische soziale Netzwerkseite Renren.[95]

2012 kaufte Facebook die mobile Fotoplattform ***Instagram*** für 1 Mrd. USD,[96] die mittlerweile 130 Mio. Nutzer beziffert.[97]

---

[87] MarketLine (2012b), S. 4;7 ff.

[88] Meeker, Mary und Liang Wu (KPCB) (Mai 2013), S. 17.

[89] Alexa Internet (2013d).

[90] Gugel (2013).

[91] MarketLine (2013), S. 4;16 ff.

[92] Bei der Berechnung des Marktanteils in der Studie wurde YouTube zu den sozialen Netzwerken gezählt

[93] Alexa Internet (2013a).

[94] MarketLine (2013), S. 18 f. ff.

[95] MarketLine (2013), S. 24.

[96] MarketLine (2013), S. 8.

[97] Kovach (2013).

3. Amazon.com Inc.

Das in Washington D.C. sitzende Unternehmen Amazon.com Inc ist einer der führenden Onlinehändler und bietet eine weite Produktpalette an (Bücher, Kleidung, Elektronik Artikel uvm.).[98] Amazon.com gliedert seine Geschäfte in drei Bereiche: Onlinehandel (59,7% des Umsatzes), Medien (37%) und sonstige (3,3%).[99] Insbesondere durch seinen starken Medienbereich zählt Amazon zu den Unternehmen, die in dem Bereich der digitalen Verwertung von Urheberrechten aktiv sind. Insbesondere in den letzten Jahren hat Amazon durch seinen E-Reader Kindle und seine Musikcloud das digitale Angebot weiter ausgebaut. Das Geschäftsmodell, dass mit dem E-Readers Kindle verbunden ist, basiert nicht auf dem Verkauf der Hardware, vielmehr sollen die Erlöse durch den an das Gerät gebundenen Verkauf von Büchern, Musik und Apps erzielt werden.[100]

Autorip ist der Name für das Angebot von Amazon, bei dem Käufer einer physischen CD gleich die MP3-Versionen kostenlos dazu erhalten. Diese Versionen liegen online auf der Amazon Cloud. Autorip gilt nicht nur für neu gekaufte CDs, sondern auch für solche, die seit 1999 erworben wurden.[101] Dieses Angebot hat das Potential, die Konkurrenz zu rein online-gestützten Musikangeboten wie iTunes zu verändern.

Amazon ist mit einem jährlichen Umsatz von 48,1 Mrd. USD Marktführer vor seinen Hauptkonkurrenten eBay (11,7 Mrd.) und Barnes & Noble (7,1 Mrd. USD).[102]

VII. Trends

Die zunehmende Bereitschaft insbesondere bei Teenagern, Daten auf Sozialen Netzwerken wie Facebook bereitzustellen, einhergehend mit dem geringen Problembewusstsein gegenüber der Weitergabe und Speicherung von personenbezogenen Daten, ist aus Datenschutzsicht besorgniserregend. Insbesondere das Posten von geographischen Daten (Name der Schule, Wohnort, Ort des Postings) und die Bekanntgabe der eignen Handynummer hat seit 2006 stark zugenommen.[103] Die Konzentration der Anbieter in Verbindung mit der Weiterentwicklung technischer Möglichkeiten der Datenaggretation ermöglicht es großen Playern in der Digitalen Welt zunehmend, aus den persönlichen Daten, die Konsumenten im Internet hinterlassen, sehr genaue Profile der Konsumentinnen und Konsumenten zu erstellen. Hier entstehen neue Herausforderungen für den Verbraucher- und den Datenschutz, zumal diese Datenaggregation für viele Verbraucher nur sehr schwer zu durchschauen ist.[104]

Besonders auffällig ist der Zuwachs von Fotoplattformen in den letzten Jahren. Die Zahl der auf Facebook hochgeladenen Fotos steigt ebenso an (zwischen Oktober und Dezember 2012 waren es täglich 350 Mio.)[105] wie die auf Instagram und Snapchat.[106] Aus urheberrechtlicher Sichtweise

---

[98] MarketLine (2012a), S. 3.

[99] MarketLine (2012a), S. 22.

[100] dpa (o.D.).

[101] Tanriverdi (2013).

[102] MarketLine (2012a), S. 22: 22 f. ff.

[103] Pew Research Center (Mai 2013c), S. 2 f. ff.

104 Buck / Eymann / Germelmann (erscheint im Tagungsband Verbraucherschutz).

[105] MarketLine (2013), S. 4.

[106] Meeker, Mary und Liang Wu (KPCB) (Mai 2013), S. 14.

entsteht damit ein neues Problem. Es geht nun nicht mehr um die Fragestellung, wie geschäftliche Unternehmen und Privatpersonen durch Filesharing oder Videostreamingplattformen die Urheberschaft von kommerziellen Anbietern (Film- und Musikstudios) verletzen, sondern vielmehr verletzen Privatpersonen möglicherweise durch das Hochladen von privaten Fotos das Persönlichkeitsrecht (Recht am eigenen Bild) von anderen Privatpersonen.

VIII. Literaturverzeichnis

Alexa Internet, Inc.: Skyrock.com [Quelle: http://www.alexa.com/siteinfo/skyrock.com (15.08.2013)].

Alexa Internet, Inc.: facebook.com, 2013 [Quelle: http://www.alexa.com/siteinfo/facebook.com (23.08.2013)].

Alexa Internet, Inc.: google.com, 2013 [Quelle: http://www.alexa.com/siteinfo/google.com#demographics (23.08.2013)].

Alexa Internet, Inc.: Top Sites, 2013 [Quelle: http://www.alexa.com/topsites (23.08.2013)].

Alexa Internet, Inc.: youtube.com, 2013 [Quelle: http://www.alexa.com/siteinfo/youtube.com (23.08.2013)].

BBC: The Pirate Bay 'breaches" BT's ban of the filesharing site, 2012 [Quelle: http://www.bbc.co.uk/news/technology-18518777 (23.08.2013)].

Center for Democracy and Technology (CDT): Mobile Platforms as Intermediaries: Liability Protections in the United States, the European Union, and Canada, 2012 [Quelle: https://www.cdt.org/report/mobile-platforms-intermediaries (23.08.2013)].

comScore: Turkey has third most engaged online audience in Europe, 2011 [Quelle: http://www.comscore.com/Insights/Press_Releases/2011/10/Turkey_Has_Third_Most_Engaged_Online_Audience_in_Europe (15.08.2013)].

dpa: Amazon-Chef Jeff Bezos im dpa-Gespräch, o.D. [Quelle: http://www.fr-online.de/digital/amazon-chef-jeff-bezos-im-dpa-gespraech,1472406,20576328.html (28.08.2013)].

eMarketer: In France, Twitter Finds an Older Niche, 2013 [Quelle: http://www.emarketer.com/Article/France-Twitter-Finds-Older-Niche/1009629 (15.08.2013)].

eMarketer: YouTube Launches Local Sites in Select Nordic Countries, 2013 [Quelle: http://www.emarketer.com/Article/YouTube-Launches-Local-Sites-Select-Nordic-Countries/1009671 (15.08.2013)].

eMarketer: In France, Mobile Devices Boost Gadget Count in Homes, 2013 [Quelle: http://www.emarketer.com/Article/France-Mobile-Devices-Boost-Gadget-Count-Homes/1009753 (15.08.2013)].

eMarketer: Twitter Is Widely Known in France, but Garners Few Regular Users, 2013 [Quelle: http://www.emarketer.com/Article/Twitter-Widely-Known-France-Garners-Few-Regular-Users/1009851 (15.08.2013)].

eMarketer: US Smartphone OS Race Still Close, as Men, Younger Users Favor Android, 2013 [Quelle: http://www.emarketer.com/Article/US-Smartphone-OS-Race-Still-Close-Men-Younger-Users-Favor-Android/1009961 (15.08.2013)].

eMarketer: Multichannel Media Consumption Becomes the Norm in the UK, 2013 [Quelle: http://www.emarketer.com/Article/Multichannel-Media-Consumption-Becomes-Norm-UK/1010049 (15.08.2013)].

eMarketer: Social Networking to Reach Half the UK Population This Year, 2013 [Quelle: http://www.emarketer.com/Article/Social-Networking-Reach-Half-UK-Population-This-Year/1010032 (15.08.2013)].

eMarketer: Social Usage Involves More Platforms, More Often, 2013 [Quelle: http://www.emarketer.com/Article/Social-Usage-Involves-More-Platforms-More-Often/1010019 (15.08.2013)].

eMarketer: UK Smartphone Users Embrace Mobile Entertainment, 2013 [Quelle: http://www.emarketer.com/Article/UK-Smartphone-Users-Embrace-Mobile-Entertainment/1010077 (15.08.2013)].

eMarketer: US Time Spent on Mobile to Overtake Desktop, 2013 [Quelle: http://www.emarketer.com/Articles/Print.aspx?R=1010095 (15.08.2013)].

Europäische Kommission: Special Eurobarometer 362 - E-Communications Haushaltsumfrage, 2011, S. 51

Eye for travel: 86pc of the UK Internet users visit a video site at least once a month, 2011 [Quelle: http://www.eyefortravel.com/social-media-and-marketing/86pc-uk-internet-users-visit-video-site-least-once-month (29.08.2013)].

Freedom House: Freedom on the Net 2012. United Kingdom 2012, 2012 [Quelle: http://www.freedomhouse.org/report/freedom-net/2012/united-kingdom (30.08.2013)].

Geens, Stefan: Internet freedom in Sweden - a closer look, 2013 [Quelle: http://www.sweden.se/eng/Home/Society/Government-politics/Reading/Internet-freedom-in-Sweden--a-closer-look/ (28.08.2013)].

Gugel, Betram: Digitaler Film- YouTube Deutschland vs. YouTube International, 2013 [Quelle: http://www.gugelproductions.de/blog/2013/youtube-steckt-in-deutschland-noch-in-den-kinderschuhen.html (28.08.2013)].

Hans-Bredow-Institut für Medienforschung an der Universität Hamburg (Hrsg.): Internationales Handbuch Medien, 28. Auflage, 2009.

International Monetary Fund: World Economic Outlook Database. 5. Report for Selected Countries and Subjects, 2013 [Quelle: http://www.imf.org/external/pubs/ft/weo/2013/01/weodata/weorept.aspx?sy=2012&ey=2016&scsm=1&ssd=1&sort=country&ds=.&br=1&pr1.x=74&pr1.y=13&c=132%2C134%2C144%2C112%2C111&s=LP&grp=0&a=#cs1 (15.08.2013)].

Internet World Stats: Internet and Facebook Usage in Europe, 2013 [Quelle: http://www.internetworldstats.com/stats4.htm (28.08.2013)].

Internet World Stats: Internet Usage, Facebook Subscribers and Population Statistics for all the Americas World Region Countries, June 30, 2012, 2013 [Quelle: http://www.internetworldstats.com/stats2.htm (05.08.2013)].

Kovach, Steve: Chart of the day: The Rise of Instagram, 2013 [Quelle: http://www.businessinsider.com/chart-of-the-day-instagram-growth-2013-6 (28.08.2013)].

MarketLine: Company Profile Amazon.com, Inc., 2012 [Quelle: http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=cbdd2acb-5634-4230-9da3-5df7e4988b3f%40sessionmgr14&vid=6&hid=19 (23.08.2013)].

MarketLine: Company Profile Google Inc., 2012 [Quelle: http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=186d8ab6-516e-49f9-9343-b684128c7acf%40sessionmgr4&vid=6&hid=21 (28.08.2013)].

MarketLine: Company Profile Facebook Inc., 2013 [Quelle: http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=93298f04-e8c2-401b-842f-4335cdf6a2af%40sessionmgr12&vid=7&hid=21 (29.08.2013)].

MCDermott, John: Foursquare selling its location data through ad targeting firm turn, 2013 [Quelle: http://adage.com/article/digital/foursquare-selling-data-ad-targeting-firm-turn/243398/ (30.08.2013)].

Mediametrie: Médiamétrie lance l´étude Social TV, 2013 [Quelle: http://www.mediametrie.fr/internet/communiques/mediametrie-lance-l-etude-social-tv.php?id=892#.UgyPTKxaf2Q (15.08.2013)].

Mediametrie: L´audience de l´internet mobile en France en juin 2013, 2013 [Quelle: http://www.mediametrie.fr/internet/communiques/l-audience-de-l-internet-mobile-en-france-en-juin-2013.php?id=914#.UgyFOqxaf2Q (15.08.2013)].

Mediametrie: L´audience de la vidéo sur internet en juin 2013, 2013 [Quelle: http://www.mediametrie.fr/internet/communiques/l-audience-de-la-video-sur-internet-en-juin-2013.php?id=915#.UgyPVKxaf2Q].

Meeker, Mary und Liang Wu (KPCB): Internet trends. D11 Conference, 2013 [Quelle: http://www.kpcb.com/insights/2013-internet-trends (15.08.2013)].

Münchner Kreis: Nutzung des mobilen Internets in Schweden privat oder geschäftlich, 2011 [Quelle: http://de.statista.com/statistik/daten/studie/209890/umfrage/nutzung-des-mobilen-internets-zu-privaten-oder-geschaeftlichen-zwecken-in-schweden/ (15.08.2013)].

NewMedia TrendWatch: Sweden, 2013 [Quelle: http://www.newmediatrendwatch.com/markets-by-country/10-europe/85-sweden (15.08.2013)].

Nord, Lars: Mapping Digital Media: Sweden, 2011 [Quelle: http://www.opensocietyfoundations.org/sites/default/files/mapping-digital-media-sweden-20110920.pdf (30.08.2013)].

Pew Research Center: Teen Internet Access Demographics, 2012 [Quelle: http://pewinternet.org/Static-Pages/Trend-Data-%28Teens%29/Whos-Online.aspx (15.08.2013)].

Pew Research Center: Demographics of internet users, 2013 [Quelle: http://pewinternet.org/Trend-Data-%28Adults%29/Whos-Online.aspx (15.08.2013)].

Pew Research Center: Device Ownership, 2013 [Quelle: http://pewinternet.org/Trend-Data-%28Adults%29/Device-Ownership.aspx (15.05.2013)].

Pew Research Center: Teens, Social Media, and Privacy, 2013 [Quelle: http://www.pewinternet.org/Infographics/2013/Teens-Social-Media-And-Privacy.aspx# (23.08.2013)].

Plus Demographics: Demographic breakdown of the Google+ users, 2013 [Quelle: http://www.plusdemographics.com/country_report.php (29.08.2013)].

Reporters without Borders: France. 2012 Surveillance, 2012 [Quelle: http://en.rsf.org/france-france-12-03-2012,42071.html (30.08.2013)].

Socialbakers: Sweden Facebook Statistics, 2013 [Quelle: http://www.socialbakers.com/facebook-statistics/sweden (15.08.2013)].

Statistics Sweden: Sending e-mail and reading news sites common on a mobile phone, 2013 [Quelle: http://www.scb.se/Pages/PressRelease____347307.aspx (15.08.2013)].

Tanriverdi, Hakan: Amzon gibt CD-Käufern gleich die MP3-Version dazu, 2013 [Quelle: http://www.sueddeutsche.de/digital/autorip-amazon-gibt-cd-kaeufern-gleich-die-mp-version-dazu-1.1705381 (29.08.2013)].

The Guardian: NSA Prism program taps in to user data of Apple, Google and others, 2013 [Quelle: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (28.08.2013)].

UN Public Administration Programme: United Nations E-Government Development Database, 2012 [Quelle: http://unpan3.un.org/egovkb/datacenter/countryview.aspx (28.08.2013)].

Wauters, Robin: Dark clouds loom over Google in the EU as Swedisch data regulator kills a Google Apps deal, 2013 [Quelle: http://thenextweb.com/google/2013/06/14/sweden-google-data-protection/ (30.08.2013)].

4. Anhang:

Rang	Rang Global	Name	Internetpräsenz	Branche	Mutterunternehmen	Geschäftsmodel
1	28	Google France	google.fr	Suchmaschine und andere Services	Google Inc.	Weitergabe persönlicher Daten Onlineverwertung Urheberrecht (Bücher)
2	1	Google	google.com	Suchmaschine und andere Services	Google Inc.	Weitergabe persönlicher Daten Onlineverwertung Urheberrecht (Bücher)
3	2	Facebook	facebook.com	Soziales Netzwerk	Facebook, Inc.	Weitergabe persönlicher Daten
4	3	YouTube	youtube.com	Videoportal	Google Inc.	Onlineverwertung Urheberrecht
5	6	Wikipedia	wikipedia.org	Online Enzyklopädie	Wikimedia Foundation, Inc.	
6	216	leboncoin.fr	leboncoin.fr	Online-Marktplatz	LBC FRANCE, SAS	
7	206	Amazon.fr	amazon.fr	Online-Marktplatz, Kindle (ebooks), MP3 etc.	AMAZON.COM, INC.	Onlineverwertung Urheberrecht
8	4	Yahoo!	yahoo.com	Suchmaschine und andere Services	Yahoo! Inc.	Weitergabe persönlicher Daten
9	325	Orange	orange.fr	Telekommunikationsanbieter	France Telecom S.A. (seit Anfang 2013 Orange S.A.)	
10	292	Freebox	free.fr	Telekommunikationsanbieter	Iliad S.A.	
11	9	Windows Live	live.com	Suchmaschine	Microsoft Corporation	Weitergabe persönlicher Daten
12	8	LinkedIn	linkedin.com	Professionelles soziales Netzwerk	LinkedIn Corporation	Weitergabe persönlicher Daten
13	536	eBay	ebay.fr	Online-Marktplatz	eBay Inc.	
14	10	Twitter	twitter.com	Soziales Netzwerk und Mikroblogging	Twitter Inc.	Weitergabe persönlicher Daten

15	467	Com-ment Ca March e	commentca-marche.net	Suchmaschine für Informationen zu Internet, Netzwerken etc.	GROUPE CCM / BENCHMARK	Weitergabe persönlicher Daten

Abbildung 1: Generell genutzte Webseiten Frankreich
Quelle: Eigene Darstellung in Anlehnung an alexa.com und diverse Unternehmenshomepages

Rang	Globaler Rang	Name	Internetpräsenz	Branche	Mutterunternehmen	für Gutachten relevantes Geschäftsmodel
1	244	Google	google.se	Suchmaschine und andere Services	Google Inc.	Weitergabe persönlicher Daten Onlineverwertung Urheberrecht
2	1	Google	google.com	Suchmaschine und andere Services	Google Inc.	Weitergabe persönlicher Daten Onlineverwertung Urheberrecht
3	2	Facebook	facebook.com	Soziales Netzwerk	Facebook, Inc.	Weitergabe persönlicher Daten
4	3	YouTube	youtube.com	Videoportal	Google Inc.	Onlineverwertung Urheberrecht
5	890	Aftonbladet	aftonbladet.se	Boulevardzeitung	Schibsted ASA	Onlineverwertung Urheberrecht
6	6	Wikipedia	wikipedia.org	Online Enzyklopädie	Wikimedia Foundation, Inc.	
7	1491	Blocket	blocket.se	Online-Marktplatz	Schibsted ASA	
8	4	Yahoo!	yahoo.com	Suchmaschine und andere Services	Yahoo! Inc.	Weitergabe persönlicher Daten
9	8	LinkedIn	linkedin.com	Professionelles soziales Netzwerk	LinkedIn Corporation	Weitergabe persönlicher Daten
10	9	Windows Live	live.com	Services der Microsoft Corp.	Microsoft Corporation	Weitergabe persönlicher Daten
11	2553	Swedbank AB	foreningssparbanken.se	Kreditinstitut	Swedbank AB (publ)	
12	2597	Expressen	expressen.se	Boulevardzeitung	Bonnier AB	Onlineverwertung Urheberrecht
13	74	thepiratebay.sx	thepiratebay.sx	Download von Filmen, Musik etc.		Onlineverwertung Urheberrecht
14	43	The Internet Movie Database	imdb.com	Online Film-, TV- und Computerspiele-Datenbank	AMAZON.COM, INC.	Onlineverwertung Urheberrecht
15	10	Twitter	twitter.com	Soziales Netzwerk und Mikroblogging	Twitter Inc.	Weitergabe persönlicher Daten

Abbildung 2: Generell genutzte Webseiten Schweden
Quelle: Eigene Darstellung in Anlehnung an alexa.com und diverse Unternehmenshomepages

Rang	Rang Global	Name	Internetpräsenz	Branche	Mutterunternehmen	für Gutachten relevantes Geschäftsmodel
1	24	Google UK	google.co.uk	Suchmaschine und andere Services	Google Inc.	Weitergabe persönlicher Daten, Onlineverwertung Urheberrecht
2	1	Google	google.com	Suchmaschine und andere Services	Google Inc.	Weitergabe persönlicher Daten, Onlineverwertung Urheberrecht
3	2	Facebook	facebook.com	Soziales Netzwerk	Facebook, Inc.	Weitergabe persönlicher Daten
4	3	YouTube	youtube.com	Videoportal	Google Inc.	Onlineverwertung Urheberrecht
5	49	BBC Online	bbc.co.uk	Nachrichtendienst	BBC Worldwide Ltd	Onlineverwertung Urheberrecht
6	92	eBay UK	ebay.co.uk	Online-Marktplatz	eBay Inc.	
7	4	Yahoo!	yahoo.com	Suchmaschine und andere Services	Yahoo! Inc.	Weitergabe persönlicher Daten
8	102	Amazon.co.uk	amazon.co.uk	MP3 etc.	AMAZON.COM, INC.	Onlineverwertung Urheberrecht
9	6	Wikipedia	wikipedia.org	Online Enzyklopädie	Wikimedia Foundation, Inc.	
10	8	LinkedIn	linkedin.com	Professionelles soziales Netzwerk	LinkedIn Corporation	Weitergabe persönlicher Daten
11	9	Windows Live	live.com	Services der Microsoft Corp.	Microsoft Corporation	Weitergabe persönlicher Daten
12	10	Twitter	twitter.com	Soziales Netzwerk und Mikroblogging	Twitter Inc.	Weitergabe persönlicher Daten
13	104	The Daily Mail	dailymail.co.uk	Zeitung	Associated Newspapers Ltd	Onlineverwertung Urheberrecht
14	35	PayPal	paypal.com	Online Bezahl-Service	eBay Inc.	
15	15	WordPress.com	wordpress.com	Weblog-Software	Automattic, Inc.	Weitergabe persönlicher Daten

Abbildung 3: Generell genutzte Webseiten Großbritannien
Quelle: Eigene Darstellung in Anlehnung an alexa.com und diverse Unternehmenshomepages

Rang	Rang Global	Name	Internetpräsenz	Branche	Mutterunternehmen	für Gutachten relevantes Geschäftsmodel
1	1	Google	google.com	Suchmaschine und andere Services	Google Inc.	Weitergabe persönlicher Daten, Onlineverwertung Urheberrecht
2	2	Facebook	facebook.com	Soziales Netzwerk	Facebook, Inc.	Weitergabe persönlicher Daten
3	3	YouTube	youtube.com	Videoportal (kostenloses hochladen, ansehen und bewerten von Videos; Video-Channel etc.)	Google Inc.	Onlineverwertung Urheberrecht
4	4	Yahoo!	yahoo.com	Suchmaschine und andere Services	Yahoo! Inc.	Weitergabe persönlicher Daten
5	11	Amazon.com	amazon.com	Kindle (ebooks), MP3 etc.	AMAZON.COM, INC.	Onlineverwertung Urheberrecht
6	8	LinkedIn	linkedin.com	Professionelles soziales Netzwerk	LinkedIn Corporation	Weitergabe persönlicher Daten
7	6	Wikipedia	wikipedia.org	Online Enzyklopädie	Wikimedia Foundation, Inc.	
8	42	Craigslist.org	craigslist.org	Online Kleinanzeigen		
9	20	eBay	ebay.com	Online-Marktplatz	eBay Inc.	
10	16	Bing	bing.com	Suchmaschine	Microsoft Corporation	Weitergabe persönlicher Daten
11	10	Twitter	twitter.com	Soziales Netzwerk und Mikroblogging	Twitter Inc.	Weitergabe persönlicher Daten
12	12	Blogspot.com	blogspot.com	free Web hosting service	Google Inc.	Weitergabe persönlicher Daten
13	26	Pinterest	pinterest.com	Soziales Netzwerk (Pinnwand-Funktion)		Weitergabe persönlicher Daten
14	9	Windows Live	live.com	Services der Microsoft Corp.	Microsoft Corporation	Weitergabe persönlicher Daten
15	63	Go	go.com	Landingpage für Disney Inhalte	The Walt Disney Company	Onlineverwertung Urheberrecht

Abbildung 4: Generell genutzte Webseiten USA
Quelle: Eigene Darstellung in Anlehnung an alexa.com und diverse Unternehmenshomepages

C. Marktüberwachung in der digitalen Welt am Beispiel des Urheberrechts und Datenschutzrechts – Vergleich der Regelungen der USA, Frankreichs, Schwedens und Englands

Auf den ersten Blick ist der Rundblick durch die untersuchten Rechtsordnungen – USA, Frankreich, Schweden und England – unergiebig. Eine eigenständige, administrative Durchsetzung oder Marktaufsicht für den digitalen Markt durch eine einzige Aufsichts- oder Regulierungsbehörde unter verbraucherspezifischen Aspekten besteht nämlich in keiner der untersuchten Rechtsordnungen. Für den Bereich des Verbraucherrechts allgemein lassen sich hingegen in den betreffenden Rechtsordnungen aufsichtsrechtliche Strukturen und behördliche Durchsetzung durchaus finden. Diese sind jedoch überwiegend sektoral (etwa Telekommunikation) oder auf bestimmte Sachfragen (etwa Datenschutz oder faire Geschäftspraktiken) beschränkt.

Die verbraucherspezifischen Gefahren, welche in der digitalen Welt für die Verbraucher auftreten, wird in den untersuchten Rechtsordnungen durch eine Vielzahl von Behörden und Mitteln begegnet. Die beiden Schutzfunktionen – Handeln einer Administrativbehörde zum repressiven Schutz der Verbraucher sowie eine administrative Aufsicht zur präventiven Vermeidung von verbraucherspezifischen Gefahren – sind in keiner der untersuchten Rechtsordnungen in einer verwaltungsrechtlichen Einheit vereint.

Eine Verknüpfung der datenschutzrechtlichen und urheberrechtlichen Aufsichtsmechanismen mit den verbraucherspezifischen Mechanismen ist dabei nur für die USA ansatzweise erkennbar. Dort fehlt es jedoch an einem ausdifferenzierten Datenschutz als technikneutraler, sektorübergreifender Regelungsmaterie. Das Fehlen eines solchen breiten datenschutzrechtlichen Ansatzes bedingt in den USA auch das Fehlen allgemeiner administrativer Strukturen für den Datenschutz. Datenschutzrecht ist in den USA daher primär – soweit ein nennenswerter Schutz überhaupt besteht – eine marktaufsichtsrechtliche Materie, welche durch die allgemeinen Verbraucherbehörden respective fachspezifischen Behörden durchgesetzt wird.

Die spezifisch datenschutzrechtliche Aufsicht ist in großem Maße von der Ausgestaltung des Datenschutzrechts insgesamt abhängig. Das europäische Datenschutzregime schreibt eine generelle, effektive und unabhängige datenschutzrechtliche Aufsicht vor. In den untersuchten europäischen Rechtsordnungen werden Datenschutz und Verbraucherschutz jeodch bislang eher getrennt betrachtet.[1] In England ist jedoch eine erste Aufweichung dieser Trennung zu sehen: 2013 hat das *Office of Fair Trading* (OFT) einen Bericht über „*Personalised Pricing*“ veröffentlicht, in dem das OFT unter anderem, auch auf Frage des Datenschutzes eingeht.[2] Der Empfehlung der

[1] Dieses Defizit ist auf Ebene der Europäischen Union angelegt, welche auch hinsichtlich des neuen ADR-Systems den Mitgliedsstaaten wohl keine zwingende Schlichtung für datenschutzrechtliche Streitigkeiten in einer Verbraucherstreitigkeit vorschreibt, siehe *Herden*, GPR 2013, 272.

[2] http://www.oft.gov.uk/shared_oft/markets-work/personalised-pricing/oft1489.pdf (zuletzt abegerufen am 13.11.2013).

Kommission zu der Durchsetzung durch *collective redress*[3] ist erstmals ein engerer formaler Zusammenhang zwischen Verbraucherrecht und Datenschutzrecht hinsichtlich durchsetzungsbezogener Fragen auch auf europäischer Ebene zu entnehmen.

Für den Bereich des Urheberrechts gibt die fast ausschließliche zivilrechtliche Ausgestaltung des Schutzes des Urheberrechts den Mangel an behördlichen Strukturen vor. Zwar besteht auch dort eine allgemeine administrative Aufsicht zur Verfolgung von Ordnungswidrigkeiten (gleichsam als sekundäre Ebene). Eine verwaltungsrechtliche Verfolgung von Missständen fehlt ebenso wie ein Eingreifen zum Schutz des einzelnen Verbrauchers bei übermäßiger Ausübung ziviler urheberrechtlicher Ansprüche.

Neben der Frage der sektoralen oder bereichsspezifischen Aufteilung der verschiedenen relevanten Einzelbehörden, welche zum Schutz der Verbraucher und den Bereich des digitalen Marktes in Frage kommen, prägen Selbstverständnis, Aufgabenzuweisungen und Zugriffsmöglichkeiten der Behörden den administrativen Verbraucherschutz für die digitale Welt. Ein korrigierendes, marktbezogenes Grundverständnis in den USA lässt sich ebenso finden wie die größtenteils rein verarbeitungsbezogene Datenschutzaufsicht in der EU, wobei in allen Rechtsordnungen nur punktuelle, handlungsbezogene Eingriffe und Korrekturmöglichkeiten bestehen und diese zudem eher restriktiv angewendet werden. Sie dienen nur in sehr begrenztem Maße einem Schutz des einzelnen Verbrauchers. Individuelle Schutzaspekte sind fast ausschließlich in den Regelungen über behördliche organisierte Schieds- oder Schlichtungsverfahren in Schweden, begrenzten Möglichkeiten von gerichtlichen Schritten und sehr unterschiedlich ausgestalteten Beschwerdemöglichkeiten gegeben. Das entspricht der typischen – auch für Deutschland charakteristischen – Aufgabenteilung zwischen zivilrechtlichem Individualschutz und administrativem Schutz der Allgemeinheit oder definierter Gruppen, die freilich durch das europäische Regime verbraucherschützender Unterlassungsklagen – in Abhängigkeit von der jeweiligen Richtlinienumsetzung – durchbrochen wird.

I. Regelungsstrukturen

1. Allgemeines

Allgemein ist festzustellen, dass der „Digitale Markt“ keine eigenständige Regelungsmaterie im Hinblick auf die verbraucherspezifischen Risiken der Nutzung von digitalen Angeboten darstellt, was wiederum einen Einfluss auf die administrative Durchsetzungsstruktur und -befugnisse hat. In den untersuchten Rechtsordnungen sind die Regelungen des Datenschutzrechts, Urheberrechts und Vertragsrechts für den digitalen Markt nicht in einem eigenständigen und abgeschlossenen Normenwerk geregelt. Vielmehr sind – soweit vorhanden – die für sich eigenständigen Regelungen des Datenschutzrechts, Urheberrechts und Vertragsrechts anwendbar. Darüberhinaus gelten die allgemeinen Regelungen des zivilen Verbraucherrechts wie auch die allgemeinen marktaufsichtsrechtlichen Regelungen. Diese Regelungen sind aufgrund ihres breiten Ansatzes weder spezifisch auf Gefahren des digitalen Marktes zugeschnitten noch decken sie diese vollständig ab. Fachspezifische und sektorale Regelungen, welche einzelne Aspekte der digitalen Welt erfassen, lassen sich in allen untersuchten Rechtsordnungen finden. Allerdings bestehen

[3] Commission Recommendation of June 2013 on common principles for injunctive and compensatory collective redress mechanism in the Member States concerning violations granted under Union Law (2013/396/EU) Abl. EU L 201/60 vom 26.7.2013.

zwischen dem US-amerikanischen und dem europäischen Ansatz zum Datenschutz nicht nur hinsichtlich des Schutzstandards, sondern auch hinsichtlich der administrativen Durchsetzung erhebliche Unterschiede: Die Regelungen des europäischen Datenschutzrechtssystems basieren auf einem breiten, technikneutralen, sektorunabhängigen und zumindest in formaler Hinsicht nicht auf Verbraucherbezogenen Modell der personenbezogenen Daten.[4] In den USA wird hingegen das Konzept der „*privacy policies*“ und Regelungen zur „*data security*“[5] verfolgt, wobei der Schutzstandard variieren kann. Das US-amerikanische Modell ist– nicht nur für die *consumer privacy* sondern auch für andere verbraucherrelevante Regelungen – stark sektoral untergliedert. Hingegen kommt es nicht zu einer allgemeinen stärkeren Erfassung der verbraucherspezifischen Gefahren für den digitalen Markt als Ganzes, da kaum sektorübergreifende Regelungen vorhanden sind. Eine besonders auf die verbraucherspezifischen Gefahren der Nutzung der Angebote der digitalen Welt und der Gefahr der Verletzung von Urheberrechten anderer durch die Verbraucher findet sich nur in Schweden und auch dort nur ansatzweise.[6]

a. Unterschiedliche Regelungsstrukturen zum Datenschutz

Die Stellung des Datenschutzes ist (noch) maßgeblich von der nationalen, konstitutionellen Stellung des Datenschutzes abhängig: Die nationale Positionierung gibt den Standard des Datenschutzes vor.[7] In Schweden[8] und auch Frankreich[9] lässt sich aufgrund eines gewachsenen konstitutionellen Verständnisses des Datenschutzrechts eine stärkere Gewichtung eines Regelungsbedürfnisses und Anwendungspraxis finden, als in den USA und in England.[10]

Die untersuchten Rechtsordnungen lassen sich dementsprechend in Bezug auf den „Datenschutz“ in zwei Lager teilen: Auf der einen Seite steht das europäische System des Schutzes

---

[4] Siehe dazu die 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. EG L 281/31 vom 23. November 1995 (nachfolgend Datenschutzrichtlinie).

[5] Siehe *Herden* Länderbericht USA, 1.c.

[6] In den USA finden sich im Digital Millenium Copyright Act (DMCA) zwar Regelungen, welche die digitale Welt und die Nutzung digitaler Inhalte unter anderem durch Umgehung von Sicherheitstechniken erfassen. Der DMCA verschärft jedoch grundsätzlich nur die bestehenden urheberrechtlichen Regelungen und enthält keine entlastenden Gründe für die Verbraucher bei unberechtigter Nutzung von urheberrechtlich geschützten Werken.

[7] Inwieweit mit einer möglichen europäischen Datenschutzgrundverordnung eine stärkere Harmonisierung in der Anwendungspraxis der Regelungen eintreten wird, bleibt abzuwarten.

[8] Zum schwedischen Grundrecht auf Datenschutz siehe Chapter 2 Article 6 para. 2 Intrument of Government für Schweden, hiernach „Schwedisches Datenschutzgesetz“.

[9] Zwar hat der Datenschutz als solches keinen Verankerung in der Verfassung, aber das Recht auf Privatleben wurde durch eine Entscheidung des Conseil constitutionel in den Verfassungsrang gehoben, siehe *Wichmann,* Länderbericht Frankreich, 1.a.aa).

[10] In England hat sich erst durch den Erlass des Human Rights Acts 1998 (HRA 1998) sowie der Umsetzung der Richtlinie 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (nachfolgend Datenschutzrichtlinie) erst langsam ein Verständnis der Notwendigkeit des Schutzes personenbezogener Daten zum Schutz der Persönlichkeit des Einzelnen entwickelt. Die in der Durant Rechtsprechung, [2003] EWCA Civ 1746, gesetzten Standards des Court of Appeal hinsichtlich des Schutzes personenbezogener Daten sind mit den Vorgeben der Datenschutzrichtlinie jedoch wohl nicht vereinbar.

personenbezogener Daten mit dem grundsätzlichen Prinzip des Erlaubnisvorbehalts für die Verarbeitung solcher Daten zum Schutz der einzelnen Person im Hinblick auf ihre Persönlichkeitsrechte.[11] Dieser Schutz wird durch administrative Aufsicht und Gewährung subjektiver Rechte des Einzelnen gewährleistet. In Schweden[12]; Deutschland[13]; England[14] und Frankreich[15] wurden die Regelungen der Datenschutzrichtlinie zum Schutz personenbezogener Daten in eigenständigen Datenschutzgesetzen, welche personenbezogene Daten in ihrer Gesamtheit erfassen, geregelt. Die Umsetzungsgesetze und nationale Auslegungen der Datenschutzrichtlinie sehen teilweise jedoch Beschränkungen auf eine feststellbare Verletzung der Integrität der betroffenen Person vor.[16]

Auf der anderen Seite verfolgen die USA einen eher marktbezogenen Ansatz des Schutzes der „*consumer privacy*". Eine Datenverarbeitung von Verbraucherdaten bedarf grundsätzlich keiner Einwilligung der betroffenen Verbraucher, es sei denn gesetzliche Regelungen ordnen dies an. Ein Beispiel für eine solche ausnahmsweise beschränkende Regelung ist das Erfordernis der elterlichen Zustimmung als eine der notwendig zu erfüllenden Bedingungen für die Nutzung von persönlichen Daten von Kindern durch die Betreiber von Internetseiten.[17]

Die US-amerikanischen Regelungen zur *privacy policy* verbieten falsche Angaben zur Einhaltung – der selbstauferlegten respective gelegentlich gesetzlich vorgegebenen – Erklärungen zur Datenspeicherung und Datensicherung als unlautere Geschäftspraktik („*unfair and deceptive trade practice*"). In den Anwendungsbereich dieser Regelungen fallen dabei sowohl die Erklärungen zur Nutzung von Verbraucherdaten als auch Erklärungen der Unternehmen zu den Standards der Sicherung der Verbraucherdaten vor Zugriffen Dritter. Stimmen die Angaben der Unternehmen in ihren *policies*, wie beispielweise hohe Maßnahmen zur Sicherung der Daten vor fremden Zugriffen oder eine Erklärung zur Nicht-Weitergabe der Daten an Werbepartnern, nicht mit der tatsächlichen Lage überein, kann die *Federal Trade Commission* (FTC) ein formelles Beschwerdeverfahren, gestützt auf ihre *unfair and deceptive trade practice* Kompetenz, gegen die betreffenden Unternehmen einleiten. Die Aussagen in den *privacy policies* werden im Ergebnis als unzutreffende Werbemaßnahmen eingeordnet und dementsprechend behandelt.

---

[11] Siehe dazu Artikel 7 der Datenschutzrichtlinie.

[12] Umsetzung der Datenschutzrichtlinie in Personuppgiftslag (1998:204).

[13] Bundesdatenschutzgesetz.

[14] Data Protection Act 1998.

[15] Loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, geändert zur Umsetzung der Vorgaben der Richtlinien durch das loi n° 2004-81.

[16] Für Schweden betrifft dies die Regelung des section 5a des Schweden Datenschutzgesetzes, welches für unstrukturierte Daten das „*misuse model*" favorisiert, siehe dazu Kirchberger/Storr,Länderbericht Schweden, 1.a. Nach diesem Ansatz finden einige der Vorschriften des Gesetzes keine Anwendung, wenn nur unstrukturierte Daten vorliegen und die Person in ihrer Integrität nicht beeinträchtigt wird; eine ähnliche Einschränkung nimmt auch die englische Rechtsprechung in der Entscheidung *Durant* des Court of Appeal aus dem Jahr 2003 vor, siehe dazu *McNamee,* Länderbericht England, 1.a.

[17] 15 USC § 6502 (b) (1) (A) (ii).

Auch soweit die Regelungen zu *unfair and deceptive trade practices* auf Staaten- und Bundesebene nicht einschlägig sind, erfolgt eine Durchsetzung von Standards zur *consumer policy* (neben anderen Instrumenten) vielfach durch die zu deren Bekämpfung zuständigen Behörden oder durch vergleichbare administrative Strukturen, teilweise sogar ohne ausdrückliche Anordnung, wie beim California Online Privacy Protection Act oder durch audrückliche Verweisung wie hinsichtlich der Regelungen für Kreditauskünfte.[18] Nicht der Schutz der Persönlichkeit des einzelnen von fehlenden Schutzmaßnahmen ist insoweit der primäre Regelungszweck, sondern erneut der Schutz der Verbraucher und Wettbewerber vor unrichtigen oder irreführenden Aussagen hinsichtlich des Schutzes privater Informationen. In den USA sind aufgrund des sehr sektoralen, informationsspezifischen und nicht breiten Ansatzes eine große Anzahl verschiedener Regelungen hinsichtlich der *consumer privacy* zu beachten. Diese geben oftmals jedoch nur ein Mindestmaß an Schutzerfordernissen vor. Wie auch andere marktbezogene verbraucherspezifische Regelungen wird der einzelne Verbraucher in den US-amerikanischen *consumer policy* Regelungen fast ausschließlich als Mitglied der Masse der Nachfrager verstanden.

Nur vereinzelnd sind in den USA datenschutzrechtliche Regelungen zu finden, welche sektorunabhängige Mindestanforderungen spezifisch für die digitale Welt festlegen[19], wobei eine leichte sektorale Aufsplitterung hinsichtlich einzelner Sektoren oder Problemstellung auch für die europäische Union festzustellen ist.[20] So gelten mit der Richtlinie zur elektronischen Kommunikation und zur Vorratsdatenspeicherung[21] Regelungen über die der Datenschutzrichtlinie hinaus[22].

Im europäischen Datenschutzsystem wird der besonders geschützte Personenkreis formal nicht durch den Begriff des „Verbrauchers“ bezeichnet, obwohl es funktional gerade um den Schutz der Person auch in ihrer Privatheit geht. Es besteht dabei bislang größtenteils keine Klarheit darüber, ob verbraucherschützende Mechanismen auf die datenschutzrechtlichen Regelungen bei Beteiligung von Verbrauchern Anwendung finden.[23]

---

[18] 15 USC § 1681s (a) (1).

[19] So zum Beispiel der California Online Privacy Protection Act (Caloppa) sowie der föderale, allerdings auf die Zielgruppe Kinder beschränkte, Children Online Privacy Protection Act.

[20] 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) umgesetzt in Schweden durch das Lag (2003:389) om elektronisk kummunikation (Schwedisches Gesetz für die elektronische Kommunikation.

[21] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG. In seiner maßgeblichen Entscheidung vom 02.03.2010 hat das deutsche Bundesverfassungsgericht die von der Vorratsdatenspeicherung gefordert sechsmonatige, vorsorglich anlasslose Speicherung von Kommunikationsverkehrdaten als mit Artikel 10 Grundgesetz unvereinbar gesehen, BVerfGE 125, 260.

[22] Zur Umsetzung der Vorgaben der Vorratsdatenspeicherung ist in Schweden jedoch kein eigenständiges Gesetz ergangen, sondern es wurde das Gesetz zur Änderung des Schwedischen Gesetzes für die elektronische Kommunikation, Chapter 6 Section 16a-f erlassen.

[23] Als „Verbraucher“ wird hier – im Sinne der europäischen vertragsrechtlichen Regelungen zum Verbraucherschutz“ eine natürliche Person verstanden, die eine Handlung weder zu gewerblichen noch zu beruflichenZwecken vornimmt (die Hereinnahme der Arbeitnehmer in den Verbraucherbegriff ist eine deutsche Besonderheit); auch in dem Entwurf

b. Fast ausschließliche zivilrechtliche Durchsetzung des Urheberrechts

Alle untersuchten Rechtsordnungen verfügen über Urheberrechtsgesetze, welche dem Inhaber des Urheberrechts grundsätzlich die ausschließlichen Rechte zur Nutzung einräumen; dabei folgen die USA und England dem copyright-Ansatz, während Frankreich und Schweden das Persönlichkeitsrecht des Urhebers in den Mittelpunkt rücken. In Schweden genießt das Urheberrecht sogar einen ausdrücklichen verfassungsrechtlichen Rang.[24] Aufgrund der internationalen Abkommen sind die Urheberrechtsgesetze in den untersuchten Rechtsordnungen trotz der divergierenden Grundansätze zumindest ansatzweise harmonisiert.[25]

In allen vier Rechtsordnungen ist kein eigenständiges Urheberrecht allein für die digitale Welt vorhanden, sondern die bestehenden urheberrechtlichen Regelungen wurden im Hinblick auf den technischen Fortschritt und die Nutzung digitaler Inhalte verändert und spezifiziert.[26] Teilweise, wie etwa in den USA oder nach der e-commerce-Richtlinie der Europäischen Union, bedeutete dies nur eine weitgehende Haftungsfreistellung für die Internet Service Provider, aber keine Lockerung der strikten urheberrechtlichen Bestimmungen für das Urheberrecht verletzenden Verbraucher.[27] In Frankreich wurden zahlreiche Gesetze erlassen, um gegen illegales Filesharing als modernes Phänomen vorzugehen, aber gleichzeitig die als zu hoch empfundenen Strafen abzumildern; die Abhilfe erfolgte also wie jüngst in Deutschland rechtssetzend und nicht administrativ.[28] In Schweden wird für den Bereich der digitalen Inhalte und temporäre Kopien eine Ausnahme von der Zuweisung exklusiver Nutzungsrechte an den Rechteinhaber zugelassen. Solche Kopien werden als fortschrittsnotwendig und -förderlich gesehen.[29] In England und den USA wird nur teilweise eine Beschränkung der strikten Urheberrechtsregelungen vorgenommen.[30] Die mit der

---

für eine Datenschutzgrundverordnung der Kommission, tauchen „Verbraucher“ nicht als geschützter Personenkreis auf, siehe dazu Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM(2012) 11.

[24] Kapitel 2 des Regeringsform (1974:152); in den USA genießt das Copyright keinen verfassungsrechtlichen Rang. Die Copyright Clause in der Verfassung gibt dem Kongress nur die Kompetenz, ein Urheberrecht zu kreieren.

[25] Für die europäische Union bestehen ebenfalls harmonisierende Rechtsakte, wie beispielweise Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (2001/29/EG). Sowohl die internationalen als auch die europäischen Angleichungsinstrumente lassen den Bereich der Nutzung von urheberrechtlich geschützten Werke durch Verbraucher durch die digitale Welt jedoch weitgehend ohne Sonderregeln; mehr auf die Bedürfnisse der digitalen Welt eingehend jedoch die Empfehlungen von *António Vitorino* hinsichtlich der Abgaben für Privatkopien und sonstige Reproduktionsformen, abrufbar unter http://ec.europa.eu/internal_market/copyright/docs/levy_reform/130131_levies-vitorino-recommendations_en.pdf (zuletzt abgerufen am 2.11.2013).

[26] So zum Beispiel in den USA mit dem Digital Millenium Copyright Act

[27] Zu der beschränkten Anwendung des Grundsatzes von *fair use* siehe *Herden*, Länderbericht USA, 4.a.

[28] Siehe *Wichmann*, Länderbericht Frankreich, 1.a.bb) (2).

[29] Siehe dazu Länderbericht Schweden, *Kirchberger/Storr*, 1. B. aa). Voraussetzung ist allerding eine Kopie von einer legalen Vorlage.

[30] In England wird das reine Streaming wohl auch als rechtmäßig anzusehen sein, siehe *McNamee,* Länderbericht England, 1. B.; in den USA wird die *defence* des *fair use* für rein private Zwecke diskutiert, siehe *Herden*, Länderbericht USA, 4.a.

UsedSoft-Entscheidung des Europäischen Gerichtshofs erfolgte Ausweitung des Erschöpfungsgrundsatzes auf digital übermittelte Software,[31] könnte hier einen Teil der Konflikte auch für den Verbraucherbereich entschärfen aber zugleich mit erheblichen – teilweise auch datenschutzrelevanten – Ausweitungen von technischen Kopierschutzmechanismen einhergehen.

Die Urheberrechtsgesetze in allen vier Rechtsordnungen sehen überwiegend zivilrechtliche Strukturen vor. Verletzungen des Urheberrechts sind bilateral zwischen Verletzer und Urheberrechtsinhaber geltend zu machen, sodass der Rechteinhaber zivilrechtlich Schadenersatz[32] oder Unterlassung verlangen kann. Die dabei zu zahlenden Schadenssummen sind für die USA aufgrund der Möglichkeit der Anlehnung an einen festen Schadensrahmen oft erheblich.[33].Sofern die Urheberrechtsverletzung online begangen wurde, sind die Regelungen hinsichtlich der Erfragung des Verletzers zudem auch zivilrechtlich gestaltet.[34] Strafrechtliche Sanktionen oder Bußgelder[35], treten neben dieses zivilrechtliche Regelungssystem, beispielweise für die Umgehung technischer Schutzmaßnahmen[36] oder die Änderung jeglicher Information über elektronische Rechte[37], wobei in Schweden dabei auch eine Haftung der Hintermänner, wie beispielweise bestimmter Internetseiten, die zu Urheberrechtsverletzungen durch Rat oder Tat verleiten, besteht.[38]

Regelungen zur administrativen Durchsetzung des Urheberrechts sind in größerem Umfang allein in Frankreich und teilweise in England hinsichtlich der in diesen Rechtsordnungen *three strikes policy* bei Verletzungen des Urheberrechts durch das Internet zu finden. Die Überwachung der Einhaltung dieser *three strikes policy* obliegt den Verwaltungsbehörden.[39] Die Haute*Autorité pour la diffusion des œuvreset la protection des droits sur internet* (HADOPI) ist beispielsweise in Frankreich die zuständige staatliche Sonderbehörde. Nach dem dritten Verstoß sind Maßnahmen gegen den Inhaber des jeweiligen Anschlusses, bis zur Abkopplung vom Netz, vorzunehmen.

---

[31] EuGH, Urt. v. 3.7.2012, Rs. C-128/11.

[32]Etwa Kapitel 7 Artikel 54 des schwedischen Urheberrechts.

[33] Tatsächlich stellt die Anwendung der *statutory damages* einen großen Kritikpunkt bei der Durchsetzung von Urheberrechten gegenüber Privatpersonen dar, siehe *Herden,* Länderbericht USA, 4.a.; Kapitel 7 Artikel 54 des schwedischen Urheberrechts: In Schweden wird grundsätzlich „vernünftigen Ersatz“ für die unrechtmäßige Ausbeutung des Werkes sowie Ausgleich der entstandenen Schäden bei absichtlicher oder fahrlässiger Handlung gewährt.

[34] Determinierung der zivilrechtlichen Durchsetzung dabei auch durch die Richtlinie 2004/48/EC; so beispielweise für die IP Adressen und Nutzerinformationen. so zum Beispiel E-Book Case in Schweden.

[35] Kapitel 7 Artikel 53 des schwedischen Urheberrechts; ebenso speziell für das Filesharing in Frankreich das HADOPI 2 Gesetz sowie das DADSVI Gesetz.

[36] Artikel 57b (2) des schwedischen Urheberrechts.

[37] Artikel 57b (1) des schwedischen Urheberrechts.

[38] Kapitel 23 s. 4 des Schwedischen Strafgesetzbuches; siehe dazu auch die Entscheidung Pirate Bay, Urteil des Schwedischen Berufungsgericht, B 4041-09 vom 26. November 2010.

[39] Siehe dazu *McNamee*, Länderbericht England, 2. sowie *Wichmann,* Länderbericht Frankreich, 1.a.bb) 4) (b).

Eine verbraucherschützende Funktion wird dem Urheberrecht in den untersuchten Rechtsordnungen nicht ausdrücklich zugeschrieben.[40] Allein in Schweden scheint sich eine Ansicht der positive Aspekt der Nutzung digitaler Inhalte durch Verbraucher durchzusetzen.[41]

Die Kontrolle einer exzessiven Ausübung der Urheberrechte obliegt damit – wenn sie überhaupt erfolgt – allein den Gerichten, aber auch nur dann, wenn bestimmte Voraussetzungen vorliegen.[42] In Schweden ist bei Auskunftsersuchen des Anschlussinhabers einer IP-Adresse zu beachten, dass das Gericht die Interessen abwägen kann, Artikel 53c des Schwedischen Urheberrechts. Verbraucher- oder Nutzerinteressen fließen aber ganz überwiegend nur bei dem für die Feinjustierung der auf Privatpersonen bezogenen materiellen Ausnahmen vom Urheberrecht sowie der Durchsetzungsinstrumente erforderlichen Interessenausgleich ein.

2. Zusammenspiel von Urheberrecht und Datenschutz

Ein Zusammenspiel von Urheberrecht und Datenschutz, welche sich in der digitalen Welt in Form der Daten von Endnutzern und Urheberrechtsverletzungen durch diese Endnutzer ergibt, wird in den untersuchten Rechtsordnungen bislang oftmals zugunsten der Urheberrechtsinhaber gelöst: Die Internetserviceprovider sind in den USA durch Gesetz zur Preisgabe der Informationen über den Anschlussinhaber verpflichtet. Auch der EuGH hat bereits entschieden, dass zwar Urheberrechteinhaber Datenschutzbestimmungen zu beachten haben, dass jedoch, sofern allein begangene Urheberrechtsverletzungen sanktioniert werden sollen, die Preisgabe von personenbezogenen Daten für den Zweck der Geltendmachung zivilrechtlicher Ansprüche erlaubt ist.[43] Datenschutz sowie das US-amerikanischer Pendant der *consumer privacy* sind damit nur bis zur Grenze des Urheberrechts geschützt.[44] In Frankreich stand die Frage des Schutzes persönlicher Daten insbesondere im Rahmen des *response graduee* und der Ermittlung des Anschlussinhabers durch Übermittlung der IP-Adresse lange in der Diskussion.[45]

---

[40] In den USA wird zwar argumentiert, dass solche Funktionen dem Copyright Act zu entnehmen seien, dies ist für die digitale Welt jedoch wohl abzulehnen, siehe *Herden*, Länderbericht USA, 4.c.

[41] Siehe zu der Frage einer verbraucherschützenden Ausrichtung des Urheberrechts auch das Positionspapier des Ministeriums für den Ländlichem Raum und Verbraucherschutz Baden-Württemberg und des Verbraucherzentrale Bundesverband e.V. „Urheberrecht 2.0 – Wo bleiben die Verbraucher“, abrufbar unter http://www.vzbv.de/cps/rde/xbcr/vzbv/Urheberrecht-wo-bleiben-die-verbraucher-Positionspapier_vzbv-mlr_vzbv.pdf (zuletzt abgerufen am 13.11.2013).

[42] Schweden: Privatkopie und Schadenersatz nur als „vernünftigen Ausgleich“; USA: sehr enge Anwendung von *fair use* bei hohen *statutory damages*.

[43] In ähnlicher Weise liegt dem EuGH derzeit eine Vorlage des BGH vor, indem die Kollision des Interesse an der Geltendmachung der markenrechtlichen Ansprüche und des Bankgeheimnisses Gegenstand der Vorlagefrage ist, siehe BGH Beschluss vom 17.10.2013, I ZR 51/12.

[44] Ephone Case, Entscheidung des Schwedischen Obersten Gerichts vom 21.12.2012, Ö 4817-09; in den USA fehlt eine generelle Debatte zum Urheberrecht, Verbraucherschutz und Datenschutz hingegen als Schnittmenge der Probleme aus der digitalen Welt für Verbraucher.

[45] Siehe *Wichmann*, Länderbericht Frankreich, 1. B. bb) (2).

II. Behördenstrukturen

1. Behördliche Rechtsdurchsetzung im Allgemeinen sowie zum Schutz des Verbrauchers

Für die behördliche Überwachung und Rechtsdurchsetzung in der digitalen Welt sind verschiedene Aspekte relevant. Zu nennen sind insbesondere die Funktion der Behörde, deren Selbstverständnis, der Aufbau sowie die personelle und sachliche Ausstattung. An dieser Stelle kann auf die unterschiedlichen Behördenstrukturen und -verständnisse nur im Allgemeinen eingegangen werden. Hinsichtlich der Stellung der Behörden im Staat bestehen zum Teil erheblich Unterschiede. So sind die Behörden in Schweden grundsätzlich sowohl frei von parlamentarischer als auch von exekutiver Kontrolle.[46]

Die behördliche Durchsetzung des Verbraucherschutzes ist bedingt durch den Ansatz des Verbraucherschutzes als auch durch die vorhandenen Regelungsstrukturen. Das deutsche Konzept des Verbraucherschutzes agiert mit verschiedenen Instrumenten, bekanntlich aber vor allem aber auch mit der Gewährung subjektiver Rechte für den Verbraucher. Die behördliche Durchsetzung des Verbraucherrechts beschränkt sich größtenteils auf die Gewährleistung dieser zivilrechtlichen Regelungsinstrumente, lauterkeitsrechtliche Marktaufsichtsmittel sowie die Verfolgung von Ordnungswidrigkeiten. Eine große Anzahl abstrakter und genereller Regelungen in Gesetzes- oder Verordnungsform regeln vor allem zivilrechtliche Verhältnisse und die subjektiven Rechte der Beteiligten. Marktzugangsregeln werden zwar vielfach durch Behörden administriert und durchgesetzt sind jedoch selten allein auf Verbraucherschutz hin orientiert.

In den USA ist der Ansatz des Verbraucherschutzes hingegen weniger eingreifend. Die Bundesbehörden – wie beispielweise die *Federal Trade Commission* (FTC) – wie auch die einzeölstaatlichen Behörden für den Verbraucherschutz – als eigenständige Behörden oder Abteilungen unter dem jeweils zuständigen *Attorney General* – verfolgen in großem Maße das Modell der Selbstregulierung durch den Markt. Sind einzelne Missstände ersichtlich, werden in der Regel in einem ersten Schritt behördliche Maßnahmen gegen die betreffenden Unternehmen aufgrund der allgemeinen Marktaufsichtsbefugnis erlassen. Bei weit verbreitenden Missständen, können die jeweils zuständigen Behörden auch abstrakt-generelle Normen erlassen. Oftmals wird in einem solchen Fall dann auch vermehrt ein Augenmerk auf Verbraucherinformation gelegt. Verstöße gegen die Anordnungen im Einzelfall als auch gegen die Regelungen können mit empfindlichen Bußgeldern belegt werden. Die zuständigen Bundesbehörden oder staatlichen Behörden können Klage zur Durchsetzung dieser Bußgelder als auch eine Massenklage im Name aller Verbraucher erheben. Ein Vorgehen gegen die Unternehmen erfolgt oftmals beispielhaft an einem Unternehmen, wobei meist nach Einleitung des formellen Verfahrens eine Einigung erreicht wird.

Gesetzgeberische Maßnahmen werden erst dann erlassen, wenn auf andere Weise die Missstände nicht gelöst werden können. Die zuständigen Verbraucherbehörden – wie beispielweise die gewählten Attorneys General- nehmen am Gesetzgebungsprozess durch eigene Entwürfe oder Stellungnahmen aktiv teil. Verbrauchergesetze aber auch behördliche Normsetzung sind zu-

[46] Kapitel 12 Artikel 2 Regeringsform (1974:152).

meist Regelungen für einen spezifischen Einzelfall, ohne darüberhinaus auch ähnliche Sachverhalte mit zu erfassen.[47] Dies bedingt auch sehr punktuelle Eingriffsbefugnisse der Behörden. Subjektive Rechte für Verbraucher werden vergleichsweise wenig und wenn durch Regelungen in den einzelnen Bundesstaaten gewährt, so dass der behördlichen Marktaufsicht eine größere Rolle zur Durchsetzung zukommt. Diese erfolgt nicht im Interesse des Einzelnen, sondern zur Verbesserung des Marktes für die Verbraucher insgesamt.

Dieser marktbezogene Ansatz des Verbraucherschutzes lässt sich aber auch in den anderen untersuchten Rechtsordnungen finden. In England, Frankreich und Schweden sind die jeweiligen Verbraucherbehörden gerade als Marktaufsichtsbehörde tätig. Die *Konsumentverket/Konsumentombudsmannen* (KO)[48] ist ebenso wie das *Office for Fair Trading* (OFT) in England oder die *Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes* (DGCCRF) in Frankreich eine Marktüberwachungsbehörde zum Schutz der Verbraucher. Eine individuelle Rechtsdurchsetzung oder Beratung der einzelnen Verbraucher findet in diesen Behörden hingegen nicht statt.[49] Die Behörden dienen den Verbrauchern nur als Anlauf- und Beschwerdestelle. In Schweden ist neben dieser marktbezogenen Aufsichtsbehörde jedoch die allgemeine Beschwerdestelle, die *Allmänna reklamationsnämnden* (ARN) vorhanden, welche als Streitbeilegungsstelle für verbraucherrechtliche Streitigkeiten tätig wird.[50].

2. Keine eigenständige Behördenstruktur für die digitale Welt im Hinblick auf Verbraucher

Eine eigenständige Behördenstruktur für die digitale Welt ist in den untersuchten Rechtsordnungen nicht zu finden. Verbraucherschutz und Datenschutz werden in den untersuchten europäischen Rechtsordnungen sowohl hinsichtlich der Regelungen als auch der Behördenstruktur und Behördenbefugnisse getrennt betrachtet.[51] In den USA ist insoweit aufgrund der Konstruktion der Regelungen zur *consumer privacy* keine wirkliche Divergenz zwischen Verbraucherschutz und Datenschutz gegeben.

a. Behörden zur Durchsetzung des Datenschutzes

In den USA fehlen eigenständige Aufsichtsbehörden zum Datenschutz, auch wenn der FTC unter der Kompetenz der „*unfair and decpetive trade practices*“ ebenso wie den Verbraucherschutzbehörden oder Attorneys General der Bundesstaaten eine Kompetenz zum Schutz der *consumer privacy* zuschreiben lässt.[52]

---

[47] Anders jetzt der California Online Privacy Protection Act, der erstmals sektorunabhängig für Websites gilt.

[48] Rechtsgrundlagen für die KO sind zum einen Förordning (2009:607) med instruktion för Konsumentverket, amended by Förordning (2011:1218) om ändring i förordningen (2009:607) med instruktion för Konsumentverket sowie die allgemeine Regelungen für Behörden enthaltene Myndighetesförordning (2007:515).

[49] Eine individuelle Beratung erfolgt in Schweden durch konsumentvägledare und spezielle Beratungsbüros (rådgivningsbyråer); Letzere werden von Industrie und öffentlichen Behörden zusammengeleitet. Beispiel: *Telekområdgivarna*

[50] Rechstgrundlage ist Förordning (2007:1041) med instruktion för Allmänna reklamationsnämnden.

[51] Eine Ausnahme kann dabei im Einzelfall das Direktmarketing sein, wenn unerlaubt Emails an einen Verbraucher versandt wird.

[52] Siehe oben 1.a.

In der europäischen Union fordert die Datenschutzrichtlinie 95/46/EG von den Mitgliedsstaaten unabhängige Datenschutzbehörden.[53] In Schweden ist dies die *Datainspektionen*, in England das *Information Commissioners Office* (ICO) sowie in Frankreich die *Commission nationale de l'informatique et des libertés* (CNIL). Neben den genuinen Datenschutzbehörden üben fachspezifische Behörden ebenfalls datenschutzrechtliche Aufsichtsaufgaben aus.[54] Bei den Beratungen zur Datenschutzgrundverordnung der Europäischen Union wird derzeit ein One-stop-one-shop-Modell für die Datenverarbeitungsprozesse in der Europäischen Union erwogen.[55] Dies hätte eine Monopolisierung der datenschutzrechtlichen Aufsicht zur Folge, deren Abgrenzung von den allgemeinen Wirtschaftsverwaltungs- und Verbraucherschutzbehörden erhebliche Schwierigkeiten bereiten würde.

Die Datenschutzbehörden wie auch die fachspezifischen Behörden sind dabei nicht notwendigerweise auf die digitale Welt im Sinne eines Zugangs zum Internet beschränkt. In den untersuchten europäischen Rechtsordnungen Schweden, England und Frankreich ist aber mit den Datenschutzbehörden ein grundlegender Bereich der digitalen Welt erfasst. Dieser betrifft jedoch allein die Datenverarbeitung als solche und nicht andere Risiken für Bürger und Verbraucher etwa die Gefahren der Begehung von Urheberrechtsverletzungen oder Nachteile aus unfairen Verträgen. Auch als Folge dieser Beschränkung auf die Datenverarbeitungen als solche, sind die Datenschutzaufsichtsbehörden keine markgerichteten Behörden, welche den Markt beaufsichtigen und den Zugang zu ihm beschränken können. In den USA ist zwar eine stärkere marktgerichtete Aufsicht für den Bereich der *consumer privacy* gegeben, doch ist auch hier keine Kompetenz der FTC zur Verdrängung von Marktteilnehmern aufgrund wiederholter Rechtsverstöße ersichtlich. In keiner der untersuchten Rechtsordnungen können Datenschutzbehörden Unternehmen insgesamt vom Markt verbannen – sei es durch Verbot der Tätigkeit sei es durch Entzug der erforderlichen Erlaubnis.

b. Zusammenspiel von Datenschutz und Verbraucherschutz hinsichtlich der Behördenstruktur:

In den untersuchten Rechtsordnungen werden Datenschutz und Verbraucherschutz auch hinsichtlich der Behördenstruktur bislang als separate Regelungskomplexe und Handlungsfelder wahrgenommen, ohne daß sich dort jeweils darüber Rechenschaft abgelegt werden würde.. Die Datenschutzbehörden sehen sich damit nicht zwangsläufig in einer Verbraucherschutzfunktion im engeren Sinne.[56] Eine solche Überschneidung lässt allein langsam die OFT erkennen.[57] Nur für einzelne Sektoren wie für die Telekommunikation sind wirtschaftlicher Verbraucherschutz und Datenschutz auch auf der Ebene der Behördenstruktur verbunden: So sind beispielsweise eigenständige Behörden für den Telekommunikationsbereich vorhanden, denen beide Aufgabenfelder obliegen.[58] Umgekehrt setzt die schwedische Datenschutzbehörde (Datainspektionen) neben den

[53] Siehe dazu die Entscheidungen des EuGH vom 09.03.2010, C-518/07 sowie vom 16.10.2012, C-614/10.

[54] So beispielsweise in England für den Bereich der Telekommunikation die Ofcom, *McNamee,* Länderbericht England, 1.c. aa).

[55] Artikel 51 (1) Entwurf für eine Datenschutzgrundverordnung KOM(2012) 11.

[56] So ausdrücklich *Wichmann*, Länderbericht Frankreich, 3.a. zum Verbraucherschutzverständnis der CNIL.

[57] Siehe oben in der Einleitung zu C.

[58] In Schweden ist so zum Beispiel die Post- och telestyrelsen (PTS) zuständig, in den USA auf förderaler Ebene die Federal Communications Commission (FCC), in England die Ofcom.

Bestimmungen des Personal Data Act zudem auch die Bestimmungen des schwedischen Credit Information Acts und des Debt Recovery Act durch.

Wenn in den USA gleichwohl ein Zusammenspiel der beiden Regelungskomplexe in den Verwaltungszuständigkeiten ist, liegt das weniger an einer gezielten rechtspolitisch motivierten Zusammenfassung als vielmehr am Fehlen eines ausgeprägten materiellen Datenschutzes und – konsequenterweise – entsprechender Behörden zu dessen Durchsetzung. Empfundene Schutzdefizite lassen sich weitgehend durch das Konzept der *unfair and deceptive trade practices* abfangen.

Auch auf europäischer Ebene wurden in den normativen Verlautbarungen der Organe der Europäischen Union Datenschutz und Verbraucherschutz bislang als unterschiedliche Regelungsmaterien gesehen. In der Empfehlung der Kommission zur kollektiven Geltendmachung von Schadenersatzansprüchen wird nun jedoch erstmals ersichtlich eine Behörde als mögliche funktionale Einheit zur Durchsetzung der Interessen von Verbrauchern auch auf dem Gebiet des Datenschutzes genannt.[59] Die Anwendbarkeit des europäischen Verbraucherrechts auf datenschutzrelevante Sachverhalte wird hingegen bislang kaum diskutiert.[60] Es wäre freilich auch für die Europäische Union vorstellbar, die Bekämpfung unfairer Geschäftspraktiken im Sinne der UGP-Richtlinie 2005/29/EG für den Datenschutz fruchtbar zu machen.[61]

c. Dualität von Marktaufsicht und Datenschutz

Mit Ausnahme der USA lässt sich eine Dualität von Datenschutzbehörden und Verbraucherbehörden in den untersuchten Rechtsordnungen feststellen. Die Verbraucherbehörden sind dabei zudem sektoral oder fachspezifisch untergliedert, so dass an dieser Stelle nur auf die wichtigsten Behörden eingegangen wird. In Schweden ist neben dem KO und der *Post and Telecom Authority* (PTS) als Aufsichtsbehörde für den Telekommunikationssektor das *Allmänna reklamationsnämnden* zu nennen, welche verbraucherbezogene Aufgaben erfüllen. Die KO dient als Marktaufsichtsbehörde für die unlauteren Geschäftspraktiken, wohingegen das *Allmänna reklamationsnämnden* als Streitbeilegungsstelle tätig ist. In England ist neben dem OFT als generelle Marktaufsichtsbehörde das *Office of Communications* (Ofcom) als Regulierungsbehörde für den Kommunikationsbereich vorhanden. In gleicher Weise ist in Frankreich eine marktausgerichtete Verbraucherbehörde vorhanden (Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes) und die CNIL als Datenschutzbehörde. In den USA sind insbesondere die FTC als auch die FCC (Federal Communications Commission) sowie die staatlichen Verbraucherbehörden und Attorneys General zu nennen.

d. Selbstverständnis der betreffenden Behörden

Die Verbraucherbehörden in allen untersuchten Rechtsordnungen sehen sich in einer Position der Überwachung des Marktes. In England erfolgt durch die Anlehnung an die von Parlament und

---

[59] Empfehlung der Kommission vom 11.06.2013, Gemeinsame Grundsätze kollektive Unterlassungs- und Schadensersatzverfahren in den Mitgliedstaaten bei Verletzung von durch Unionsrecht garantierten Rechten, Abl. EU L 201/60 vom 26.7.2013.

[60] Grundlegend zur Anwendung der ADR-Richtlinie auf datenschutzrechtliche Fragen nunmehr *Herden*, GPR 2013, 272, wo die Anwendung abgelehnt wird. In der ADR-Richtlinie werden die nationalen Behörden nur als Aufsichtsbehörden für die Feststellung, ob die AS-Stelle die Kriterien der Richtlinie erfüllen, genannt, Artikel 15 ADR-Richtlinie.

[61] Unter dem deutschen zivilrechtlichen Ansatz wird dies von den Zivilgerichten vielfach so gesehen: OLG Karlsruhe NJW 2012, 3312; HOLG Hamburg GRUR-RR 2013, 482. Anders freilich OLG München MMR 2012, 317.

Regierung als wichtig gekennzeichneten Punkte noch eine relativ enge Anlehnung an von außen kommende Vorgaben, wohingegen die schwedischen Verbraucherbehörden schon allein aufgrund ihrer unabhängigen Stellung eine solche enge Abstimmung nicht für notwendig erachten. Dennoch ist auch hier eine enge Absprache mit dem Parlament und der Regierung ersichtlich.

Die Verbraucherbehörden setzen in einem hohen Maße auf Informationen an Verbraucher aber auch auf die Informationsgewinnung durch die Verbraucher. In den untersuchten Rechtsordnungen können sich Verbraucher an die eingerichteten Beschwerdestellen wenden, welche dann die Behörden als eine maßgebliche Informationsquelle dienen. Andererseits sehen sich die Behörden in einer aufklärerischen Rolle, welcher sie durch allgemeine Informationen an die Verbraucher nachkommen. Eine ausreichende Verbraucherinformation wird als maßgebliche Marktlenkungsmaßnahme verstanden. Marktkorrigierende Maßnahmen werden erst als sekundäre Mittel betrachtet. In den untersuchten Rechtsordnungen wird von diesen eingreifenden Maßnahmen nur zurückhaltend und punktuell Gebraucht gemacht. Vielmehr wird versucht, bereits informell Konflikte zu lösen oder durch informatorische Maßnahmen an die Unternehmen solche nicht entstehen zu lassen.

Die Verbraucherbehörden in den untersuchten Rechtsordnungen sehen sich in erster Linie nicht als Organisation zur Durchsetzung individueller Rechte oder Verhinderung einzelner Schädigungen. Vorteile und Nutzen für die Verbraucher werden grundsätzlich als Ganzes und auf die Entwicklung für die Zukunft betrachtet. In Schweden wird der Direktor des KO im Rahmen seiner Ombudsmanfunktion jedoch auch teilweise für den einzelnen Verbraucher tätig, was auch seine besonders starke Stellung mit erklärt.

Die Datenschutzbehörden in England, Schweden und Frankreich sind schon aufgrund ihrer europarechtlichen Vorgaben zur effektiven und unabhängigen Durchsetzung des Datenschutzrechts berufen. Allerdings sehen sich auch die Datenschutzbehörden in einer stark auf Information ausgerichteten Rolle. Beim englischen ICO ist über die reine informatorische Tätigkeit hinauseine klare Kooperationsbereitschaft – beispielsweise durch freiwillige Audits–zwischen Unternehmen und ICO erkennbar.[62] Die französische Datenschutzaufsicht erarbeitet in Kooperation mit den betroffenen Datenverarbeitern Berufsregelungen. Zudem vergibt sie nach einem kostenpflichtigen Verfahren für die Unternehmen datenschutzrechtliche Gütesiegel.

An der Spitze der Behörden sind einzelne Direktoren[63] oder Gremien[64] zu finden. Inwieweit diese obersten Behördenvertreter das Selbstverständnis oder interne Politik der Behörden maßgeblich prägen, wurde von den Länderberichterstattern nicht besonders hervorgehoben. Die Behördenvertreter der unabhängigen Behörden werden direkt von den Staatsoberhäuptern, bzw. Regierungen oder Parlamenten ernannt werden. Die Benennung bestimmter Personen kann im Einzelfall von der politischen Situation beeinflusst sein.

---

[62] Zu den einzelnen Formen des Audits *McNamee*, Länderbericht England, 3. C. cc) (1).

[63] So der Information Commissioner in England, der Vorsitzende der FTC in den USA und neuerdings der DIrektor der Datainspektionen in Schweden.

[64] Beratend zu Seite stehen dem Direktor des Datainspektionen ein Advisory Council; ebenso sind einige Aufgaben der FTC nur durch Mehrheitsentscheidungen der gesamten Federal Trade Commission möglich; ein besonders großes Gremium ist auch die CNIL, welche aus 17 Mitgliedern besteht.

3. Keine Behördenstruktur für Urheberrecht

Hinsichtlich des Urheberrechts sind keine Aufsichtsbehörden für die Durchsetzung des Urheberrechts noch eine Aufsicht bei einer solchen Durchsetzung durch die geschädigten Urheberrechteinhaber vorhanden. Die Aufgabe der Durchsetzung einzelnes Aspekte des Urheberrechts, beispielsweise der *three-strikes-policy*, obliegt den zuständigen Verwaltungsbehörden, wobei in Frankreich mit der HADOPI eine Sonderbehörde geschaffen wurde. Inwieweit kartellrechtliche Aufsichtsstrukturen für den Bereich des Urheberrechts verwendet werden, wird von den Länderberichterstattern nicht erörtert.

4. Zusammenspiel zwischen den Behörden

Kompetenzüberschneidungen der für den Bereich der digitalen Welt zuständigen Behörden sind nicht ersichtlich. Zwar sind gemeinsame Zuständigkeiten in Einzelfällen möglich[65], dies scheint jedoch keine Probleme in den jeweiligen Rechtsordnungen zu verursachen. Wird der Verbraucherdatenschutz in den untersuchten Rechtsordnungen nicht als echte Schnittmenge zwischen Datenschutz und Verbraucherschutz und damit eigenständige Regelungsmaterie wahrgenommen, überrascht das fehlende Kompetenzproblem nicht. Durch die für die Zukunft voraussichtlich erwogene stärkere Monopolisierung der datenschutzrechtlichen Aufsicht[66] könnten sich gegebenenfalls Kompetenzüberschneidungen der Marktaufsichtsbehörden eines Landes und der zuständigen Datenschutzaufsicht in einem anderen Mitgliedsland der EU ergeben.

III. Behördliches Instrumentarium

Den verschiedenen einschlägigen Behörden der untersuchten Rechtsordnungen steht ein sehr breites Instrumentarium zur Verfügung. Dabei sind die Vorstellungen von Möglichkeiten und Grenzen, von Aufsicht, Weisungsrechten und Rechtsschutz im Einzelnen höchst unterschiedlich. Diese Unterschiede betreffen sowohl allgemeine Faktoren behördlichen Handelns wie auch die verschiedenen Maßnahmetypen.

Die Rechtsqualität der Handlungen der hier relevanten Behörden ist von den Berichtserstattern nicht diskutiert worden. Eine Klärung dieser Frage fehlt in den untersuchten rechtsordnungen oftmals schon grundsätzlich.[67] Eine klare Unterscheidung zwischen „öffentlichem“ und „zivilem“ Handeln, wie sie für das deutsche Recht vorliegt, ist nicht in allen untersuchten Rechtsordnungen gegeben. Für die grenzüberschreitende Durchsetzung ist eine Klärung dieser Frage jedoch oftmals essentiell, da sich die behördlichen Handlungsbefugnisse im Ausgangspunkt auf das jeweilige Staatengebiet beschränken und die Normen des internationalen Verwaltungsrechts und der grenzüberschreitenden Behördenkooperation sehr stark von denen des Internationalen Privatrechts und der justiziellen Zusammenarbeit in Zivilsachen unterscheiden.

---

[65] So grundsätzlich für das US-amerikanische Recht für die FTC und die FCC.

[66] Der Entwurf für eine Datenschutzgrundverordnung sieht in Artikel 51 (2) die ausschließliche Zuständigkeit einer Datenschutzaufsichtsbehörde eines Mitgliedsstaates, in der ein datenverarbeitendes Unternehmen seinen Hauptsitz hat, auch für die Niederlassungen eines Unternehmens in den anderen Mitgliedsstaaten vor.

[67] Siehe für Siehe *Kleve/Schirmer*, England und Wales, in: Schneider (Hrsg.), Verwaltungsrecht in Europa (2007), 35, 96: keine verwaltungsverfahrensrechtliche Handlungsformenlehre als Folge der nach wie vor nicht restlos abeschlossnen Emanzipation vom Privatrecht.

1. Faktoren für das Instrumentarium der berufenen Behörden

a. Zweck und Funktion

Die Nutzung des den einzelnen Behörden zur Verfügung stehenden Instrumentariums orientiert sich in sämtlichen untersuchten Rechtsordnungen am generellen Zweck und der Funktion der jeweiligen Behörden. Dabei sind – auch im Blick auf die verschiedenen Gegenstände der Verwaltungstätigkeit – unterschiedliche Akzente zu erkennen: Teilweise geht es – entsprechend der generellen Doppelfunktion von verbaucherschützender Verwaltungstätigkeit – um die schlichte Durchsetzung vorhandener Standards, teilweise steht mehr die auf eine präventive Marktüberwachung folgende flexiblere Reaktion im Mittelpunkt.

So haben die Datenschutzaufsichtsbehörden in Frankreich, England und Schweden den durch die Datenschutzrichtlinie determinierten Auftrag der effektiven Durchsetzung des Datenschutzrechts. Die Verbraucher-, bzw. Marktaufsichtsbehörden in Schweden, England und Frankreich sind hingegen für die Vermeidung und Beseitigung irreführender Praktiken und damit der Herstellung eines funktionierenden Marktes für die Verbraucher zuständig und verfügen bereits durch die offenere Zielvorgabe über mehr Spielräume. Auch die Federal Trade Commission (FTC) in den USA ist Marktaufsichtsbehörde in diesem Sinn, welche zudem den Datenschutz als eine solche Marktbedingung versteht und auf diesem Weg einen Aspekt des Verbraucherdatenschutzes gewährleistet.

Insgesamt steht für die digitale Welt die Durchsetzungsfunktion behördlichen Handelns bislang deutlich im Vordergrund, zumal für eine echte Marktüberwachung die Kapazitäten der Überwachung und Ermittlung regelmäßig viel zu begrenzt sind. Eine Übertragung der Trägerschaft von Einrichtungen der Alternativen Streitschlichtung könnte hier eine erhebliche Stärkung der betreffenden Behörden bedeuten.

b. Ermessensspielräume

Eigene Ermessensspielräume der jeweiligen Behörden in den untersuchten Rechtsordnungen divergieren hinsichtlich der Konkretisierung der rechtlichen Regelungen aber auch der politischen Handlungsspielräume:

Die datenschutzrechtlichen Aufsichtsbehörden in England, Schweden und Frankreich sind an die Vorgaben der Datenschutzrichtlinie gebunden, welche eine effektive Durchsetzung der datenschutzrechtlichen Vorgaben fordert. Sofern nationale Umsetzungen und Anwendungen in der Rechtsprechung jedoch eigene Lösungswege darstellen, kann dies Auswirkungen auf die Spielräume der betreffenden Behörden haben. Die Unabhängigkeit der europäischen Datenschutzaufsichtsbehörden macht sie jedoch vom Ansatz her freier in ihrer Aufsichtsaufgabe als dies bei Behörden der Fall ist, welche durch Aufsichts- und insbesondere Weisungsbefugnisse in eine administrative Hierarchie eingebunden sind.

Eine ähnlich unabhängige Stellung weisen auch die KO in Schweden und die FTC in den USA als Verbraucher- und Marktaufsichtsbehörden auf.[68] Die eingeräumten Spielräume schlagen sich zum Beispiel in der Möglichkeit der Auswahl der Verfahrensweisen und der zu untersuchenden

[68] Auch das Office of Fair Trading in England gilt nach dem Enterprise Act 2002 als „non-ministerial government department".

Unternehmen am Markt aus. Eine Pflicht zur Ergreifung bestimmter Maßnahmen gegen einzelne Unternehmen oder zum Schutz des einzelnen, individuellen Verbrauchers gibt es in keiner der untersuchten Rechtsordnungen. Die Verbraucher- bzw. Marktaufsichtsbehörden sehen sich gerade nicht in der Aufgabe der Annahme eines Einzelfalles, sondern zur Optimierung der Situation für die Verbraucher insgesamt.

2. Erkennen: Tatsachenermittlung, Verbraucherbeschwerden, ADR und Schiedsverfahren

a. Informationsabfrage bei den Unternehmen durch die Behörde

Ermittlungsbefugnisse sind die Basis jeder Verwaltungstätigkeit, soll diese nicht rein durch Zufälle ausgelöst werden. Besteht ein Grund zu Annahme eines rechtswidrigen Verhaltens der Unternehmen, stehen den Behörden unterschiedliche Mittel zur Gewinnung von Informationen zur Verfügung. In England, Frankreich, USA und Schweden haben die Behörden nach eingegangenen Beschwerden oder bei eigenen Ermittlungen die Möglichkeit mit behördlichen Anordnungen die Unternehmen zur Angabe von Informationen oder Übersendung von Unterlagen zu zwingen. In England fehlt es an autonomen Betretungsrechten des ICO als reguläres Handlungsinstrument ohne richterliche Genehmigung, während die schwedische Datenschutzaufsicht im Einzelfall auch die Möglichkeit der Durchsuchung der betroffenen Unternehmen und deren Grundstücken hat.

b. Auditing und Zertifizierung

Neben der reinen Informationsabfrage bei Unternehmen (wie auch Informationweitergabe an Unternehmen), setzen insbesondere die englische und die französische Datenschutzaufsicht auf eine Kooperation mit den Unternehmen und nähere Prüfung der Datenverarbeitungsprozesse. Das englische ICO[69] als Aufsichtsbehörde für den Datenschutz verfolgt in großem Maße das Konzept des Auditing, wobei ein solches Audit sowohl freiwillig als auch angeordnet erfolgen kann. Dabei werden nicht alle möglichen Fragen des Datenschutzes in einem solchen Audit überprüft, sondern nur ausgewählte Aspekte. Die CNIL in Frankreich vergibt nach einem für die Unternehmen kostenpflichtigen Verfahren und positivem Ergebnis ein datenschutzrechtliches Gütesiegel.

c. Beschwerdestelle und Anlaufstelle für Verbraucher

Die Datenschutz- und Verbraucherschutzbehörden sind in allen Rechtsordnungen Anlaufstellen für die Verbraucher. Die Aufnahme von Beschwerden dient dabei vor allem als Informationsquelle für die Behörden, nicht jedoch der Problemlösung im Einzelfall. Eine Beratung erfolgt durch die betreffenden Behörden nicht, auch wenn im Einzelfall die Behörde aufgrund einzelner Beschwerden das direkte Gespräch mit den Unternehmen sucht. Oftmals verweisen die Anlaufstellen dann an die jeweiligen Beratungsstellen der Verbraucherverbände oder wie in Schweden an das *Allmänna reklamationsnämnden* als relevante Schiedsstelle. Auch gibt es in Schweden die Besonderheit der von Unternehmen und Behörden gemeinsam getragenen Beratungsstellen für Verbraucher, welche organisatorisch von der KO als Verbraucherbehörde getrennt ist.[70]

---

[69] Für die anderen Rechtsordnungen wird von einem solchen Audit für den Bereich des Datenschutzrechts als auch des Verbraucherrechts und der zuständigen Behörden nicht berichtet.

[70] Siehe dazu im Näheren *Kirchberger/Storr*, Länderbericht Schweden, 3. a..

d. Streitbeilegung

In Schweden findet sich die Besonderheit einer staatlich geführten allgemeinen Schieds- oder Schlichtungsstelle für Verbraucherstreitigkeiten. Das *Allmänna reklamationsnämnden* wird als behördliche Organisation geführt. Verbraucher können sich an das *Allmänna reklamationsnämnden* wenden, welches dann versucht eine Einigung zwischen Unternehmer und Verbraucher herbeizuführen. Auch die Berichte des *Allmänna reklamationsnämnden* sind für alle Beteiligten eine wichtige Erkenntnisquelle.

3. Informieren: Verbraucherberatung, Politikberatung und Information der Öffentlichkeit

a. Informationen an Verbraucher und Unternehmen

In allen untersuchten Rechtsordnungen geben die jeweiligen Verbraucher- und Datenschutzbehörden Informationen an Verbraucher und Unternehmen heraus. Diese Funktion der Informierung von Verbrauchern und Unternehmen macht nach den Befunden der Länderberichte einen großen Anteil der behördlichen Aktivitäten aus.

b. Herausgabe von Berichten

Die Datenschutz- und Verbraucherschutzbehörden sind in den untersuchten Rechtsordnungen entweder zur Herausgabe von Berichten verpflichtet oder geben diese auf freiwilliger Basis heraus. Bei großer Unabhängigkeit der Behörden wie in Schweden und den USA für die Verbraucherschutzbehörden, wie aber auch für die Datenschutzbehörden, dienen solche Berichte oftmals der Rechenschaft über die eigenen Tätigkeiten. Für die Marktteilnehmer sind diese Berichte auch deshalb von Interesse, weil sie auch die Haltung der Behörden zu bestimmten rechtlichen Punkten als auch die Tätigkeitsschwerpunkte wiedergeben. Funktional sind sie vielfach Rechts- zumindest aber Rechtserkenntnisquelle.

4. Handeln: Maßnahmen für den Einzelfall, Normsetzung, Sanktionen

a. Regelungen und Anordnungen im Einzelfall

Bei Feststellung von unrechtmäßigen Verhalten können alle Aufsichtsbehörden in den untersuchten Rechtsordnungen Anordnungen erlassen, welche die Feststellung rechtswidrigen Verhaltens, Unterlassung bestimmter Verhaltensweisen oder Verpflichtung zur Vornahme bestimmter Handlungen enthalten können. Bei den datenschutzrechtlichen Aufsichtsbehörden beschränkt sich die Anordnung auf die Datenverarbeitungsprozesse. Bei den Verbraucherschutzbehörden sind die Anordnungen zumeist auf die jeweiligen Handlungen gegenüber den Verbauchern beschränkt. Die Anordnungen der Behörden sind damit rein handlungsbezogen. Eine Bereinigung des Marktes von den Akteuren, die wiederholt gegen die Bestimmungen zum Schutz der Verbraucher verstoßen, ist direkt nicht möglich. Inwieweit die Verbraucherbehörden bei wiederholten Datenschutzverstöße im Rahmen ihrer Kompetenzen eingreifen, wurde für England, Schweden und Frankreich nicht berichtet. Durch die marktbezogene Sichtweise der Regelungen zur *consumer privacy* kann die FTC als Verbraucherbehörde auch bei „Datenschutzverstößen“ eingreifen.

Gegen die Anordnungen im Einzelfall ist in allen Rechtsordnungen die Möglichkeit der Überprüfung möglich, wobei diese entweder durch die erlassende Behörde selbst, einen bestimmten Gerichtszweig oder administrative oder zivile Gerichte erfolgt. In Schweden findet sich die Besonderheit für den Fall, die Rechtslage hinsichtlich eines Punktes ungeklärt ist; die KO erlässt dann keine

Anordnung, sondern bringt den Fall vor Gericht, um eine Klärung herbeizuführen.[71] Wird eine Klage des KO direkt beim Market Court erhoben, so ist gegen dessen Entscheidung keine Berufungsmöglichkeit gegeben.

b. Durchsetzung individueller Verbraucherrechte

Die Verbraucherbehörden und Datenschutzbehörden werden zwar für die Verbraucher im Allgemeinen tätig, jedoch fehlt überwiegend sowohl eine allgemeine Beratung im Einzelfall als auch eine individuelle Rechtsdurchsetzung oder -durchsetzungshilfe durch die Behörden.[72]

Grundsätzlich dienen die Behörden als reine Anlauf- und Beschwerdestellen für Verbraucher. Eine Beratung erfolgt in Schweden durch KonsumentEuropa als Untereinheit der KO nur bei grenzüberschreitenden Sachverhalten. Ansonsten sind in Schweden auch Beratungsbüros vorhanden, welche gemeinschaftlich von Industrie und Staat getragen werden, in denen sich die Verbraucher beraten lassen können. Die bei den Behörden eingereichten Beschwerden sind für die Behörden jedoch entscheidend für ihre Tätigkeit, da sie den Behörden als Informationsquelle für die Marktsituation und damit als Kriterien für ihr behördliches Handeln dienen. In den USA beispielsweise werden die Beschwerden in einer umfangreichen Datenbank gesammelt, auf die mehrere Behörden gleichzeitig Zugriff haben, um so den Datenfluss zu bündeln. Auch in England dienen die Beschwerden als Information und – oftmals maßgebliche – Anregung für das behördliche Handeln. Bei gravierenden Fällen gehen die Behörden auch einzelnen Beschwerden nach, wobei dann die Unternehmen von den Behörden direkt kontaktiert werden und die Verbraucher nicht beteiligt werden.

In Schweden findet sich ferner die Besonderheit, dass das *Allmänna reklamationsnämnden* als behördlich organisierte Schlichtungsstelle für Verbraucher tätig wird. Nach Eingang einer schriftlichen Beschwerde eines Verbrauchers wegen einer Streitigkeit mit einem Unternehmer wird ein schiedsähnliches Verfahren initiiert. Dieser auf Streitbeilegung gerichtete Mechanismus ist für die Verbraucher kostenfrei und dauert ungefähr 6 Monate. In diesem Verfahren erfolgt keine eigenständige Beweisaufnahme, sondern die Entscheidung erfolgt auf der Grundlage der eingereichten Unterlagen. Bindend ist eine solche Entscheidung des *Allmänna reklamationsnämnden*, da nur eine Empfehlung ausgesprochen wird. Die erzielte Einigung ist nicht bindend und gegen sie steht keine Berufung offen; es steht den Parteien frei, die staatlichen Gerichte anzurufen. In der überwiegenden Anzahl von Fällen wird jedoch der Empfehlung des *Allmänna reklamationsnämnden* gefolgt (75%). Das mag auf Unternehmerseite auch daran liegen, dass bei Nichtbeachtung der Empfehlungen des National Boards for Consumer Disputes der Name des Unternehmen auf einer „schwarzen Liste“ in einem Verbrauchermagazin veröffentlicht wird.[73]

In ähnlicher Weise ist das französische CRLC eine Organisation zur Streitbeilegung, wobei die CRLC dezentralisiert organisiert sind. Zuständig ist das *département* in dem der Verbraucher seinen Wohnsitz hat. In einem solchen Verfahren versucht erst ein bestellter Berichterstatter eine Einigung zwischen den Parteien zu erreichen, schlägt die CRLC einen Vergleich vor. Falls ein solcher Vergleich fehlschlägt, informiert der CRLC den Verbraucher nicht nur über die Möglichkeit

[71] *Kirchberger/Storr,* Länderbericht Schweden, 4.a. cc).

[72] Eine Ausnahme bildet dabei im Einzelfall die KO in Schweden, siehe oben 4. a. dd.

[73] http://ec.europa.eu/consumers/empowerment/docs/SV_web_country_profile.pdf.

der Erhebung einer Klage, sondern gibt zudem zusätzliche hilfreiche Informationen für das gerichtliche Verfahren.[74]

c. Kollektive Durchsetzung von Verbraucherrechten

In Schweden und den USA können die Verbraucherbehörden zudem in Gerichtsverfahren für die Verbraucher beteiligt werden. In den USA können die Verbraucherbehörden oder Attorneys General auf Staatenebene Massenklagen anregen und dabei als Kläger auftreten. Auch die FTC kann für die Gesamtheit der Verbraucher Kompensationen einklagen. In Schweden ist neben der Funktion der Betreibung von Massenklagen auch die Prozessvertretung im Einzelfall durch den Verbraucherombudsmann möglich. In besonderen Fällen wird damit die Behörde auch in einem individuellen Fall für den Verbraucher aktiv.

d. Erlass von abstrakt-generellen Regelungen

In den untersuchten Rechtsordnungen spielen der Erlass von abstrakt-generellen Regelungen, also die administrative Normsetzung, für den Bereich des Datenschutzes und des Verbraucherschutzes eine wichtige Rolle. Die Wirkung dieser Regelungen – wie auch die Verfahren dieser Normsetzung – variieren dabei zwischen und innerhalb der einzelnen Rechtsordnungen. In den USA sind beispielweise neben der formellen Setzung von Regelungen auch die informelle Regelungssetzung bekannt, wobei jedoch nur die formelle Regelungssetzung vor den Gerichten als zu beachtende Normen Wirkung entfaltet. Die informellen Regelungen dienen den Unternehmen allein als nichtbindende Leitlinie, dessen Einhaltung vor den Gerichten nicht die Einhaltung der gesetzlichen Verpflichtung betrachtet werden muss.

In England gewinnt die Regelungssetzung gerade für den Bereich der Selbstverpflichtung besondere Bedeutung. Diese Selbstverpflichtungen werden von der Behörde mit den betreffenden Unternehmenssparten erarbeitet, wobei insbesondere öffentliche Konsultationen zur Gewinnung der Akzeptanz für die etablierten Regelungen dienen. In ähnlicher Weise ist die Erarbeitung solcher Regelungen in Frankreich relevant. In den USA sind die Beteiligungsrechte der Unternehmen als auch Verbraucher im formellen Regelungsverfahren vorgesehen. Die Wirkung der Regelungen kann für den Bereich der Selbstregulierung bedeuten, dass sich die Aufsichtsbehörde ein Stück aus der Aufsicht in dem jeweiligen Bereich zurückzieht. Andererseits kann die Regelungssetzung auch bedeuten, dass bislang gesetzlich nicht näher spezifizierte Regelungen getroffen werden, deren Einhaltung zugleich die Einhaltung der gesetzlichen Regelungen bedeutet. Ein Verstoß gegen die Regelungen hingegen stellt dann ebenfalls einen von der Behörde oder anderen Beteiligten – gegebenenfalls zu Geldbuße – zu ahnenden Verstoß da.

Für die USA findet sich zudem eine aus konkreten Maßnahmen zur Regelung des Einzelfalls hervorgehende Normbildung. Zumindest die Regelungen der FTC entfalten grundsätzlich auch Wirkungen für andere Marktteilnehmer und wirken also normsetzend. Erlässt die FTC eine Anordnung, die ein bestimmtes Verhalten als rechtswidrig anordnet und wird diese Anordnung veröffentlicht, so sind auch andere Unternehmen an diese Anordnung gebunden. Auf diese Weise wird es der FTC als Aufsichtsbehörde ermöglicht, ihre Ressourcen effektiv in einem einzigen Verfahren einzusetzen und den Markt als Ganzes zu beeinflussen, ohne langwierige formelle Regelungssetzungsprozesse durchzuführen. Im Ergebnis kann damit die Untersagung im Einzelfall die gleiche Wirkung wie behördliche Normen der FTC entfalten. Die mögliche Wirkung gegen alle

[74] http://ec.europa.eu/consumers/empowerment/docs/FR_web_country_profile.pdf

Marktteilnehmer führt jedoch zur Einbindung der betroffenen Unternehmen in das Verfahren gegen das betroffene Unternehmen. Sofern zwischen der Behörde und Unternehmen ein Vergleich erzielt wurde, hat dieser jedoch keine Wirkung für den gesamten Marktsektor. Ein vergleichbarer Mechanismus – Anordnung gegen Individuum mit direkter Wirkung für alle Marktbeteiligte – wurde für die anderen Rechtsordnungen nicht berichtet, ist aber auch in Europa nicht unbekannt.[75]

e. Informelle Verfahrensweisen

Neben der Herausgabe informeller Leitlinien und Stellungnahmen, sind in allen untersuchten Rechtsordnungen die betreffenden Aufsichtsbehörden auf eine informelle Klärung der jeweiligen Streitpunkte bedacht. In den untersuchten Rechtsordnungen versuchen die Verbraucherbehörden möglichst minimal in den Markt einzugreifen, was zum einen an einer großen Kooperationsbereitschaft der Unternehmen[76] als auch den Bestrebungen der Behörde, schnell und effektiv informelle Lösungen zu erzielen, zu liegen scheint. Behördliche Anordnungen werden daher nicht in jedem Fall als standardmäßiges Handlungsmittel favorisiert. In Schweden wird beispielweise erst nach einem Versuch der informellen Klärung der Streitpunkte ein offizielles Verfahren eingeleitet; zudem wird – auch nach Beschreitung des formellen Weges – stets versucht einen Vergleich zu erreichen.

f. Bußgelder und andere „Strafsummen“

Bußgelder werden von den Aufsichtsbehörden sowohl für den Verbraucherbereich als auch den Datenschutzbereich angewandt. Diese sind Beispielsweise bei Verstoß gegenbehördliche Regelungen, Gesetze oder Anordnungen im Einzelfall zu verhängen. In den USA zählt dabei bei länger andauernden Maßnahmen jeder einzelne Tag als separater Verstoß. Die Bußgeldsummen variieren, wobei in England das ICO die Obergrenze von 500,000 £ zuletzt fast ausgereizt hat.[77] In Frankreich hat die CNIL zudem die Möglichkeit, die verhängten Sanktionen zu veröffentlichen, Artikel 46 LILF.

In den untersuchten Rechtsordnungen haben die jeweiligen Behörden hingegen keine eigenen (kriminal-)strafrechtlichen Befugnisse. Sofern strafrechtliche Verfahren angestrebt werden, werden die Verfahren an die jeweiligen Strafverfolgungsbehörden abgegeben. Sofern in den USA auf Staatenebene die Attorneys General selbst (respective diesem zugeordnete Stellen) die relevanten Verbraucherschutzbehörden sind, finden sich beide Funktionen zumindest unter einem Dach vereint.

5. Einbindung in das Gerichtssystem

Die Einbindung der relevanten Behörden in das System der Zivilgerichte und ihrer Entscheidungen divergiert zwischen den untersuchten Rechtsordnungen erheblich. Für England ist zu beachten, dass die englischen Gerichte aufgrund des Common Law Systems maßgeblich eine Rechtssetzungsfunktion haben (auch wenn dies formal anders nämlich im Sinne eines besonderen Erkenntnisvorgangs beschrieben wird). Die Ausführungen des Court of Appeal in der Durant Entscheidung zum Anwendungsbereich des englischen Datenschutzgesetzes hat Auswirkungen

[75] Etwa bei der *erga omnes*-Wirkung bestimmter registrierter Verdikte gegen unfaire Vertragsklauseln nach polnischem Recht.

[76] So beispielsweise für die USA, Schweden und England berichtet.

[77] Siehe McNamee, Länderbericht England, 3. a. dd).

auch auf das ICO. Es ist nicht ersichtlich, dass das ICO eine eigenständige Rechtsauffassung aufweist, welche von der der englischen Gerichte abweicht.

In England und Frankreich ist nicht ersichtlich, dass die Verbraucherbehörden oder Datenschutzbehörde in irgendeiner Weise in zivilrechtliche Klagen von Verbraucher gegen Unternehmen involviert sind. Individuelle Streitigkeiten von Verbrauchern werden damit von den betreffenden Aufsichtsbehörden weder auf zivilrechtlichen noch auf verwaltungsgerichtlichem Weg behandelt. Die britischen Behörden können die Anordnungen gegen die Unternehmen zwar inzwischen teilweise ohne gerichtliche Hilfe aussprechen, in einigen Fällen aber müssen sie sich für deren Durchsetzung oder aber für Betretungsrechte an das Gericht wenden. Im Vergleich zu Deutschland mangelt an einer klaren konsistenten eigenständigen Befugnis zum Erlaß vollstreckbarer Titel und deren Vollstreckung für alle Maßnahmen und alle Behörden; auch hier ist die Emanzipation vom Privatrecht nicht abgechlossen.

In den USA kann die FTC als Bundesbehörde die Unternehmen zur Zahlung einer *civil penalty* vor Gericht verpflichten und diese gerichtlich einfordern. Darüber hinaus können sie vor Gericht – allerdings im Ermessen des Gerichts stehende – Schadensersatzsummen u.a. zur Kompensation der Einbußen bei den Verbrauchern beantragen. Auf der Staatenebene werden in den USA die Verbraucherschutzbehörden oder die Attorneys General als Kläger in *class action* Verfahren tätig, wobei dann die Schadenssummen an die Verbraucher ausgeschüttet werden, die sich als Geschädigte melden. Auch in Schweden unterstützt die KO Verbraucher mit *class actions* und kann geschädigten Verbrauchern durch Stellung eines Prozessvertreters helfen.

Welches Gericht für eine Klage zuständig ist, ist von Rechtsordnung und jeweiligen Situation abhängig. So differenziert man in Schweden beispielsweise nach der Unsicherheit der betreffenden Rechtslage. Nur wenn bislang ein Streitpunkt noch nicht von den Gerichten entschieden wurde, wird vom schwedischen Verbraucherombudsmann der Market Court direkt angerufen.

6. Einbindung der Stakeholder

Bei den normsetzenden Tätigkeiten der Behörden ist eine Einbindung durch Konsultation[78] oder Sicherstellung der formellen Einbindung[79] zu verzeichnen. In England werden beispielsweise Konsultationen zu den selbstregulatorischen Pflichten durchgeführt. In Schweden sind bei Vereinbarungen zu den Werbemaßnahmen und in Frankreich beispielsweise bei datenschutzrechtlichen Berufsregelungen die relevanten Stakeholder eingebunden. In den USA können die Unternehmen können in den relevanten Normsetzungsverfahren Stellungnahmen abgeben. Vor allem aber wird von den Behörden in großem Maße auf eine Information der betreffenden Unternehmen und Verbraucher gesetzt. Freiwillige Auditangebote und Gütesiegelverfahren zeugen von einer stärkeren präventiven Kooperationsbereitschaft der Behörden in England und Frankreich.[80]

---

[78] So für die Selbstregulierung für England berichtet, *McNamee,* Länderbericht England, 3. b. cc).

[79] *Herden,* Länderbericht USA, 3. a. ff).

[80] Generell zu der Frage eines „cooperative legalism" für den datenschutzrechtlichen Aufsichtsbereich in Europa aus amerikanischer Rechtsperspektive Francesca Bignami, „Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy †" 59 Am. J. Comp. L 411 (2011).

Die Einbindung von Verbraucherinteressenverbänden wurde von den meisten Länderberichterstattern nicht besonders hervorgehoben. In den USA werden die Verbraucherinteressen zumindest durch die formalen Rechte auf Beteiligung an den behördlichen Regelungen zur Spezifizierung der gesetzlichen Vorgaben berücksichtigt.

Bei behördlichen Handlungen im Einzelfall wird in den Länderberichten nur zu den USA von der Beteiligung auch Dritter berichtet, da das behördliche Einschreiten im Einzelfall eine normsetzende Funktion für alle Marktbeteiligte hat. Dementsprechend können bei Untersagungsverfügungen auch Dritte beteiligt werden. Durch die große Bereitschaft zur informellen Problemlösung und Abschluss von Vergleichen scheinen die teils schwerwiegenden Handlungsformen der Behörden abgeschwächt zu werden.

IV. Grenzüberschreitende Durchsetzung

Die grenzüberschreitende Durchsetzung im Bereich der Digitalen Welt scheint – anders als in Deutschland für das Datenschutzrecht[81] – bislang kaum eine eigenständige Rolle zu spielen. Generell beschränken sich die öffentlich-rechtlichen Befugnisse von Behörden grundsätzlich auf das jeweilige Hoheitsgebiet; hingegen entfalten Urteile aus zivilgerichtlichen Unterlassungsklagen von verbänden regelmäßig weitreichende grenzüberschreitende Wirkungen. Ähnliche Wirkungen dürften sich im europäischen Binnenmarkt – wenn nicht *de jure* so doch wenigstens *de facto* – aus den Regelungen zur Verwaltungszusammenarbeit und dem Herkunftslandsprinzip ergeben[82], welches für den administrativen Verbraucherschutz die Behörden des Herkunftslandes in die Pflicht nimmt; die Erfüllung dieser Pflicht läßt sich – nach den Regeln über die Verwaltungszusammenarbeit – auch durch die Behörden des Ziellandes beeinflussen. Für den Bereich der datenschutzrechtlichen Streitigkeiten ist jedoch ein grenzüberschreitender Bezug fast immer gegeben. In der Europäischen Union ist durch die Datenschutzrichtlinie sowie wohl zukünftig durch die Datenschutzgrundverordnung eine Regelung für grenzüberschreitende, behördliche Durchsetzung gegeben. Für den Bereich der verbraucherrechtlichen Durchsetzungen gilt die Datenschutzgrundverordnung.

V. Perspektiven und Gestaltungsmöglichkeiten für das deutsche Recht

Die rechtsvergleichenden Ergebnisse für Frankreich, Schweden, USA und England zeigen, dass bislang die Digitale Welt – hinsichtlich der Anforderungen und Gefahren für Verbraucher – weder als eigenständige Regelungsmaterie noch als Kompetenzfeld für eine eigenständige Behörde existiert. Die Positionen und Schutzbedürfnisse von Verbrauchern und von durch Datenverarbeitung Betroffenen werden – mit Ausnahme der USA, in der datenschutzrechtliche Regelungen als Mindestmaß und als Marktverhaltensregel vorhanden sind – immer noch weitgehend als zwei geschiedene Regelungsbereiche verstanden. Auch die Behördenstrukturen spiegeln diese Differenzierung wieder: Den verbraucherspezifischen Gefahren in der digitalen Welt wird in den untersuchten Rechtsordnungen durch fachspezifische oder sektorale Regelungen und Behördenstrukturen begegnet. Es werden die allgemeinen datenschutzrechtlichen und verbraucherspezifischen Behördenbefugnisse und -handlungsmittel, soweit sie den relevanten Bereich der digitalen Welt

[81] Siehe zuletzt OVG Schleswig NJW 2013, 1977 („Gegenüber Facebook können keine datenschutzrechtlichen Anordnungen auf der Grundlage deutschen materiellen Datenschutzrechts ergehen.“) sowie BeckRS 2013, 49918.

[82] Unionsrechtlich sind hier vor allem die e-commerce-Richtlinie 2000/31/EG, die Dienstleistungsrichtlinie 2006/123/EU und die – zur Novellierung anstehende – Rechtsdurchsetzungsverordnung 2006/2004 zu nennen.

erfassen, angewendet. In den USA wird der digitalen Welt als Schnittmenge verschiedener Regelungsbereiche durch die FTC noch am ehesten begegnet, obwohl dort sowohl keine strukturierten datenschutzrechtlichen oder verbraucherrechtlichen Regelungen im Allgemeinen bestehen. Im Ergebnis beschränkt sich die behördliche Aufsicht in den untersuchten Rechtsordnungen für den Bereich des Datenschutzes und des Verbraucherschutzes auf genuine aufsichtsrechtliche und informatorische Tätigkeiten zum Schutz der Verbraucher im Ganzen oder gestützt auf die datenschutzrechtlichen Aufsichtsbefugnisse. Eine beratende Tätigkeit oder Hilfe im Einzelfall, abgesehen von der Organisation von Schiedsverfahren oder Anregung von Sammelklagen, findet nicht statt.

Kaum administrative Kontrolle und Durchsetzung von Schutzstandards findet sich hingegen im Urheberrecht. Zwar werden die verschiedenen Instrumente der Bekämpfung von filesharing-Aktivitäten und ähnlichen Urheberrechtsverletzungen rechtsstaatlich organisiert administriert. Jedoch liegt der Schutz der privaten Rechtsverletzer in diesen Bereichen vor allem in dem eingeführten Verfahren und nicht in generellen Aktivitäten zur Aufspürung verbraucherschädlichen Verhaltes von Urheberrechtsinhabern. Da die Urheberrechtsinhaber zur Durchsetzung ihres Urheberrechts – von wenigen Ausnahmen, denen überwiegend Vollstreckungscharker oder eine dem Arrest vergelichbare Sicherungsfunktion zukommt – keines behördlichen Verfahren bedürfen, sind die Möglichkeiten zur Beteiligung von Behörden beschränkt. Eine Einbindung von möglichen Behörden für die digitale Welt wäre immerhin in das zivilrechtliche Verfahren zur Durchsetzung denkbar, beispielsweise zur Notifizierung bei Erlass einer Abmahnung oder der Möglichkeit zur Stellungnahme in einem Zivilprozess mit Verbraucherbeteiligung, eventuell auch erst aber einer gewissen Streitwert. Durch solche Maßnahmen wären die zuständigen Behörden zumindest über aktuelle Entwicklungen und das Ausmaß der Urheberrechtsdurchsetzungen mit Verbraucherbeteiligung informiert. Denkbar wäre auch eine behördliche Einstufung entsprechender Geschäftsmodelle als *unfair commercial practice*, was freilich wegen der verfassungsrechtlichen Rechtsschutzgarantie rechtsstaatlichen bedenken begegnen dürfte.

In Deutschland findet sich – abgesehen von den allgemeinen Ordnungs- und Sonderordnungsbehörden – nur eine sehr begrenzte behördliche Aufsichtsstruktur für die digitale Welt, wie beispielsweise in Ansätzen bei der Bundesnetzagentur für den Bereich der Telekommunikation sowie bei den Landesdatenschutzbehörden. Bei Überlegungen zur Etablierung ähnlicher Strukturen und Handlungsbefugnisse und -mittel wie in den untersuchten Rechtsordnungen, sind verschiedene Aspekte zu bedenken, die sich aus europarechtlichen und nationalen, verwaltungsrechtlichen Vorgaben oder aber aus rechtsvergleichender Perspektive ergeben.

Die Europäischen Rechtsakte des Verbraucherschutzes[83] – auch in der digitalen Weilt – sind in Deutschland fast ausschließlich zivilrechtlich umgesetzt, so daß die öffentlich-rechtliche Rechtsdurchsetzung noch in den Kinderschuhen steckt. Für die grenzüberschreitende behördliche Durchsetzung sind mit der Durchsetzungsverordnung 2006/2004 europäische Vorgaben vorhanden, denen innerstaatlich vor allem das BVL – unterstützt durch die Unterlassungsklagen des vzbv – Wirkung verleiht. Für den Bereich des Datenschutzes sind mit der Datenschutzrichtlinie neben subjektiven Rechten auch Vorgaben für eine Datenschutzaufsicht gegeben.

[83] So beispielweise nun mehrere Rechtsakte zusammenfassend die Richtlinie 2011/83/EU über die Rechte der Verbraucher, Abl. EU L 304/64 vom 22.11.2011.

Nationaler Spielraum auf Behördenebene zur Durchsetzung und Gewährleistung der europäischen Verbraucherrechte ist in diesem Grenzen in erheblichem Umfang vorhanden. Alleingänge für bestimmte behördliche Kompetenzen und Handlungsmittel im Bereich der digitalen Welt bedürfen jedoch vorsichtiger Prüfung. So sind mit dem Entwurf für die Datenschutzgrundverordnung hinsichtlich des Datenschutzrechts Monopolisierungen der datenschutzrechtlichen Aufsicht angedacht. Eine zweite aufsichtsrechtliche Struktur daneben, welche ebenfalls der Durchsetzung des Datenschutzrechts diente, würde dann den Bestimmungen einer solchen Datenschutzgrundverordnung zuwiderlaufen.

Eine marktbezogene Aufsicht, abseits der nur in Ansätzen so angelegten Aufsicht für Datenverarbeitungsprozesse, für das Verhalten am Markt oder deren Zugang bedürfte ebenfalls des Einklangs mit den europäischen Vorgaben. Eine entsprechende behördliche Aufsichtsstruktur für unlautere Geschäftspraktiken ist in der Lauterkeitsrichtlinie als eine Option vorgesehen und bislang für Deutschland nicht umgesetzt. Eine marktbereinigende Funktion im Sinne des Ausschlusses von Marktteilnehmern durch die öffentliche Verwaltung ist den untersuchten Rechtsordnungen in den Spezialbereichen Datenschutz und Urheberrecht nicht zu entnehmen, so dass dort ebenfalls nur verhaltensbezogene Anordnungen getroffen werden. Für Deutschland müßten entsprechende Behröden aus kompetenzrechtlichen Gründen wohl auf Landesebene errichtet werden.[84] Auch die Durchsetzung von Marktzugangsbeschränkungen ist in Deutschland wohl nur ausnahmsweise durch eine Bundesbehörde möglich.

Die Rechtsdurchsetzung von zivilrechtlichen Ansprüchen von Verbrauchern durch eine Behörde oder Hilfestellungen bei einer solchen Rechtsdurchsetzung, in der Form wie es der schwedische Ombudsmann vornimmt, dürfte in Deutschland im Regelfall die Subsidiarität des Verwaltungshandelns entgegenstehen. Die Organisation von behördlich mitgetragenen Beratungsstellen hingegen ist denkbar. Die Durchsetzung von individuellen Ansprüchen und Beratung im Einzelfall müsste jedoch durch eine entsprechende personelle und sachliche Ausstattung abgedeckt sein.

Die direkte Übertragung der Instrumente und behördlichen Strukturen ins deutsche Recht ohne Betrachtung der jeweiligen nationalen Settings sollte vermieden werden, da die jeweiligen nationalen behördlichen Strukturen, Selbstverständnisse, Akzeptanz in den Rechtsordnungen und die Gesamtheit der behördlichen Handlungsmittel und Befugnisse maßgeblich für den Erfolg und die Effektivität der behördlichen Aufsicht beitragen. Dementsprechend sollte die Implementierung neuer behördlicher Strukturen als *Transplants* aus den fremden Rechtsordnungen in die deutsche Rechtsordnung nur unter sorgfältiger Betrachtung der vorhandenen behördlichen Strukturen und Regelungsmöglichkeiten erfolgen.

Neue Perspektiven, welche in den untersuchten Rechtsordnungen bereits ansatzweise angelegt sind, könnten sich insbesondere aus den Aktivitäten in den bereichen ADR und *collective redress* ergeben. Der europäische Gesetzgeber hat mit der ADR-Richtlinie[85] und der Empfehlung zum

[84] Ob die Bundesländer dazu auch ohne den Bund befugt wären, harrt noch der Klärung.

[85] Richtlinie 2013/11/EU über die alternative Streitbeilegung verbraucherrechtlicher Streitigkeiten, Abl. EU L 165/63 vom 18.06.2013 (ADR-Richtlinie).

collective redress[86] neue Impulse für das Verbraucherrecht gegeben, welche auch für eine verbraucherspezifische, für die digitale Welt spezifizierte behördliche Strukturen brauchbar gemacht werden könnten. Die Empfehlung zum *colletive redress* sieht ausdrücklich behördliche Möglichkeiten zur Koordinierung von Verbraucherklagen unter Einbezug datenschutzrechtliche Ansprüche vor. Schiedsstellen, wie sie die ADR-Richtlinie fordert, sollen auch durch Behörden geführt werden können.[87] Zwar werden datenschutzrechtliche Sachverhalte durch die ADR-Richtlinie nicht zwingend erfasst, doch mangels schiedsrechtlicher Regelungen in den datenschutzrechtlichen Rechtsakten der EU und dem Mindestharmonisierungsansatz der ADR-Richtlinie, könnten die Mitgliedsstaaten eine solche Erweiterung auf datenschutzrechtliche Verbraucherschutzstreitigkeiten vornehmen. Die behördliche Anbindung von *collective redress* oder behördlichen Stellen der Alternativen Streitschlichtung bieten, ebenso wie behördliche Beschwerdestellen, die Möglichkeit der Informationsbündelung. Informationen über Probleme von Verbrauchern mit Unternehmern und Datenverarbeitern könnten die relevanten Aufsichtsbehörden direkt erreichen, auch ohne eine Pflicht zur Rechtsdurchsetzung im Einzelfall zu begründen. In den untersuchten Rechtsordnungen scheinen gerade die behördlichen Beschwerdestellen den Aufsichtsbehörden als unersetzliche Informationsquelle über Missstände zu dienen. Die Bundesnetzagentur verfügt bereits eine solche Möglichkeit zur Entgegennahme von Beschwerden, ohne dabei in jedem Einzelfall aktiv zu werden.[88]

Den untersuchten Rechtsordnungen ist ebenfalls zu entnehmen, dass die Einbindung der relevanten Stakeholdern (Unternehmen und Verbrauchergruppen) für die individuelle Beratung der Verbraucher aber auch für den Erlass von allgemein verpflichtenden Regelungen sowie Regelungen für die Selbstverpflichtungen zu berücksichtigen sind. Diese können zudem zur Entlastung behördlicher Strukturen für die Beratung von Verbrauchern als auch Akzeptanz der aufsichtsrechtlichen Strukturen beitragen.

[86] Siehe oben Fußnote 3.

[87] Artikel 4 (2) ADR-Richtlinie.

[88] Jahresbericht 2012 der Bundesnetzagentur, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2013/Jahresbericht2012.pdf?__blob=publicationFile&v=4 (zuletzt abgerufen a, 2.11.2013).

D. Länderberichte

I. Länderbericht zur „Übersicht über die Regulierung des Datenschutzes und des Urheberrechts in der digitalen Welt in Frankreich“

1. Regelungsstruktur der materiellen Standards im Datenschutz- und Urheberrecht

a. Struktur des materiellen Datenschutzrecht in Frankreich

aa) Verfassungs- und grundrechtliche Verankerung des Datenschutzrechts und Gesetzgebungsentwicklung

Der Datenschutz hat zwar in der französischen Verfassung selbst keine spezielle Verankerung erfahren, jedoch wird dem Recht auf Privatleben durch eine Entscheidung des *Conseil constitutionnel* aus dem Jahr 1995 gleichwohl Verfassungsrang eingeräumt.[1] Der *Conseil constitutionnel* hat des Weiteren in einem obiter dictum aus dem Jahr 1999 das Recht auf Achtung des Privatlebens als in Art. 2 der Erklärung der Menschenrechte von 1798 enthalten erachtet.[2]

Das Recht auf Achtung des Privatlebens ist Ausdruck des Persönlichkeitsrechtsschutzes. Im Unterschied zum deutschen Recht existiert im französischen Recht allerdings kein allgemeines Persönlichkeitsrecht, stattdessen wurden eine Reihe einzelner Verfahren einzelne Persönlichkeitsschutzrechte herausgebildet.[3] Beispielsweise zählen hierzu das Recht am eigenen Bild, die Achtung der strafrechtlichen Unschuldsvermutung und das Urheberrecht.[4] Dabei stützte sich die Rechtsprechung für deren Entwicklung und privatrechtliche Absicherung zunächst nicht auf die Menschenrechtserklärung, sondern auf die deliktische Generalklausel des Art. 1382 f. Code civil.[5] Seit dem Jahr 1970 findet sich in Art. 9 Code civil das Postulat des Rechts auf Achtung des Privatlebens („*Chacun a droit au respect de sa vie privée*“) und damit eine ausdrückliche gesetzliche Grundlage für den Persönlichkeitsschutz.[6] Vergegenwärtigt man sich die große symbolische und politische Bedeutung des Code civil, wird der besondere Stellenwert einer Verankerung des Persönlichkeitsschutzes in Art. 9 deutlich.

Die Fortentwicklung des Persönlichkeitsschutz hat letztlich auch die Schaffung datenschutzrechtlicher Regelungen gefördert. Grundlegend für das französische Datenschutzrecht ist das *loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*[7] (LIFL). Die Bedeutung

---

1 *Barton/Weißnicht*, Online-Überwachung im Unternehmen – Ein Überblick über die Rechtslage in Frankreich, MMR 2008, 149 mit Hinweis auf Conseil Constitutionnel, Décision n° 94-352 DC du 18 janvier 1995. Abrufbar unter www.conseil-constitutionnel.fr/decision/1995/94352dc.htm.

2 *Trebes*, GRUR Int 2006, 91 mit Hinweis auf Conseil Constitutionnel, Décision n° 99-416 DC du 23 juillet 1999. Abrufbar unter www.conseil-constitutionnel.fr/decision/1999/99416dc.htm.

3 *Kannowski* in Staudinger, BGB Vor § 1, Rn. 31.

4 Zu den Persönlichkeitsschutzrechten im Einzelnen näher *Trebes*, GRUR Int 2006, 91 (92 f.).

5 *Trebes*, GRUR Int 2006, 91.

6 *Kannowski* in Staudinger, BGB Vor § 1, Rn. 31.

7 J.O. 1978, S. 227 ff. Zu Entstehungsgeschichte und –bedingungen *Desgens-Pasanau*, La protection des donnés à caractère personnel, 2012, S. 3 f.; *Grewe*, Transparenz, Informationszugang und Datenschutz in Frankreich, DÖV 2002, 1022 (1023 f.)

des Persönlichkeitsschutzes kommt bereits in Art. 1 dieses Gesetzes zum Ausdruck: „Die Informatik (...) soll im Dienste jedes Bürgers stehen. Sie darf weder die menschliche Identität noch die Menschenrechte, weder das Privatleben noch die öffentlichen oder privaten Freiheiten beeinträchtigen.“[8] Das LIFL aus dem Jahr 1978 ist auf den Schutz des Privatlebens des Einzelnen vor den Gefahren und Nachteilen insbesondere der automatisierten Erfassung, Speicherung und Aufbereitung personenbezogener Daten gerichtet.[9] Es war mithin wie das BDSG auf den Schutz der Daten natürlicher Personen beschränkt und sowohl bei Verarbeitung personenbezogener Daten durch öffentliche wie auch private Datenverarbeiter anwendbar.[10] Neben materiellrechtlichen Vorgaben für die automatische und manuelle Datenverarbeitung wird durch das das loi no. 78-17 für die automatische Datenverarbeitung zusätzlich eine Registrierungspflicht implementiert.[11]
Die spätere europäische Datenschutzrichtlinie wurde in Frankreich nur mit deutlicher Verzögerung und nach Einleitung verschiedener Vertragsverletzungsverfahren erst im Jahr 2004 umgesetzt – letztlich durch entsprechende Modifizierung des ursprünglichen Gesetzes von 1978.[12] Dies geschah durch das loi n° 2004-801[13] und hatte einige grundlegende Änderungen zur Folge. Besonders hervorzuheben ist die mit dieser Gesetzesnovellierung einhergehende Vereinfachung der Formalitäten zur verpflichtenden Registrierung bei der automatischen Datenverarbeitung.[14] Zugleich wurden aber auch die die Rechte der Betroffenen gestärkt.[15]
Vergleichsweise geringe Bedeutung kommt der Vielzahl kleiner Gesetzesänderungen zu. Aktuell liegt das französische Datenschutzgesetz in *der version consolidée au 13 octobre 2013* vor.

bb) Bestand und Grundstruktur der Regelungen zum Datenschutzrecht

(1) Anwendungsbereich des LIFL

Das LIFL ist anwendbar auf die Verarbeitung (*traitement*) personenbezogener Daten (*données à caractère personnel*) durch eine verantwortliche datenverarbeitende Stelle (*responsable de traitement*) sofern die Verarbeitung dem französischen Recht unterfällt.[16]

---

8 Übersetzung *Le Friant*, Der Schutz personenbezogener Daten für Arbeitnehmer in Frankreich, RdA 2003, 33 (34). Im Original: „*L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aufx libertés individuelles ou publiques.“*

9 Vgl. *Barton/Weißnicht*, MMR 2008, 149 (152).

10 *Bodenschatz,* Der europäische Datenschutzstandard, 2010, S. 71; *Ellge*r, Der Datenschutz im grenzüberschreitenden Datenverkehr, 1. Aufl. 1990, S. 363.

11 *Bodenschatz*, S. 71; Grewe, DÖV 2002, 1022 (1024).

12 *Féral-Schuhl*, Cyberdroit, 2008, Rn. 11.12.

13 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.

14 *Barton/Weißnicht*, MMR 2008, 149 (152); Grewe, DÖV 2002, 1022 (1027).

15 *Aye*, Verbraucherschutz im Internet nach französischem und deutschem Recht, 2005, S. 112; *Vulliet-Tavernier*, Après la loi du 6 août 2004 : nouvelle loi « informatique et libertés », nouvelle CNIL ?, Droit social 2004, 1055.

16 *Desgens-Pasanau*, S. 7.

(a) Personenbezogene Daten

Eine Legaldefinition der „personenbezogenen Daten“ ist in Art. 2 Abs. 2 LIFL enthalten. Sie ist an die Definition der Datenschutzrichtlinie angelehnt, entspricht dieser jedoch nicht gänzlich.[17] Um personenbezogene Daten handelt es sich demnach bei allen Informationen, „die sich auf eine natürliche Person beziehen, die unter Bezug auf eine Identifikationsnummer oder auf einen oder mehrere spezifische Faktoren ihrerseits identifiziert wird oder identifiziert werden kann“.[18] Der Begriff „personenbezogene Daten“ ist, wie die Definition zeigt, weit zu verstehen.[19] Name, Identifikationsnummern, Telefonnummer, Stimme, Bilder, genetische Fingerabdrücke oder IP-Adresse sind typische Beispiele für personenbezogene Daten i.S.d. Art. 2 Abs. 2 LIFL.[20]

Es macht zudem keinen Unterschied, ob die Identifizierung mittelbar oder unmittelbar erfolgen kann.[21] Deshalb kommt es nicht allein auf die Verknüpfung der Daten mit einem Namen als Identifikationsmerkmal an, denn eine mittelbare Identifizierung ist u.a. auch anhand der Sozialversicherungsnummer, eines Lichtbilds oder schon wieder durch das Herstellen einer Beziehung oder eines Zusammenhangs, beispielsweise bei Geburtsdatum und -ort, Wohnort, etc., möglich.[22]

Ausgenommen vom Anwendungsbereich des LIFL sind allerdings die Daten juristischer Personen. Das Datenschutzgesetz findet folglich grundsätzlich keine Anwendung. Ein wichtiger Sonderfall liegt aber bei sogenannten gemischten Datensätzen (*fichiers mixtes*) vor: wenn hierin auch personenbezogene Daten wie der Name der Geschäftsführung oder professionelle Kontakte enthalten sind, ist der Anwendungsbereich des LIFL wiederum eröffnet.[23]

(b) Datenverarbeitung

Nach dem französischen Datenschutzgesetz stellt jeglicher Umgang mit den personenbezogenen Daten unabhängig vom konkret eingesetzten Verfahren eine Verarbeitung personenbezogener Daten dar (vgl. Art. 2 Abs. 3 LIFL). Das gilt insbesondere für deren „(...) Erlangung, Aufzeichnung, Organisation, Speicherung [...] Blockierung, Löschung oder Zerstörung“.[24] Unerheblich ist für die Anwendbarkeit des LIFL auch, ob die Datenverarbeitung automatisch oder manuell vollzogen

---

17 *Vulliet-Tavernier*, Droit social 2004, 1055 (1056).

18 Übersetzung *Barton/Weißnicht*, MMR 2008, 149 (152). Im Original: „*Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.*“

19 *Desgens-Pasanau*, S. 8.

20 *Féral-Schuhl*, Rn. 11.22.

21 Vgl. *Ellger*, S. 363.

22 *Vulliet-Tavernier*, Droit social 2004, 1055 (1056).

23 *Desgens-Pasanau*, S. 8.

24 Übersetzung *Barton/Weißnicht*, MMR 2008, 149 (152). Im Original: „*Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction*.“

wird.[25] Der Begriff der Datenverarbeitung darf also ebenfalls weit verstanden werden.[26] Auch werden an die Ausgestaltung der Datenverarbeitung keine besonderen (technischen) Anforderungen gestellt, so dass beispielsweise eine einfache Exeldatei ausreichen kann.[27]

(c) Verantwortliche datenverarbeitende Stelle

Als verantwortliche Stelle definiert wird unter Vorbehalt ausdrücklich anders lautender Regelungen in Art. 3 Abs. 1 LIFL „... eine Person, eine öffentliche Behörde, ein Institut oder jegliche andere Organisation, die die Zwecke und Mittel der Datenverarbeitung festlegt."[28] Die Definition der verantwortlichen datenverarbeitenden Stelle ist insbesondere für die Bestimmung des durch die die Datenverarbeitung betreffenden Regelungen Verpflichteten maßgeblich.[29] Im Umkehrschluss zu Art. 3 Abs. 1 LIFL ergibt sich, dass ein externer Dienstleister (Subunternehmer), der auf Rechnung der für die Verarbeitung verantwortlichen Stelle tätig wird, nicht als direkt verantwortlich betrachtet wird und ihn vor allem keine Registrierungs- bzw. Anzeigepflichten treffen, auch wenn er die Pflicht zur Sicherstellung der Sicherheit und Vertraulichkeit der ihm durch seinen Auftraggeber anvertrauten Daten hat.[30]

(d) Anwendbarkeit des französischen Rechts

Das anwendbare nationale Recht bestimmt sich nach dem Sitz der verantwortlichen datenverarbeitenden Stelle.[31] Maßgeblich für die Anwendbarkeit französischen Rechts und damit des LIFL ist nach Art. 5 LIFL, ob die verantwortliche Stelle auf dem französischen Staatsgebiet niedergelassen ist (*le responsable est établi sur le territoire français*). Abzustellen ist nur auf das Ausüben der Tätigkeit im Rahmen der Niederlassung auf dem französischen Staatsgebiet, auf die Rechtsform der Niederlassung kommt es nicht an. Das LIFL ist nach Art. 5 auch auf diejenigen Stellen anwendbar, die zwar nicht auf dem französischen Staatsgebiet oder innerhalb der Europäischen Union niedergelassen sind, jedoch zur Datenverarbeitung auf Mittel zurückgreifen, die auf dem französischen Staatsgebiet belegen sind und nicht nur die bloße Durchleitung der Daten betreffen. Was genau unter den Mitteln der Datenverarbeitung (*moyens de traitement*) zu verstehen ist, gilt auch in Frankreich als umstritten: Im Zusammenhang mit der Sammlung von Daten wird beispielsweise auf eine tendenziell weite Begriffsauslegung verwiesen, so dass auch die Verwendung von Cookies auf den Rechnern der Internetnutzer als *moyen de traitement* angesehen werden dürfte.[32]

---

25 *Féral-Schuhl*, Rn. 11.22.

26 *Desgens-Pasanau*, S. 8 f.

27 *Desgens-Pasanau*, S. 9.

28 Übersetzung *Barton/Weißnicht*, MMR 2008, 149 (152). Im Original: „*Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.*"

29 *Vulliet-Tavernier*, Droit social 2004, 1055 (1056).

30 *Desgens-Pasanau*, S. 9.

31 *Vulliet-Tavernier*, Droit social 2004, 1055 (1056).

32 *Desgens,Pasanau*, S. 10.

(2) Vorgaben für die Datenverarbeitung[33]

(a) Zulässigkeitsvoraussetzungen

Fragen der Zulässigkeit der Datenverarbeitung sind zusammen im LIFL in Kapitel II geregelt. Teilweise ist die Verarbeitung von Daten auch gänzlich verboten, teilweise nur bestimmten Stellen erlaubt.

Art. 6 LIFL stellt zunächst Bedingungen an die zu verarbeitenden Daten selbst, welche sich aus Art. 6 der Datenschutzrichtlinie herleiten[34] und als „Datenschutzgrundsätze" bezeichnet werden können.[35] Die Daten müssen auf redliche und rechtmäßige Weise (*de manière loyale et licite*) erhoben und verarbeitet werden (Art. 6 Nr. 1). Die Zwecke der Datenerhebung müssen bestimmt, eindeutig und rechtmäßig (*finalités déterminées, explicites et légitimes*) sein und diese Zwecke müssen auch im Nachhinein bei der Datenverarbeitung weiterhin Beachtung finden (Art. 6 Nr. 2). Wie sich beispielsweise gegenüber Banken und Kreditinstituten zeigt, werden hier verhältnismäßig strenge Maßstäbe angelegt.[36] In Hinblick auf die Zielsetzung ihrer Erhebung und vorherigen Verarbeitung müssen die Daten zweckmäßig, stichhaltig und maßvoll (*adéquates, pertinentes et non excessives*) sein (Art. 6 Nr. 3). Darüber hinaus müssen die Daten genau, vollständig und – sofern notwendig – aktuell (*exactes, complètes et, si nécessaire, mises à jour*) sein (Art. 6 Nr. 4). Zudem müssen Maßnahmen ergriffen werden um sichzustellen, dass in Hinblick auf die Zwecke ihrer Erhebung und Verarbeitung ungenaue oder unvollständige Daten gelöscht oder berichtigt werden. Schließlich dürfen die Daten nur so vorgehalten werden, dass eine persönliche Identifizierung der Betroffenen nur während eines Zeitraums möglich ist, der den für die Zwecke der Erhebung und Verarbeitung notwendigen Zeitraum nicht überschreitet (Art. 6 Nr. 5).

Art. 7 LIFL schreibt sodann die Zustimmung (*consentement*) des Betroffenen als grundsätzlich notwendige Voraussetzung für die Zulässigkeit der Datenverarbeitung vor. Daneben enthält Art. 7 eine abschließende Aufzählung andernfalls (also ohne Zustimmung) zu erfüllender Bedingungen. Dazu gehören das Bestehen einer gesetzlichen Pflicht der datenverantwortlichen Stelle, die Lebensrettung des Betroffenen, die Ausübung einer behördlichen bzw. öffentlichen Aufgabe, mit der die verantwortliche Stelle oder der Auftraggeber betraut ist, Ausführungen im Rahmen eines (vor-)vertraglichen Rechtsverhältnis mit dem Betroffenen oder das Bestehen eines legitimen Interesses der verantwortlichen Stelle oder des Auftraggebers unter dem Vorbehalt, dass weder Interessen noch Rechte oder Grundrechte des Betroffenen verkannt werden. Abgesehen von dieser letzten Bedingung orientiert sich Art. 7 LIFL eng an Art. 7 der Datenschutzrichtlinie.[37] Gerade diese letzte Bedingung birgt allerdings eine erhebliche Gefahr der Aushebelung des Zustimmungserfordernisses. Die Handhabung der verantwortlichen Stellen und auch der französischen Datenschutzbehörde, der *Commission nationale de l'informatique et des libertés* (CNIL), weisen in diese Richtung und führen dazu, dass in der Praxis die Einholung der Zustimmung des Betroffenen auf die gesetzlich speziell vorgesehenen Fälle (z.B. Art. 8, Art. 56 oder Art. 32 Abs. 2 LIFL) beschränkt wird.[38]

---

[33] Sondervorschriften enthält das LIFL für die Datenverarbeitung zur Forschung im Gesundheitsbereich, bei Behandlung oder Prävention und zu journalistischen sowie künstlerischen oder literarischen Zwecken.

[34] *Vulliet-Tavernier*, Droit social 2004, 1055 (1056).

[35] *Barton/Weißnicht*, MMR 2008, 149 (153).

[36] *Féral-Schuhl*, Rn. 12.11.

[37] *Vulliet-Tavernier*, Droit social 2004, 1055 (1056).

[38] *Desgens,Pasanau*, S. 55.

Wie bereits angedeutet, finden sich daneben für bestimmte Arten von Daten Spezialvorgaben. Grundsätzlich verboten sind nach Art. 8 Abs. 1 LIFL die Erhebung und Verarbeitung personenbezogener Daten, die direkt oder indirekt Aufschluss geben über Rassenzugehörigkeit, ethnische Abstammung, politische, weltanschauliche oder religiöse Meinungen, die Gewerkschaftszugehörigkeit der betroffenen Personen oder deren Gesundheit oder Sexualleben betreffen. Hierbei handelt es sich nämlich um sog. sensible Daten („données dites sensibles“).[39] Insoweit der Zweck der Verarbeitung es für bestimmte Kategorien von Daten erfordert, können gem. Art. 8 Abs. 2 LIFL Ausnahmen vom grundsätzlichen Verbot des Art. 8 Abs. 1 LIFL bestehen. Dazu zählen unter anderem das ausdrückliche Einverständnis des Betroffenen, dessen eigenes Öffentlichmachen der jeweiligen Daten und die gerichtliche Rechtsdurchsetzung.[40]

(b) Anzeige- bzw. Genehmigungspflicht

Neben den allgemeinen Zulässigkeitsvoraussetzungen kennt das französische Datenschutzrecht mit der Anzeige- bzw. Genehmigungspflicht[41] eine zusätzliche vorab zu erfüllende Formalität: Im Falle der automatisierten Datenverarbeitung (vgl. Art. 22 Abs. 1 LIFL) muss grundsätzlich eine Anzeige gegenüber der CNIL erfolgen. Sofern die Datenverarbeitung aber einer Genehmigung nach Art. 25-27 LIFL bedarf, eine bloße Archivierung erfolgt oder ein Datenschutzbeauftragter bestellt wurde, entfällt die Anzeigepflicht. Eine weitere Ausnahme liegt vor, wenn die Datenverarbeitung nur zu persönlichen Zwecken vorgenommen wird.

(c) Weitere Anforderungen

Weitere Pflichten der für die Datenverarbeitung verantwortlichen Stelle ergeben sich aus Art. 32-37 LIFL. Darunter fallen die Pflicht zur Information des Betroffenen nach Art. 32 LIFL, die Pflicht zur Datensicherheit nach Art. 34 LIFL, die Pflicht zur Information der CNIL bei Sicherheitsgefährdungen nach Art. 34 bis LIFL und schließlich die Pflicht zur Beendigung der Datenvorhaltung sowie zur Löschung nach Art. 36 LIFL. Daneben regelt Art. 35 LIFL besondere Pflichten beim Einsatz von Subunternehmern/-verarbeitern der verantwortlichen Stelle.

Sofern nicht bereits im Vorfeld durch die verantwortliche Stelle oder ihren Vertreter über diese Punkte informiert wurde, umfasst die Pflicht zur Information des Betroffenen nach Art. 32 LIFL die Information über die Identität der verantwortlichen Stelle und ggf. die ihres Vertreters (Nr. 1), den mit der Datenverarbeitung verfolgten Zweck (Nr. 2), den verpflichtenden oder freiwilligen Charakter der Antworten (Nr. 3), diesbezügliche eventuelle Konsequenzen einer fehlenden oder fehlerhaften Antwort (Nr. 4), Empfängern oder Empfängerkategorien (Nr. 5), die nach der Sektion 2 des Kapitels V LIFL bestehenden Rechte der Betroffenen[42] (Nr. 6) und geplante Datenübertragungen in Staaten außerhalb der Europäischen Union (Nr. 7). Zusätzliche Informationspflichten bestehen bei elektronischen Kommunikationsdiensten. Diese betreffen beispielsweise die Erfassung der Verbindungsdaten, insbesondere durch Verwendung von Cookies.[43] Unbeachtlich sind die Informationspflichten des Art. 32 LIFL u.a. aber, wenn ursprünglich zu einem anderen Zweck erhobene Daten lediglich zu historischen, statistischen oder wissenschaftlichen Zwecken beibehalten werden. Art. 32 Abs. 6 LIFL enthält zudem den Hinweis, dass die Vorschriften des Art. 32 LIFL auf Datenverarbeitungen, welche die Prävention, die Aufklärung, die Feststellung oder die Verfolgung

---

39 *Vulliet-Tavernier*, Droit social 2004, 1055 (1057).

40 Ausführlicher zu den insgesamt zehn Ausnahmemöglichkeiten *Vulliet-Tavernier*, Droit social 2004, 1055 (1057).

41 Dazu näher unten.

42 Dazu näher unten.

43 *Féral-Schuhl*, Rn. 12.30.

von Straftaten (*la prévention, la recherche, la constatation ou la poursuite d'infractions pénales*) zum Ziel haben, keine Anwendung finden.
Die sich aus Art. 34 LIFL ergebende Pflicht zur Datensicherheit erstreckt sich nicht nur auf das Treffen aller dienlichen Vorsichtsmaßnahmen zur Gewährleistung der Sicherheit der Daten, sondern insbesondere auch auf die Verhinderung ihrer Verzerrung, ihrer Beschädigung oder eines unberechtigten Zugangs Dritter (*empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès*).[44]
Anbieter elektronischer Kommunikationsdienste müssen außerdem gem. Art. 34 bis LIFL im Falle einer Verletzung personenbezogener Daten unverzüglich die CNIL benachrichtigen. Bei drohender Gefährdung oder Beeinträchtigung personenbezogener Daten oder des Privatlebens des Nutzers oder einer anderen natürlichen Person ist auch der Betroffene unverzüglich zu benachrichtigen. Die Notwendigkeit der Benachrichtigung des Betroffenen entfällt jedoch, wenn die CNIL gerade für die im konkreten Fall verletzten personenbezogenen Daten eine sich aufgrund der durch den Anbieter angewandten Sicherungsmaßnahmen ergebende Unverständlichkeit der Daten für unberechtigte Dritte festgestellt hat.
Die Verarbeitung personenbezogener Daten durch einen Subunternehmer bzw. –verarbeiter darf nach Art. 35 LIFL zudem nur auf Weisung der verantwortlichen Stelle vorgenommen werden. Hierbei muss vor allem sichergestellt sein, dass der Subverarbeiter die in Art. 34 LIFL erwähnten Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit (*mesures de sécurité et de confidentialité*) der Daten ergreift. Die Einschaltung eines Subverarbeiters führt aber nicht zur Befreiung der verantwortlichen Stelle von der Verantwortlichkeit für die Einhaltung der Vorgaben des LIFL.

(3) Rechte der Betroffenen

Dem von der Datenverarbeitung Betroffenen gewährt das LIFL verschiedene Rechte.
An erster Stelle steht das Recht, sich der Datenverarbeitung zu widersetzen bzw. ihr zu widersprechen (*droit de s'opposer*) (Art. 38 LIFL). Ein solches Recht haben allerdings nur natürliche Personen in Hinblick auf die Verarbeitung ihrer eigenen personenbezogenen Daten. Insbesondere sollen sie ohne Entstehung von Kosten dem Einsatz ihrer personenbezogenen Daten zu Werbezwecken widersprechen können. Ausnahmen sind vorgesehen bei Bestehen einer gesetzlichen Pflicht zur Datenverarbeitung und bei ausdrücklichem Ausschluss dieses Rechts in der Genehmigung der Datenverarbeitung durch die CNIL.
Des Weiteren haben die Betroffenen gem. Art. 39 Abs. 1 LIFL unter der Voraussetzung des Nachweises ihrer Identität ein Abfragerecht (*droit d'interroger*) gegenüber der verantwortlichen Stelle. Abgefragt werden kann ob (*confirmation*) personenbezogene Daten Gegenstand einer Verarbeitung sind (Nr. 1), Informationen bzgl. Verarbeitungszwecken, bzgl. Kategorien der verarbeiteten personenbezogenen Daten, bzgl. Empfängern oder Empfängerkategorien (Nr. 2), ggf. Informationen im Hinblick auf die Datenübertragung in Staaten außerhalb der Europäischen Union (Nr. 3), in zugänglicher Form die Übermittlung aller über den Betroffenen vorgehaltenen personenbezogenen Daten nebst jeglicher verfügbaren Information (*toute information disponible*) über ihre Herkunft (Nr. 4) und Informationen, die es ermöglichen die Logik der automatischen Verarbeitung zu erkennen und ihr zu widersprechen (*de connaître et de contester*), falls auf deren Grundlage Entscheidungen mit rechtlichen Wirkungen für den Betroffenen getroffen werden (Nr. 5). Vom Betroffenen dürfen hierfür maximal die Reproduktionskosten verlangt werden. Zudem muss dem

[44] Ausführlicher zur Pflicht zur Datensicherheit *Féral-Schuhl*, Rn. 12.21 ff.

Informationsgesuch innerhalb einer Frist von zwei Monaten nachgekommen werden.[45] Die Informationsrechte der Betroffenen gem. Art. 39 LIFL unterscheiden sich von den Informationspflichten der verantwortlichen Stelle gem. Art. 32 LIFL dahingehend, dass die Informationen des Art. 32 LIFL verpflichtend erteilt werden müssen, die des Art. 39 LIFL nur auf Nachfrage (*à la demande*). Außerdem können sich Abweichungen in Hinblick auf den Zeitpunkt der Informationserteilung ergeben. Die verantwortliche Stelle kann sich nur nachweislich missbräuchlichen Anfragen widersetzen; hierfür obliegt ihr allerdings die Beweislast.
Art. 40 LIFL räumt dem Betroffenen zudem einen Anspruch auf Berichtigung, Vervollständigung, Aktualisierung, Sperrung oder Löschung (*rectifiées, complétées, mises à jour, verrouillées ou effacées*) ein, soweit seine personenbezogenen Daten nicht stimmen bzw. unvollständig, missverständlich oder veraltert (*inexactes, incomplètes, équivoques, périmées*) sind oder soweit ihre Erhebung, ihr Gebrauch, ihre Übermittlung an Dritte oder ihre Beibehaltung (*la collecte, l'utilisation, la communication ou la conservation*) untersagt sind. Wurden Daten an Dritte übermittelt, muss die verantwortliche Stelle für die Übernahme der getroffenen Änderungen sorgen. Die verantwortliche Stelle hat dem Betroffenen auf Anfrage und ohne Entstehung von Kosten nachzuweisen, dass sie dem Verlangen des Betroffenen nachgekommen ist. Wurde eine Veränderung vorgenommen, kann sich der Betroffene auch evtl. von ihm im Vorfeld getragenen Abfragekosten erstatten lassen.
Verfahrensmodifikationen beim Zugangs- und Abfragerecht des Betroffenen sind gem. Art. 40 LIFL nur vorgesehen, wenn die Staatssicherheit, die Landesverteidigung oder die öffentliche Sicherheit (*la sûreté de l'Etat, la défense ou la sécurité publique*) betroffen sind. Hier besteht lediglich ein indirektes Zugangsrecht mit Zwischenschaltung der CNIL.[46]
Ein weiterer Sonderfall liegt bei medizinischen personenbezogenen Daten vor, Art. 41 LIFL. Der Betroffene hat ein Wahlrecht zwischen der direkten Übermittlung der vorhandenen Daten oder der Zwischenschaltung eines durch ihn benannten Arztes.

(4) Grenzüberschreitender Datenverkehr

Maßgeblich für die Anwendbarkeit französischen Rechts und damit des LIFL ist nach Art. 5 LIFL zunächst die Niederlassung der verantwortlichen Stelle auf dem französischen Staatsgebiet.[47] Für den grenzüberschreitenden Datenverkehr[48] enthält das französische Datenschutzgesetz außerdem Regelungen betreffend die Übertragungen von personenbezogenen Daten in Staaten außerhalb der Europäischen Union.[49] Nach Art. 68 LIFL soll eine solche Übertragung nur bei in Hinblick auf die Privatsphäre, Freiheitsrechte und Grundrechte sichergestelltem ausreichendem Schutzniveau gestattet sein. Maßgeblich für die Bewertung des Schutzniveaus sind insbesondere die geltenden Rechtsvorschriften des jeweiligen Staats, die dort angewandten Sicherheitsmaßnahmen, die Charakteristika der Datenverarbeitung selbst, wie ihre Zwecke und Dauer, sowie die Natur, Herkunft und Bestimmung der personenbezogenen Daten.
Falls die Bedingung eines ausreichenden Schutzniveaus nicht erfüllt sein sollte, kann ein Datentransfer nur bei ausdrücklichem Einverständnis des Betroffenen erfolgen oder wenn aufgrund einer der Voraussetzungen des Art. 69 LIFL die Notwendigkeit der Übermittlung gegeben ist: Die

---

45 *Desgens,Pasanau*, S. 57. Ausführlicher zu den Formalitäten der Abfrage durch den Betroffenen und Beantwortung durch die verantwortliche Stelle *Féral-Schuhl*, Rn. 12.47 f.

46 *Vulliet-Tavernier*, Droit social 2004, 1055 (1057 f.). Ausführlicher dazu *Desgens,Pasanau*, S. 58 f.

47 Ausführlicher s.o.

48 Zur Rechtslage vor Umsetzung der Datenschutzrichtlinie *Ellger*, S. 370 ff.

49 Ausführlicher dazu *Féral-Schuhl*, Rn. 15.00 ff.

Rettung des Lebens des Betroffenen (Nr. 1), der Schutz des öffentlichen Interesses (Nr. 2), die Ermöglichung der gerichtlichen Feststellung, Ausübung oder Verteidigung eines Rechts (Nr. 3), unter bestimmten Umständen die Einsichtnahme in ein öffentliches Register (Nr. 4), die Ausführung eines Vertrags zwischen der verarbeitenden Stelle und dem Betroffenen bzw. die Vornahme vorvertraglicher Handlungen auf Wunsch des Betroffenen (Nr. 5) oder im Rahmen eines den Betroffenen begünstigenden Vertrags zugunsten Dritter (Nr. 6). Weitere Ausnahmen sind im Falle einer Erlaubnis der CNIL möglich, müssen durch die CNIL allerdings der Europäischen Kommission sowie den Kontrollbehörden der anderen Mitgliedstaaten zu Kenntnis gebracht werden. Die Einschlägigkeit der in Art. 69 LIFL aufgelisteten Ausnahmefälle bedeutet jedoch ein Entfallen der Notwendigkeit einer Erlaubnis durch die CNIL und ist aus Perspektive der CNIL deshalb eng auszulegen und auf Einzel- und Ausnahmefälle zu begrenzen.[50]

cc) Durchsetzungsmechanismen

Durch das loi n° 78-17 wurde erstmalig eine nationale Datenschutzkomission geschaffen.[51] Die Durchsetzung der Vorschriften des LIFL obliegt der CNIL. Eine Anrufung der CNIL ist jedoch aus Sicht des Einzelnen nicht zwingend erforderlich, zugleich steht den Betroffenen im Falle einer Rechtsverletzung nämlich auch der Weg der gerichtlichen Durchsetzung frei. Eine wichtige Rolle spielt die Deliktshaftung nach Art. 1382 Code civil.[52] Beide Durchsetzungsmöglichkeiten bestehen nebeneinander, unterscheiden und ergänzen sich aber insofern, als die Tätigkeit der CNIL nicht lediglich auf die nachträgliche Sanktionierung von Rechtsverstößen gerichtet ist, sondern gleichermaßen präventiv tätig wird.[53] Dies geschieht insbesondere durch deren Aufklärungsarbeit gegenüber den datenverarbeitenden Stellen und betroffenen Personen in Hinblick auf ihre jeweiligen Rechte und Pflichten.[54]

Hinzu kommen strafrechtliche Sanktionen. Zunächst enthält Art. 50 LIFL den Verweis auf das französische Strafgesetzbuch, nämlich auf die Art. 226-16 bis 226-24 Code pénal. Art 226-16 Code pénal beispielsweise stellt die Missachtung der gesetzlichen Rahmenbedingungen bei der Verarbeitung personenbezogener Daten unter bis zu fünfjährige Freiheits- bzw. Geldstrafe i.H.v. 300.000 Euro. Die gleiche Strafe droht nach Art. 226-17 Code pénal bei Missachtung der nach Art. 34 LIFL bestehenden Pflicht zur Datensicherheit, nach Art. 226-18 Code pénal bei Erhebung personenbezogener Daten auf betrügerische, unredliche und unrechtmäßige Art und Weise, gem. Art. 226-18-1 Code pénal bei Verarbeitung personenbezogener Daten zu Werbezwecken trotz Widerstand/Widerspruch (*opposition*) des Betroffenen, gem. Art. 226-19 Code pénal die Sammlung von sog. sensiblen Daten außerhalb der gesetzlich vorgesehen Fälle und ohne Einwilligung der Betroffenen, gem. Art. 226-20 Code pénal die Datenspeicherung über den erlaubten Zeitraum hinaus, gem. Art. 226-21 Code pénal u.U. die Zweckentfremdung der Daten und gem. Art. 226-22 Code pénal potentiell rufschädigende oder intimsphäreverletzende Verbreitung personenbezogener Daten ohne Einverständnis des Betroffenen. Daneben enthält das LIFL aber auch eigene strafrechtliche Regelungen. Im Falle einer Behinderung der Tätigkeit der CNIL kann gem. Art. 51 LIFL eine Freiheitsstrafe von einem Jahr oder eine Geldstrafe von 15.000 Euro verhängt werden.

---

50 *Desgens,Pasanau*, S. 50.

51 *Bodenschatz*, S. 71; *Grewe*, DÖV 2002, 1022 (1024).

52 Ausfühlicher zu den eine deliktische Haftung auslösenden Verhaltensweisen *Féral-Schuhl*, Rn. 12.14 und 12.26.

53 Vgl. *Vulliet-Tavernier*, Droit social 2004, 1055 (1057). Eingehender zum Verhältnis der CNIL zur gerichtlichen Durchsetzung *Mattatia*, CNIL et tribunaus : concurrence ou complémentarité dans la répression des infractions à la loi informatique et libertés?, RSC 2009, 317 (327 ff.).

54 *Barton/Weißnicht*, MMR 2008, 149 (152).

Darüber hinaus sind auch die Verschaffung des unberechtigten Zugangs zu Datenverarbeitungssystemen und die Veränderung oder Hinzufügung von Daten sowie die Verfälschung der Funktionsfähigkeit des Systems nach Art. 323-1 bis 323-3 Code pénal strafbar.[55]

b. Struktur des materiellen Urheberrechts in Frankreich

aa) Bestand und Grundstruktur der Regelungen zum Urheberrecht

Die für das Urheberrecht in Frankreich maßgeblichen Regelungen finden sich im französischen Gesetzbuch zum Geistigen Eigentum, dem *Code de la propriété intellectuelle* (CPI). Der CPI enthält in Teil 2 Bestimmungen über das gewerbliche Eigentum (*propriété industrielle*); in Teil 1 Bestimmungen über das geistige Eigentum im engeren Sinne (*propriété littéraire et artistique*), worunter das Urheberrecht (*droit d'auteur*) und verwandte Schutzrechte (*droits voisins du droit d'auteur*) fallen. Zu deren Schutz bzw. Durchsetzung finden sich gemeinsame Regelungen in Buch 3 des Teil 1. Hier sind auch daneben Sonderregeln über die Rechte von Datenbankbetreibern verortet.

bb) Sonderregeln für die digitale Welt

(1) Überblick

Speziell in Bezug auf die Verbraucher und die digitale Welt kommt im französischen Urheberrecht den neueren Regelungen über Urheberrechtsverstöße im Internet ein besonderer Stellenwert zu. Die zunehmende Verbreitung des Internets und die erheblichen technischen Fortschritte der letzten Jahre haben nämlich auch in Frankreich zu einem Anstieg der Urheberrechtsverstöße, insbesondere durch illegales Filesharing (*téléchargement illégal*) geführt.[56] Beispielsweise soll die Verbreitung von Musikdateien im Internet lediglich zu fünf Prozent auf legalem Wege erfolgen.[57]
Gegen Urheberrechtsverletzungen im Internet wurden in Frankreich in den letzten Jahren deshalb eine Reihe neuer Regelung geschaffen, die sowohl auf Prävention als auch auf Repression abzielen. Die einzelnen Maßnahmen richten sich nicht nur gegen denjenigen, der die Urheberrechtsverletzung durch illegales Filesharing begeht, sondern betreffen ebenfalls die Erbringer von Onlinedienstleistungen, den Inhaber des benutzten Internetanschlusses sowie dessen Internetprovider. Das liegt auch an der besseren Identifizierbarkeit letztgenannter Personen. Hinzu kommt die größere Effektivität einer Verringerung der Möglichkeiten und Wege illegalen Filesharings.
Neben der Einführung neuer Repressions- und Präventionsregelungen wurde eine staatliche Sonderbehörde eingerichtet, die hohe Autorität für die Verbreitung von Werken und den Schutz von Rechten im Internet (*Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* – HADOPI).[58] Vor allem mithilfe des Verfahrens der „abgestuften Antwort“ (*réponse graduée*) soll sie insbesondere Urheberrechtsverletzungen durch illegales Filesharing im Internet

---

55 *Aye*, S. 113.

56 Belege zum Ausmaß des illegalen Filesharings bis zum Jahr 2010 bei *Derieux/Granchet*, Lutte contre le téléchargement illégal, Lamy : Rueil-Malmaison Cedex (Frankreich) 2010, Rn. 2-13. Bis zum Jahr 2006 s. *Cédras*, Un aspect de la cybercriminalité en droit français : le téléchargement illicite d'œuvres protégées par le droit d'auteur, Revue internationale de droit pénal (RIDP) Vol. 77 (2006), S. 586-610 (594 f.).

57 *Mirski*, HADOPI : Des premiers resultats concluant, Revue internationale de la propriété industrielle et artistique (RIPIA) 2011, S. 61-62 (61).

58 Internetauftritt unter <www.hadopi.fr>.

eindämmen. Dabei handelt es sich um eine Art „Three-Strikes"-System,[59] bei dem letztlich u.a. die Sperrung des Internetzugangs droht und das seit Ende 2010 zur Anwendung kommt.[60]
Nicht zu vernachlässigen ist allerdings, dass es einerseits Mittel gibt, um die Identifikation anhand der IP-Adresse zu umgehen und sich andererseits im Internet immer mehr alternative Methoden zum Filesharing unter Verwendung von „peer to peer"-Software auftun.[61] Es kann mithin weiter zu vergleichbaren Urheberrechtsverletzungen im Internet kommen. Deshalb werden daneben Erwartungen in Aufklärungsmaßnahmen im Rahmen des Schulunterrichts zur Schaffung eines größeren Unrechtsbewusstseins und in die Weiterentwicklung des legalen Angebots im Internet gesetzt.[62]
Teilweise im Zusammenhang mit der *réponse graduée*, aber auch losgelöst davon, sind in Frankreich darüber hinaus verschiedene Einzelprobleme Gegenstand juristischer Auseinandersetzung und Diskussion. Diese betreffen unter anderem die Rechtsnatur und die Qualifikation des illegalen Filesharings, insbesondere im „peer to peer"-System, die mögliche Anwendung der Ausnahmeregelungen über die *copie privée* oder *représentation privée*, die Frage, ob es sich bei IP-Adressen um personenbezogene Daten handelt, die Rechtsnatur und Grundrechtskonformität der (behördlichen) Sanktionen.[63] Gerade die umstrittene Identifikation des Anschlussinhabers anhand der IP-Adresse,[64] der Umgang mit datenschutzrechtlichen Fragen[65] und die Beeinträchtigung von Kommunikationsfreiheit und Persönlichkeitsrechten standen über längere Zeit im Zentrum der Kritik am Verfahren der *réponse graduée* und der drohenden Sperrung des Internetanschlusses.

(2) Neue gesetzliche Rahmenbedingungen: DADVSI, HADOPI 1 und HADOPI 2

Auf dem Gebiet des Urheberrechts wurde der französische Gesetzgeber zur Bekämpfung der Urheberrechtsverletzungen im Internet, insbesondere des illegalen Filesharings, in den letzten

---

59 Vgl. *Benabou*, The Chase: The French Insight into the 'Three Strikes System', in: *Stamatoudi* (Hrsg.), Copyright Enforcement and the Internet, Wolters Kluwer: Alphen aan den Rijn (Niederlande) 2010, S. 163-182; *Gesmann-Nuissl/Wünsche*, Neue Ansätze zur Bekämpfung der Internetpiraterie – ein Blick über die Grenzen, GRURInt 2012, S. 225-234 (231); *Pritzkow*, Zur Sperrung des Internetzugangs nach den Hadopi-Gesetzen in Frankreich, MR-Int 2010, S. 51-54 (54); *Solmecke/Sebastian/Sahuc*, Experiment Internetsperre: Das erste Jahr des Hadopi-Gesetzes, MMR-Aktuell 2011, 316298; *Spies*, Frankreich: Eins, zwei drei, das Internet ist weg – oder doch nicht?, MMR 2009, S. 437-438 (437).

60 Zu den verfassungsrechtlichen Bedenken aus deutscher Sicht gegenüber Internetsperren *Greve/Schärdel*, Zwischenruf – Internetsperren wegen Urheberrechtsverstößen, ZRP 2009, S. 54- 55 (55).

61 *Kerr-Vignale*, RIPIA 2010, S. 78 f.

62 Vgl. *Mirski*, RIPIA 2011, S. 61-62. Stichwörter "éducation" und "chronologie des médias".

63 *Derieux/Granchet*, Rn. 26.

64 Dazu *Marino*, Recueil Dalloz 2010, S. 163.

65 Dazu *Nérisson,* GRURInt 2010, S. 637-639 (639), *Strowel*, S. 151 f.

Jahren in drei Schritten tätig[66]: Zuerst 2006 mit dem DADVSI Gesetz,[67] dann im Juni 2009 mit dem HADOPI 1 Gesetz[68] und schließlich im Oktober 2009 mit dem HADOPI 2 Gesetz[69].
Hintergrund für dieses gesetzgeberische Tätigwerden war die Tatsache, dass für Urheberrechtsverstöße im Internet im französischen Gesetzbuch des Geistigen Eigentums (*Code de la propriété intellectuelle*) zwar bereits überwiegend strafrechtliche[70] Sanktionen zur Verfügung standen, diese jedoch als zu streng und (deshalb) als unanwendbar oder ungeeignet erachtet wurden.[71] Auf zivilrechtlichem Weg können zudem Schadensersatzansprüche geltend gemacht werden, allerdings fielen diesbezügliche Urteile im Einzelnen sehr maßvoll aus: Beispielsweise im Musikbereich liegt der zugesprochene Schadensersatz bei illegalem Filesharing bei ein bis zwei Euro pro Titel, zuzüglich Gerichtskosten.[72]
Ein erster Entwurf des DADVSI Gesetzes, das auch der Umsetzung der Richtlinie 2001/29/EG[73] dient, wurde bereits im November 2003 im französischen Ministerrat (*Conseil des ministres*) präsentiert.[74] Tatsächlich wurde es nach verschiedenen Änderungen aber erst 2006 verabschiedet.[75] Das Gesetz legt den Grundstein für präventives und repressives Vorgehen speziell gegen illegales Filesharing (aber auch andere im Internet begangene Verletzung von Urheberrechten oder verwandten Schutzrechten). In der französischen Literatur wird diese zweiseitige Ausrichtung der Maßnahmen auch mit den Bezeichnungen „*volet pénal*" für die repressiven Strafregelungen und „*volet civil*" für die zivilrechtlich eingeordneten Präventionsregelungen veranschaulicht.[76] Nicht verhehlen lässt sich, dass das DADVSI Gesetz auch weiterhin die strafrechtliche Ahndung des illegalen Filesharings und damit im Zusammenhang stehender Handlungen ermöglichen will.[77]

---

66 Detaillierte Literaturhinweise hierzu bei *Sirinelli et al.*, Code de la propriété intellectuelle, 11. Aufl. Dalloz: Paris 2010, *Commentaire* zur *Première partie*, S. 5 ff. Zu den Quellen des französischen Internetrechts im Allgemeinen s. *Duong*, Les sources du droit d'internet : du modèle pyramidal au modèle en réseau, Recueil Dalloz 2010, S. 783-789.

67 Gesetz Nr. 2006-961 vom 1.8.2006 in Bezug auf das Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft (*loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information* – DADVSI).

68 Gesetz Nr. 2009-669 vom 12.6.2009 zur Förderung der Verbreitung und des Schutzes von Werken im Internet (*loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection des œuvres sur internet*, auch „*Création et Internet*" genannt bzw. HADOPI 1).

69 Gesetz Nr. 2009-1311 vom 28.10.2009 in Bezug auf den strafrechtlichen Schutz des Geistigen Eigentums (*loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique* – HADOPI 2).

70 Insbesondere Art. L. 335-2, L. 335-3 und L. 335-4 CPI.

71 *Derieux/Granchet*, Rn. 28.

72 *Dimeglio*, Téléchargement illégal : quels sont les risques encourus?, LeJournalduNet, Chronique e-Business vom 01.03.2007, abrufbar unter <http://www.journaldunet.com/ebusiness/expert/ 9763/telechargement-illegal---quels-sont-les-risques-encourus.shtml>.

73 Richtlinie2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.

74 *Derieux/Granchet*, Rn. 16, dort Fn. 2.

75 Zu den verschiedenen erwägten Lösungen *Geiger*, « HADOPI », ou quand la répression devient pédagogique, Recueil Dalloz 2011, S. 773-779 (774 f.).

76 *Sirinelli et al.*, *Commentaire* zu Art. L. 335-2-1 und *Commentaire* zu Art. L. 336-1.

77 *Dimeglio*. Zum strafrechtlichen Ansatz des Gesetzes DADVSI eingehend ein Rundbrief des französischen Justizministeriums, circulaire du garde des Sceaux du 3 janv. 2007, CRIM 2007 – 1/G3-030107.

Von einer – ursprünglich angestrebten – Entkriminalisierung (*dépénalisation*) kann mithin keine Rede sein.[78]
Das HADOPI 1 Gesetz ist – als Reaktion auf eine Entscheidung des französischen Verfassungsrats (*Conseil constitutionnel*) zum DADVSI Gesetz[79] – in Bezug auf strafrechtliche Regelungen vergleichsweise zurückhaltend.[80] Es verfolgt vielmehr einen verwaltungsrechtlichen Ansatz, wobei neben zusätzlichen Präventionsregelungen die Schaffung der HADOPI-Behörde als Sonderbehörde gegen Urheberrechtsverletzungen im Internet im Vordergrund steht.[81]
Anders das HADOPI 2 Gesetz: Wie schon die Gesetzesbezeichnung („*protection pénale de la propriété littéraire et artistique*“) zeigt, bezieht es sich stark auf den strafrechtlichen Schutz des Geistigen Eigentums. Die strafrechtlich orientierten Regelungen des CPI erhalten hierdurch schließlich ihre vorliegende und wohl auch endgültige Fassung. Ferner trägt das HADOPI 2 Gesetz dem Umstand Rechnung, dass auch das HADOPI 1 Gesetz vom französischen Verfassungsrat (*Conseil constitutionnel*) in einigen Teilen erneut für verfassungswidrig erklärt wurde.[82]

(3) Strafrechtliche Durchsetzung

(a) Bestrafung der Förderung von Urheberechtsverletzungen im Internet

Art. 21 des DADVSI Gesetzes schafft im CPI einen neuen Art. L. 335-2-1 im bereits bestehenden Kapitel V („*Dispositions pénales*“) über die strafrechtlichen Bestimmungen. Systematisch befindet sich dieses Kapitel des CPI im Ersten Teil über das Urheberrecht i.w.S., dort in Buch III über die Allgemeinen Bestimmungen in Bezug auf das Urheberrecht, verwandte Schutzrechte und Rechte der Ersteller von Datenbanken, und schließlich dort in Titel III über die Prävention, Verfahren und Sanktionen bei Verstößen.[83] Aufgrund von Art. L. 335-2-1 CPI können bestimmte Personen, die den verbotenen Austausch geschützter Werke in Netz(werk)en erleichtern, ermöglichen oder fördern, mit ähnlichen Strafen belegt werden, wie sie für den Urheberrechtsverstoß selbst bestimmt sind.[84] Inspiriert wird die Vorschrift des Art. L. 335-2-1 CPI durch die Entscheidungen *Grokster*[85] in den Vereinigten Staaten und *Kazaa*[86] in Australien.[87] Ihr Vorteil liegt darin, dass die Softwareersteller üblicherweise einfacher strafrechtlich verfolgbar sind als die einzelnen Internetnutzer und somit größere Steuerungseffekte erzielt werden können.[88] Vorgesehen sind nach Art. L. 335-2-1 CPI eine Gefängnisstrafe von drei Jahren und eine Geldstrafe von 300.000 Euro. Tathandlung ist das vorsätzliche Herstellen, öffentliche Zurverfügungstellen oder öffentliche Bekanntgeben von

---

78 Vgl. Geiger, Recueil Dalloz 2011, S. 775.

79 Décision du Conseil constitutionnel n° 2006-540 DC du 7 juill. 2006.

80 *Marino*, La loi du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet (dite HADOPI 2), Recueil Dalloz 2010, S. 160-164 (161).

81 Vgl. *Derieux/Granchet*, Rn. 39.

82 Décision du Conseil constitutionnel n° 2009-580 DC du 10 juin 2009. Dazu *Verpeaux*, La liberté de communication avant tout. La censure de la loi Hadopi 1 par le Conseil constitutionnel, JCP G 2009, étude 274, S. 46-52.

83 Première partie (La propriété littéraire et artistique), Livre III (Dispositions générales relatives au droit d'auteur, aux droits voisins et droits des producteurs de bases de données), Titre III (Prévention, procédures et sanctions).

84 *Sirinelli et al.*, *Commentaire* zu Chapitre V vor Art. L. 335-1.

85 MGM und 27 andere Gesellschaften c/ Grokster, 27.6.2005, 545 U.S. 913 (2005).

86 Universal Music Australia und 29 andere Gesellschaften v. Sharman Networks und neun andere Gesellschaften, FCA 1245 (5.12.2005).

87 *Sirinelli et al.*, *Commentaire* zu Art. L. 335-2-1.

88 Vgl. *Cédras*, RIDP Vol. 77 (2006), S. 598.

Software, die offensichtlich dazu bestimmt ist, geschützte Werke oder Gegenstände unbefugt öffentlich zur Verfügung zu stellen (Art. L. 335-2-1 Abs. 1 Nr. 1 CPI). Diese strafrechtliche Verantwortlichkeit besteht unbeschadet einer Verantwortlichkeit wegen Beihilfe und stellt im Wesentlichen darauf ab, ob hinreichend vorsätzlich („*sciemment*“)[89] gehandelt wird und die Software offensichtlich („*manifestement*“) für die genannten Zwecke bestimmt ist.[90] Beides muss eindeutig nachgewiesen werden. Zum anderen sind die gleichen Strafen für die ebenfalls hinreichend vorsätzliche Anstiftung, was auch durch Werbeanzeige geschehen kann, zur Benutzung besagter Software vorgesehen (Art. L. 335-2-1 Abs. 1 Nr. 2 CPI). Vormals wurden diese Bestimmungen des Abs. 1 durch einen Abs. 2 für diejenigen Arten von Software für unanwendbar erklärt, die zur computerunterstützten Gruppenarbeit mit Simultanzugriff auf Programme und Dateien, bzw. zur Suche oder zum Austausch von nicht der urheberrechtlichen Vergütungspflicht unterworfenen Dateien oder Objekten bestimmt sind. Dieser zweite Absatz des Art. L. 335-2-1 CPI ist durch den französischen Verfassungsrat (*Conseil constitutionnel*) für verfassungswidrig erklärt worden.[91] Nachdem jedenfalls bis 2011 keinerlei[92] bzw. bis 2010 kaum[93] Urteile auf Grundlage des Art. L. 335-2-1 CPI ergangen sind, entsteht der Eindruck, dass diese Vorschrift in der Praxis nicht wirklich zur Anwendung kommt. Ferner finden die Internetnutzer immer wieder neue Plattformen und Wege zu illegalem Filesharing, weshalb sich hier kein deutlicher Rückgang speziell aufgrund des Art. L. 335-2-1 CPI verzeichnen lässt.[94]

(b) Bestrafung der Verletzung oder Umgehung technischer Schutz- oder Informationsmaßnahmen

Hinzu kommt die Einführung von Strafen für die Verletzung oder Umgehung technischer Schutz- oder Informationsmaßnahmen (DRM, Digital Rights Management) durch Art. 22 des DADVSI Gesetzes in Art. L. 335-3-1, L. 335-3-2, für Urheberrechte und in Art. L. 335-4-1, L. 335-4-2 CPI für verwandte Schutzrechte.[95]

(c) Bestrafung der Urheberrechtsverletzung durch illegales Filesharing

Ursprünglich enthielt der Entwurf zum DADVSI Gesetz in Art. 24 durch Schaffung eines neuen Art. L. 335-11 CPI außerdem eine besondere Strafregelung gerade und ausdrücklich für das illegale Filesharing.[96] Erklärtes Ziel war dabei die Entkriminalisierung der mit überwiegend fehlendem Unrechtbewusstsein handelnden Internetnutzer (*contraventionnalisation* statt *pénalisation*).[97] Vorgesehen war ein durch Dekret des die Regierung beratenden obersten Verwaltungsgerichts (*décret en Conseil d'État*) näher auszugestaltendes System abgestufter Strafen mit unterschiedlichen Sanktionen im Verhältnis zur Schwere der Rechtsverletzung; beispielsweise wurde der einfache

---

89 „sciemment“ entspricht dem *dolus directus* und umfasst jegliches Handeln mit Vorbedacht, was sowohl Absicht als auch Wissentlichkeit bedeuten kann.

90 *Sirinelli et al.*, *Commentaire* zu Art. L. 335-2-1.

91 Décision du Conseil constitutionnel n° 2006-540 DC du 7 juill. 2006.

92 *Geiger*, Recueil Dalloz 2011, S. 775.

93 *Benabou*, S. 166.

94 *Benabou*, S. 166.

95 Vgl. *Binctin*, Droit de la propriété intellectuelle, Lextenso éditions: Paris 2010, Rn. 1220 ff.*; Cédras*, RIDP Vol. 77 (2006), S. 597; *Dimeglio*.

96 *Nérisson*, Frankreich – Die erste Stufe der Internetsperre bei Online-Urheberrechtsverletzungen soll Ende Juni eintreten, GRURInt 2010, S. 637-639 (637).

97 Vgl. *Derieux/Granchet*, Rn. 36.

Download mit einer Geldstrafe von 38 Euro belegt.[98] Über eine solches „pädagogische[s] Bußgeld“ hinaus hätten aber auch schwerwiegendere Sanktionen verhängt werden können.[99] Gerade für dieses abgestufte System wurde der Begriff der „*réponse graduée*“[100] ursprünglich geprägt.[101] Nach der Entscheidung des französischen Verfassungsrats (*Conseil constitutionnel*) ist die spezielle Strafregelung allerdings verfassungswidrig.[102] Begründet wird die Verfassungswidrigkeit mit einer Diskriminierung der Filesharer gegenüber anderen Urheberrechtsverletzern, wenn für vergleichbare Verletzungen unterschiedliche Strafen vorgesehen werden. Das würde dem Grundsatz der Gleichheit vor dem Gesetz (*égalité devant la loi pénale*) widersprechen. Kritisiert wird in der Literatur, dass diese Entscheidung die Unterschiede zwischen einem unbedachten und kaum unrechtsbewussten Internetnutzer, der lediglich für den Eigengebrauch handelt, und denjenigen Urheberrechtsverletzern, die vielfach und gewinnorientiert handeln, vernachlässigt.[103] Außerdem wird angebracht, dass das Verhältnismäßigkeitsprinzip (*principe de proportionnalité*), wie es in einem abgestufen Strafsystem zum Ausdruck kommt, verfassungsrechtlich gegenüber dem Gleichbehandlungsgrundsatz (*principe d’égalité*) gleichwertig ist und im Urteil nicht angemessen berücksichtigt wird.[104]

Wegen der Entscheidung des französischen Verfassungsrats (*Conseil constitutionnel*) werden bei illegalem Filesharing nun weiterhin die für jegliche Art der Urheberrechtsverletzung vorgesehenen strafrechtlichen Sanktionen aus Art. L. 335-2, L. 335-3 und L. 335-4 CPI angewandt, die bis zu einer Gefängnisstrafe von drei Jahren und bis zu einer Geldstrafe von 300.000 Euro reichen können.[105] Hierbei handelt es sich allerdings um eine Strafobergrenze, die durch die Gerichte in der Praxis deutlich unterschritten und in der Regel zur Bewährung ausgesetzt wird.[106] Einige Gerichte gehen nicht einmal so weit, sondern wollen in bestimmten Fällen sogar die Ausnahme der Privatkopie (*exception de copie privée*) anwenden. Diese Tendenz der Rechtsprechung scheint jedoch seit dem – eine derartige Entscheidung[107] des Berufungsgerichts in Montpellier (*Cour d’appel de Montpellier*) aufhebenden – Urteil des französischen Kassationsgerichts (*Cour de cassation*) vom 30.5.2006 im Rückgang.[108] Die Auslegung der Vorschriften zur *copie privée*[109] als auf Fälle des

---

98 *Dimeglio*.

99 *Nérisson*, GRURInt 2010, S. 637.

100 Sogar teilweise noch kämpferischer als „*riposte graduée*“ bezeichnet.

101 *Cédras*, RIDP Vol. 77 (2006), S. 596; *Geiger*, Recueil Dalloz 2011, S. 775.

102 Décision des Conseil constitutionnel n° 2006-540 DC vom 27.7.2006, JO vom 3.8.2006, S. 11541, Rn. 65. Deutsche Übersetzung abrufbar unter <http://www.conseil-constitutionnel.fr /conseil-constitutionnel/root/bank/download/2006540DCde2006_540dc.pdf>.

103 *Cédras*, RIDP Vol. 77 (2006), S. 596; *Geiger*, Recueil Dalloz 2011, S. 775.

104 *Cédras*, RIDP Vol. 77 (2006), S. 596.

105 Zu diesen allgemeinen strafrechtlichen Sanktionen *Binctin*, Rn. 1176 ff.

106 Vgl. *Cédras*, RIDP Vol. 77 (2006), S. 597; *Dimeglio*.

107 Diese Entscheidung hatte jedoch nicht direkt das Filesharing im Internet zum Gegenstand, sondern die Verbreitung auf CDs gebrannter Filme im Freundeskreis, vgl. zu CA Montpellier, 10.3.2005, Anm. von *Caron*, Le téléchargement d’oeuvres protegées entre contrefacon et copie privée, JCP G 2005, II 10078, S. 1130-1131.

108 CA Aix-en-Provence, 5.9.2007, RTD com. 2008, S. 301; *Dimeglio* (Fn. 13).

109 Ausführlich zur *exception de copie privée Cédras*, RIDP Vol. 77 (2006), S. 600 ff. Dazu auch *Singh*, Loi « Création et Internet » : une obligation « floue » à la charge de l’internaute ?, Recueil Dalloz 2009, S. 306-307.

illegalen Filesharings im Internet unanwendbar wird auch durch einen Rundbrief des französischen Justizministeriums[110] bestärkt. Gleichwohl werden darin abgestufte Strafen empfohlen, insbesondere die Geldstrafe unter Berücksichtigung des Einkommens des Betroffenen, der Anzahl der ausgetauschten Dateien, des Zeitpunkts des Filesharings (vor oder nach Markteinführung des Werkes) und der automatischen Zurverfügungstellung im Rahmen von „peer to peer"-Software.[111] Der französische Gesetzgeber hat seine Lehren aus den Urteilen des französischen Verfassungsrates zu den DADVSI und HADOPI 1 Gesetzen gezogen: Das HADOPI 2 Gesetz schafft keinen neuen, speziellen Straftatbestand für illegales Filesharing, sondern die Möglichkeit der Verhängung einer Zusatzstrafe (*peine complémentaire*), nämlich die Sperrung des Internetanschlusses, bei Urheberrechtsverletzungen nach Art. L. 335-2, L. 335-3 und L. 335-4 CPI. Durch Art. 7 des HADOPI 2 Gesetzes entsteht dafür ein neuer Art. L. 335-7 CPI; der bisherige Art. L. 335-7 CPI zu zivilrechtlichen Schadensersatzansprüchen im Rahmen einer Art Adhesionsverfahren entfällt.[112] Wie schon die Bezeichnung als Zusatzstrafe erkennen lässt, kann diese Strafe zusätzlich zu den nach Art. L. 335-2, L. 335-3 und L. 335-4 CPI drohenden Gefängnis- und Geldstrafen verhängt werden. Art. 131-11 Abs. 2 des französischen Strafgesetzbuchs (*Code pénal*) ermöglicht jedoch auch die Anordnung der Zusatzstrafe allein. Diese will so vor allem „pädagogisch" erscheinen, was nicht über ihre Eingriffsintensität hinweg täuschen darf:[113] Für die Dauer von bis zu einem Jahr kann eine Sperrung des Internetanschlusses sowie das Verbot des Abschlusses eines neuen Providervertrags ausgesprochen werden, Art. L. 335-7 Abs. 1 CPI. Die Sperrung soll sich nach Art. L. 335-7 Abs. 2 CPI bei kombinierten Verträgen nicht auf die anderen Komponenten wie Festnetz- oder Fernsehanschluss beziehen. In Hinblick auf den Gleichbehandlungsgrundsatz erscheint dabei problematisch, dass sich in einigen Regionen Frankreichs die bloße Sperrung des Internets bei solchen kombinierten Verträgen technisch nicht umsetzen lässt.[114] Außerdem bleibt die Sperrung ohne Einfluss auf die gegenüber dem Internetprovider geschuldeten Grundgebühren und ähnliche vertragliche Zahlungspflichten (vgl. Art. L. 335-7 Abs. 3 CPI). Art. L. 121-48 des französischen Verbrauchergesetzbuchs (*Code de la consommation*), wonach bei Änderungen der Vertragskonditionen eine Informationspflicht des Internetproviders und ein erleichtertes Kündigungsrecht des Anschlussinhabers bestehen, wird für den Lauf der Internetsperre ausdrücklich für unanwendbar erklärt. Sofern sich doch die Möglichkeit der Kündigung während des Zeitraums der Internetsperre ergibt, hat der Anschlussinhaber gem. Art. L. 335-7 Abs. 4 CPI die dadurch entstehenden Kosten zu tragen. Eine Besonderheit gegenüber anderen strafrechtlichen Sanktionen ist die Tatsache, dass die Verurteilung nach Art. L. 335-7 CPI keine Aufnahme ins Vorstrafenregister findet, Art. L. 335-7 Abs. 7 CPI i.V.m Art. 777 Nr. 3 des französischen Strafprozessgesetzbuchs (*Code de procédure pénale*). Allerdings wird die Effektivität dieser Sanktion teilweise stark bezweifelt.[115] Einerseits bleibt sie ohnehin wirkungslos, wenn der Urheberrechtsverletzter selbst gar keinen eigenen Internetanschluss hat. Andererseits kann er trotz eigener Anschlusssperre weiterhin einen fremden Internetzugang (eines anderen Familienmitglieds oder eines Mitbewohners) nutzen.

---

110 Circulaire du garde des Sceaux du 3 janv. 2007 (Fn. 18).

111 *Dimeglio*.

112 Zum bisherigen Art. L. 335-7 *Sirinelli et al.*, *Annotation* zu Art. L. 335-7.

113 *Marino*, Recueil Dalloz 2010, S. 161.

114 *Solmecke/Sebastian/Sahuc*, MMR-Aktuell 2011, Nr. 316298.

115 *Marino*, Recueil Dalloz 2010, S. 162.

Im Hinblick auf die Strafzumessung implementiert Art. 9 des HADOPI 2 Gesetzes den neuen Art. L. 335-7-2 CPI. Durch das Gericht zu berücksichtigen sind hier die Umstände und die Schwere der Urheberrechtsverletzung, sowie die Person des Verletzers und insbesondere dessen berufliche oder soziale Tätigkeit als auch seine sozio-ökonomische Situation. Dazu gehört beispielsweise die Abhängigkeit vom Internet bei der Ausübung der beruflichen Tätigkeit.[116] Die Dauer der verhängten Strafe muss darüber hinaus den Schutz des Geistigen Eigentums und die Achtung vor der Meinungsäußerungs- und Kommunikationsfreiheit („*droit de s'exprimer et de communiquer librement*"), insbesondere von zu Hause aus, in Einklang bringen.
Widersetzt sich der wegen illegalem Filesharing mit einer Internetsperre bestrafte Urheberrechtsverletzer dem Verbot einen neuen Internetprovidervertrag abzuschließen, droht ihm nach Art. 434-41 des französischen Strafgesetzbuchs (*Code pénal*) eine Gefängnisstrafe von zwei Jahren und eine Geldstrafe von 30.000 Euro.

(d) Bestrafung der Inhaber von zu Urheberechtsverletzungen benutzter Internetanschlüsse
Außerdem wird den Inhabern eines Internetanschlusses durch das DADVSI Gesetz eine Pflicht zur Überwachung ihres Anschlusses gem. Art. L. 335-12 CPI auferlegt.[117] Der Anschlussinhaber soll darauf achten, dass sein Anschluss nicht zu Zwecken der Vervielfältigung oder Darbietung geistiger Schöpfungen ohne Ermächtigung durch die Rechteinhaber benutzt wird. Diese Überwachungspflicht aus Art. L. 335-12 CPI ist jedoch mit keinerlei Sanktion versehen und daher ineffektiv. Sie wird durch Art. 7 des HADOPI 1 Gesetzes aufgehoben.
Durch Art. 8 des HADOPI 2 Gesetzes entsteht aber ein neuer Art. L. 335-7-1 CPI. Im Falle einer besondere Fahrlässigkeit („*négligence caractérisée*") bei der Überwachung der Internetverbindung kann die Zusatzstrafe der Internetsperre, wie sie in Art. L. 335-7 CPI für den Urheberrechtsverletzer vorgesehen ist, unter denselben Bedingungen auch gegenüber dem – notwendigerweise personenverschiedenen [118] – Anschlussinhaber ergehen. Sie ist dann allerdings gem. Art. L. 335-7-1 Abs. 3 CPI auf einen Monat beschränkt. Für das Strafmaß ist ebenfalls Art. L. 335-7-2 CPI zu beachten (s.o.). Würde man bei einem Urheberrechtsverstoß (z.B. wegen illegalen Filesharings) automatisch den Inhaber des Internetanschlusses als Besitzer der festgestellten IP-Adresse für die Urheberrechtsverletzung verantwortlich machen, könnte dadurch die strafrechtliche Unschuldsvermutung gefährdet sein.[119] Um diese Problematik zu umgehen stellt Art. L. 335-7-1 CPI darauf ab, ob der Anschlussinhaber dem illegalen Filesharing freien Lauf lässt.[120] Sein Strafrisiko kann er durch Sicherung des Internetzugangs nach dem neuesten Stand der Technik reduzieren – allein die Einrichtung eines Routerpasswortes dürfte hierfür jedoch nicht ausreichend sein.[121] Kritisieren lässt sich daran – mit Verweis auf die durch Hacker vorgeführte Verwendung selbst der IP Adresse des französischen Kultusministeriums zu Urheberrechtsverletzungen durch illegales Filesharing – die technische Unfähigkeit durchschnittlicher Internetanschlussinhaber zur vollständigen Sicherung ihrer Verbindungen.[122] Des Weiteren enthält die Vor-

116 *Marino*, Recueil Dalloz 2010, S. 162.

117 *Geiger*, Recueil Dalloz 2011, S. 776.

118 *Larrieu/Le Stanc/Tréfigny-Goy*, Droit du numérique, Recueil Dalloz 2010, pan. 1966 – Commerce électronique, S. 1966-1975 (1967).

119 Vgl. Décision du Conseil constitutionnel n° 2009-580 DC du 10 juin 2009.

120 *Derieux/Granchet*, Rn. 493.

121 *Solmecke/Sebastian/Sahuc*, MMR-Aktuell 2011, Nr. 316298.

122 *Benabou*, S. 177; ähnlich *Marino*, Recueil Dalloz 2010, S. 163.

schrift mit der Voraussetzung einer *négligence caractérisée* speziell in Hinblick auf die Verbindungsüberwachung einen unbestimmten, noch ausfüllungsbedürftigen Rechtsbegriff,[123] was allerdings vom französischen Verfassungsrat mit dem Bestimmtheitsgrundsatz (noch) für vereinbar gehalten wird.[124] Nach Art. L. 335-7-1 Abs. 2 CPI beurteilt sich die *négligence caractérisée* vor allem danach, wie der Anschlussinhaber bei aufgetretenen Urheberrechtsverletzungen auf die Hinweise und Empfehlungen der HADOPI-Behörde gem. Art. L. 331-25 CPI im Rahmen des Verfahrens der *réponse graduée* (s.u.) reagiert hat.[125] Eine weitere Konkretisierung nimmt Art. R. 335-5 CPI vor, wonach innerhalb eines Jahres nach nachweisbarer Erteilung der zweiten Empfehlung noch eine erneute Urheberrechtsverletzung im Rahmen der dem Anschlussinhaber zuzurechnenden Verbindungen vorgefallen sein muss. Nach Art. R. 335-5 CPI besteht die *négligence caractérisée* dann entweder darin, dass keine Maßnahmen zur Sicherung des Anschlusses ergriffen wurden, oder darin, dass dies nicht sorgfältig genug geschehen ist. Trotz Bedenken in Bezug auf den Nachweis der *négligence caractérisée* sollen vor allem die besseren Strafverfolgungsmöglichkeiten für die Lösung des Art. L. 335-7-1 CPI sprechen: Die Nichteinrichtung von Sicherungsmaßnahmen ist erheblich einfacher nachzuweisen als ein Urheberrechtsverstoß.[126] Dennoch bedarf es in jedem Fall einer tatsächlichen Urheberrechtsverletzung, nicht lediglich der potentiellen Ermöglichung durch Nichtsicherung des Internetanschlusses. Insoweit ist aber die Feststellung der Urheberrechtsverletzung unverzichtbar.
Falls der bestrafte Anschlussinhaber die Internetsperre nicht respektiert und während ihrer Laufzeit einen neuen Internetprovidervertrag abschließt, setzt er sich zusätzlich einer Geldstrafe von maximal 3.750 Euro aus (Art. L. 335-7-1 Abs. 4 CPI).

(e) Bestrafung der Internetprovider

Strafrechtliche Maßnahmen gegen den Internetprovider sind aufgrund des Art. 12 der E-Commerce Richtlinie[127] eingeschränkt.[128] In Frankreich gibt es keine strafrechtlichen Sanktionen gegenüber den Internetprovidern unmittelbar wegen Urheberechtsverletzungen. Stattdessen sieht Art. L. 335-7 Abs. 6 CPI lediglich eine Bestrafung bei Verstoß gegen verhängte und dem Provider mitgeteilte Internetsperren vor: Die trotz Mitteilung nicht innerhalb von 15 Tagen vorgenommene Umsetzung der Internetsperre durch den Internetprovider kann eine Geldstrafe von maximal 5.000 Euro zu Folge haben.

(4) Regelungen mit Präventivcharakter

Durch Art. 27 des DADVSI Gesetzes wird im CPI ein neues Kapitel VI („*Prévention du téléchargement illicite*“) zur Prävention der Urheberechtsverletzungen im Internet, insbesondere durch illegales Filesharing, geschaffen.[129] Es beinhaltet zunächst zwei Artikel, Art. L. 336-1 und L. 336-2 CPI. Ziel dieser beiden Vorschriften ist, andere Personen als die Internetnutzer, welche letzteren

---

123 Vgl. *Derieux/Granchet*, Rn. 494; *Marino*, Recueil Dalloz 2010, S. 162.

124 Décision du Conseil constitutionnel n° 2009-580 DC du 10 juin 2009, Rn. 29.

125 *Pritzkow*, MR-Int 2010, S. 53.

126 *Marino*, Recueil Dalloz 2010, S. 163.

127 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“).

128 *Benabou*, S. 166.

129 *Dimeglio*.

aber die Mittel für urheberrechtlich verbotene Handlungen liefern, zu sensibilisieren und zu verpflichten.[130] Art. 9 des HADOPI 1 Gesetzes ändert den Titel dieses neuen Kapitels VI in Prävention des illegalen Filesharings und der illegalen Zurverfügungstellung urheberrechtlich oder durch ein verwandtes Schutzrecht geschützter Werke und Gegenstände („*Prévention du téléchargement et de la mise à disposition illicites d'œuvres et d'objets protégés par un droit d'auteur ou un droit voisin*“).

(a) Gerichtliche Verpflichtbarkeit des Erstellers zur Softwaremodifikation

Der seit dem DADVSI Gesetz unverändert gebliebene Art. L. 336-1 CPI bestimmt in seinem Abs. 1, dass, sobald eine Software in erster Linie für das illegale Zurverfügungstellen urheberrechtlich geschützter Werke oder Gegenstände benutzt wird, der Präsident des *tribunal de grande instance*[131] im vereinfachten und beschleunigten Verfahren einstweilig unter Androhung eines Zwangsgeldes jedwede Maßnahmen anordnen kann, die für den Schutz dieses Rechts notwendig sind und dem Stand der Technik entsprechen. Wesentliches Kriterium ist, ob die fragliche Software in erster Linie (*principalement*) so benutzt wird, weshalb auch Software erfasst sein kann, die zwar für verschiedene Anwendungen gedacht war, jedoch zum überwiegend illegalen Austausch zweckentfremdet wurde.[132] Die möglichen Maßnahmen können beispielsweise in der Implementation von Vorrichtungen bestehen, die verbotene Handlungen verhindern oder zumindest erschweren.[133] In erster Linie geht es also um technische Schutzmaßnahmen.[134] Nach Art. L. 336-1 Abs. 2 CPI dürfen die angeordneten Maßnahmen aber nicht die Veränderung der wesentlichen Merkmale oder des ursprünglichen Verwendungszwecks zum Ziel haben. Eine solche Reichweite wird als unverhältnismäßig eingestuft.[135] Einen konkreten Adressaten der Maßnahmen benennt Art. L. 336-1 CPI nicht ausdrücklich. Aus der systematischen Verortung im Kapitel zur Prävention des illegalen Filesharings, dessen zwei Vorschriften sich zum Zeitpunkt des DADVSI Gesetzes nicht an die Internetnutzer selbst richten, kann der Schluss gezogen werden, dass es sich hier um den Softwareersteller handeln muss.[136] An ihre Grenzen stößt die Regelung des Art. L. 336-1 CPI bei sog. freier Software, deren Quellcodes frei zugänglich sind und verändert werden dürfen.[137] Eine Konkretisierung des Antragsberechtigen fehlt – anders als bei Art. L. 336-2 CPI – ebenfalls. Es dürfte auf den im neuen Art. L. 336-2 CPI genannten Personenkreis abzustellen sein. Darüber hinaus erklärt Art. L. 336-1 Abs. 3 CPI den Art. L. 332-4 CPI auf die betroffenen Softwarearten für anwendbar. Demnach kann zudem die durch den Präsidenten des *tribunal de grande instance* auf Antrag angeordnete Beschlagnahme der Software nach dem in Art. L. 332-4 CPI näher beschriebenen Verfahren erfolgen.

(b) Pflichten der Internetprovider

Art. L. 336-2 CPI sieht in seiner auf dem DADVSI Gesetz beruhenden Fassung zunächst eine Pflicht der Internetprovider vor, auf eigene Kosten ihre Nutzer über die Gefahren des illegalen

---

130 *Sirinelli et al.*, *Commentaire* zu Chapitre VI vor Art. L. 336-1; ähnlich *Geiger*, Recueil Dalloz 2011, S. 776, dort Fn. 27 a.E.

131 In seiner Funktion ähnlich dem vorsitzenden Richter am Landgericht.

132 *Sirinelli et al.*, *Commentaire* zu Art. L. 336-1.

133 *Sirinelli et al.*, *Commentaire* zu Art. L. 336-1.

134 *Cédras*, RIDP Vol. 77 (2006), S. 598.

135 *Sirinelli et al.*, *Commentaire* zu Art. L. 336-1.

136 Vgl. *Sirinelli et al.*, *Commentaire* zu Chapitre VI vor Art. L. 336-1.

137 Vgl. *Cédras*, RIDP Vol. 77 (2006), S. 598 f.

Filesharings und Zurverfügungstellens für geistige Schöpfungen zu informieren, wobei die Modalitäten des Nachrichtenversands ein *décret* des *Conseil d'Etat* regeln soll.[138] Art. L. 336-2 CPI wird durch Art. 10 des HADOPI 1 Gesetzes modifiziert und regelt jetzt die gerichtliche Verpflichtbarkeit der Erbringer von Internetdienstleistungen zur Vorbeugung und Beendigung von Urheberrechtsverstößen (s.u.). Eine Pflicht der Internetprovider zur Information ihrer Kunden besteht jedoch weiterhin aufgrund und nach Maßgabe des Art. L. 331-27 CPI: Im Internetprovidervertrag müssen die Pflichten des Anschlussinhabers nach Art. L. 336-3 CPI (s.u.) und die von der HADOPI-Behörde im Falle eines Verstoßes zu erwartenden Maßnahmen klar und lesbar erwähnt werden. Ferner sind die bei Verletzung von Urheberrechten oder verwandten Schutzrechten drohenden straf- und zivilrechtlichen Sanktionen wie auch die Anwendung des Art. L. 335-7-1 CPI (Sperrung des Internetanschlusses) aufzuführen. Außerdem haben die Internetprovider ihre neuen Kunden und diejenigen, deren Vertrag fortgesetzt wird, über das legale Angebot an kulturellen Inhalten im Internet, über das Bestehen von Sicherungsmitteln, mit denen Verstöße gegen die Pflicht aus Art. L. 336-3 CPI verhindert werden können, sowie über die Gefährdung des innovativen künstlerischen Schaffens und des Wirtschaftssektors Kultur durch die Missachtung des Urheberrechts und verwandter Schutzrechte zu informieren (Art. L. 331-27 Abs. 2 CPI).

(c) Gerichtliche Verpflichtbarkeit der Internetdienstleister zur Vorbeugung und Beendigung von Urheberrechtsverstößen

Sofern es durch den Inhalt eines Internetdienstes zur Verletzung eines Urheberrechts oder eines verwandten Schutzrechts kommt, kann das den daraus entstehenden Streitfall im Eilverfahren entscheidende *tribunal de grande instance* auf Verlangen der Rechteinhaber oder derjenigen, die für diese auftreten,[139] zur Vorbeugung oder Beendigung einer solchen Verletzung gem. Art. L. 336-2 CPI jedwede geeignete Maßnahme gegenüber jedem, der zur Abhilfe beitragen kann, anordnen.

(d) Weitere Pflichten der Internetdienstleister

Nach Art. L. 336-4 CPI sind die Erbringer von Internetdienstleistungen verpflichtet, dem Nutzer in Übereinstimmung mit Art. L. 331-10 CPI und Art. L. 111-1 des französischen Verbrauchergesetzbuchs (*Code de la consommation*) die wesentlichen Merkmale der zulässigen Benutzung der von ihnen zur Verfügung gestellten geschützten Werke oder Gegenstände zur Kenntnis zu bringen.

(e) Pflichten des Internetanschlussinhabers

Ferner werden durch Art. 11 des HADOPI 1 Gesetzes die neuen Art. L. 336-3 und L. 336-4 CPI geschaffen. Durch das HADOPI 1 Gesetz kommt es zwar zur Aufhebung des Art. L. 334-12 CPI in seiner Fassung nach dem DADVSI Gesetz, allerdings wird die Grundidee im neuen Art. L. 336-3 CPI wieder aufgegriffen.[140] Demnach hat der Anschlussinhabers – soweit erforderlich – die Pflicht darauf zu achten, dass sein Anschluss nicht zu Zwecken der Vervielfältigung, Darbietung, Zurverfügungstellung oder öffentlicher Wiedergabe urheberrechtlich oder durch ein verwandtes Schutzrecht nach den Büchern I und II des CPI geschützter Werke oder Gegenstände ohne Ermächtigung durch die Rechteinhaber benutzt wird. Art. L. 336-3 CPI beinhaltet kein direktes Verbot an den Anschlussinhabern den Internetanschluss für die beschriebenen Zwecke zu nutzen, sondern eine allgemein Pflicht zur Überwachung der Verbindung um sicherzustellen, dass

---

138 *Cédras*, RIDP Vol. 77 (2006), S. 596; *Dimeglio*.

139 Konkretisiert in Art. L. 321-1 und L. 331-1 CPI.

140 *Benabou*, S. 177.

diese nicht für Urheberrechtsverletzungen benutzt wird.[141] Um seine – für Art. L. 336-3 Abs. 1 CPI verneinte[142] – Verfassungskonformität zu gewährleisten, wird Art. L. 336-3 CPI durch Art. 10 des HADOPI 2 Gesetzes um einen Abs. 2 ergänzt. Demzufolge zieht die Verletzung der Pflicht aus Abs. 1 vorbehaltlich der Art. L. 335-7 und L. 335-7-1 CPI keine (weitere) strafrechtliche Verantwortlichkeit nach sich. Allerdings richtet sich die in Hinblick auf die Art. L. 335-7 und L. 335-7-1 CPI geäußerte Kritik (s.o.) auch gegen Art. L. 336-3 CPI.

2. Ausrichtungen und Gegenstände der relevanten Verwaltungsbehörden

a. Verbraucherschutz durch die öffentliche Verwaltung im Allgemeinen

Verbraucherschutz findet in Frankreich auch durch Verwaltungsbehörden statt. Anders als in Deutschland erfolgt der Verbraucherschutz in Frankreich jedoch nicht mit Ausnahme einiger Sonderbereiche durch die allgemeinen Verwaltungsbehörden. Vielmehr gibt es auf dem Gebiet des Verbraucherrechts Sonderbehörden. Zu erwähnen ist insbesondere die *Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes* (dgccrf). Hier handelt es sich jedoch keineswegs um eine reine Verbraucherschutzbehörde. Bereits die Bezeichnung der Behörde weist darauf hin, dass neben Verbraucherangelegenheiten auch die Wettbewerbsüberwachung und Betrugsbekämpfung umfasst sind.

b. Organisation des verwaltungsrechtlichen Datenschutzes in Frankreich

Für den verwaltungsrechtlichen Datenschutz wurde durch das loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (LIFL) mit der *Commission nationale de l'informatique et des libertés* (CNIL) eine eigene, unabhängige Sonderbehörde geschaffen. Aufgrund ihrer sehr frühen Implementierung kommt dem französischen Datenschutzbehörde eine Vorreiterrolle zu. Sie ist von vornherein auf die Durchsetzung des französischen Datenschutzgesetztes ausgerichtet. Dabei wird sie aber nicht nur repressiv, sondern auch präventiv tätig.

c. Behördlicher Schutz des Urheberrechts

In Frankreich wurde – im Rahmen einer Reihe von seit 2006 verfolgten Gesetzgebungsprojekten – neben der Einführung neuer Repressions- und Präventionsregelungen eine staatliche Sonderbehörde eingerichtet, die Hohe Autorität für die Verbreitung von Werken und den Schutz von Rechten im Internet (*Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* – HADOPI).[143] Die neugeschaffene HADOPI-Behörde soll Urheberrechtsverstößen zunächst vorbeugen, aber auch bei ihrer strafrechtlichen Verfolgung mitwirken. Gegenüber den Inhabern von Internetanschlüssen, die aufgrund der dokumentierten IP-Adressen mit illegalem Filesharing in Verbindung gebracht werden, reagiert die HADOPI-Behörde mit dem dreistufigen Verfahren der *réponse graduée*. Auf elektronischem Wege spricht sie gegebenenfalls eine erste Empfehlung aus, mit der der Anschlussinhaber zur Ordnung gerufen und vor den Folgen weiterer Verstöße gewarnt werden soll. In der Regel dürfte der Großteil der Betroffenen bereits wegen

---

141 *Benabou*, S. 177.

142 Décision du Conseil constitutionnel n° 2009-580 DC du 10 juin 2009.

143 Internetauftritt unter <www.hadopi.fr>.

dieser Warnhinweise das Filesharing einstellen[144] bzw. ihren Zugang besser sichern.[145] Daher ist in den wenigsten Fällen tatsächlich eine Sperrung des Internetanschlusses zu erwarten.

d. Beurteilung der Möglichkeit behördlichen Eingreifens zum Schutz vor übermäßiger Urheberrechtsdurchsetzung

Anders als in Deutschland kann der Verletze bzw. sein Anwalt in Frankreich im Fall einer Verletzung Geistigen Eigentums durch illegales Filesharing nicht im Wege einer Abmahnung ähnlich der nach § 97a UrhG gegen den Verletzer vorgehen. Eine mit § 97a UrhG vergleichbare Vorschrift findet sich im französischen Recht nämlich nicht. Vielmehr obliegt die Urheberrechtsdurchsetzung in erster Linie der HADOPI-Behörde selbst.

3. Für den verwaltungsrechtlichen Datenschutz zu behandelnden Sachfragen

a. Grundverständnis der betreffenden Behörde

Bei der CNIL handelt es sich nicht nur um eine vergleichsweise früh eingerichtete Datenschutzbehörde, sondern als Besonderheit kommt hinzu, dass es sich hier um die erste unabhängige Regulierungsbehörde (*autorité administrative indépendante* – AAI) in Frankreich handelt. Inzwischen darf die CNIL als in Frankreich äußerst respektiert, gar als „moralische Autorität" bezeichnet werden.[146] Auch aus dieser ursprünglichen Sonderrolle ergibt sich die besondere Stellung der CNIL. Betont wird die Unabhängigkeit der CNIL ausdrücklich in Art. 11 LIFL: „*La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante.*" Die CNIL ist gem. Art. 19 LIFL direkt dem französischen Präsidenten unterstellt; ihre Bediensteten werden durch ihn ernannt. Auch Art. 21 LIFL bekräftigt die Weisungsunabhängigkeit der Mitglieder der LIFL: "*Dans l'exercice de leurs attributions, les membres de la commission ne reçoivent d'instruction d'aucune autorité.*" Die für eine unabhängige Tätigkeit notwendige Mittelausstattung wird durch Art. 12 LIFL garantiert, welcher das loi du 10 août 1922 für nicht anwendbar erklärt und die Haushaltsführung der CNIL direkt der Kontrolle des obersten Rechnungshofes (*Cour des comptes*) unterstellt. Allerdings hat die CNIL dem französischen Präsidenten, Premierminister und Parlament jährlich einen Bericht zu präsentieren, in dem sie über die Ausübung und Erfüllung ihrer Aufgaben Rechenschaft ablegt (Art. 11 LIFL a.E.).

Zwar kommt Fragen des Datenschutzrechts in Bezug auf den Schutz personenbezogener Daten natürlicher Personen zwangsläufig eine hohe Verbraucherrelevanz zu, die CNIL selbst versteht sich jedoch nicht als Verbraucherschutzbehörde im engeren Sinne. Die Durchsetzung der Vorschriften des französischen Datenschutzgesetzes durch Kontrolle der Einhaltung der Vorgaben des LIFL und der Möglichkeit ggf. Sanktionen zu verhängen, macht einen wesentlichen Teil des Tätigkeitsspektrums der CNIL aus. Zudem läuft das Anzeige- bzw. Genehmigungsverfahren über die CNIL. Daneben wird die Behörde allerdings auch präventiv tätig, indem sie nicht nur die von einer Datenverarbeitung Betroffenen, sondern auch die verantwortlichen Stellen über ihre jeweiligen Rechte und Pflichten informiert.

---

144 *Spies*, MMR 2009, S. 438.

145 *Pritzkow*, MR-Int 2010, S. 54.

146 *Le Friant*, RdA 2003, 33 (40).

b. Behördenstruktur und Ausgestaltung der Zuständigkeiten

aa) Zusammensetzung und Organisationsstruktur

Nach Art. 13 LIFL besteht die CNIL aus 17 Mitgliedern: Zwei Parlamentsabgeordnete und zwei Senatoren gehören dazu, die jeweils durch das Parlament bzw. den Senat auf eine die pluralistische Repräsentation gewährleistenden Art und Weise benannt werden. Zwei Mitglieder werden vom Rat für Wirtschaft, Soziales und Umwelt (*Conseil économique, social et environnemental*) aus dessen Reihen gewählt. Hinzu kommen zwei aktuelle oder ehemalige Mitglieder des obersten französischen Verfassungsrats (*Conseil d'Etat*), die durch dessen Generalversammlung gewählt werden. Auf gleiche Weise werden auch jeweils zwei aktuelle oder ehemalige Mitglieder des französischen Kassationsgerichts (*Cour de cassation*) und des Rechnungshofs (*Cour des comptes*) zu Mitgliedern der CNIL bestimmt. Außerdem werden drei aufgrund ihrer Kenntnisse der elektronischen Datenverarbeitung oder der individuellen Freiheitsrechte betreffenden Fragestellungen als besonders qualifiziert erachtete Persönlichkeiten per Dekret zu Mitgliedern der CNIL ernannt. Bei den letzten beiden Mitgliedern handelt es sich ebenfalls um aufgrund ihrer Kenntnisse der elektronischen Datenverarbeitung als besonderes qualifiziert erachtete Persönlichkeiten, allerdings werden diese durch den Parlamentspräsidenten und den Senatspräsidenten benannt. Mit lediglich beratender Funktion gehören zur CNIL des Weiteren der *Défenseur des droits* (eine Art Grundrechtemahner) oder sein Vertreter. Die Funktion als Mitglied der CNIL besteht für fünf Jahre und kann einmal verlängert werden. Sie ist gem. Art. 14 inkompatibel mit bestimmten anderen Funktionen und Tätigkeiten. Mitglieder der CNIL dürfen insbesondere nicht zugleich Regierungsmitglieder sein. Auch anderweitige Interessenkollisionen sollen weitmöglichst ausgeschlossen sein. Darüber hinaus bestehen diesbezügliche Mitteilungspflichten der Mitglieder gegenüber dem Präsidenten der CNIL, die allen anderen Mitgliedern zugänglich gemacht werden müssen.

Aus den Reihen der Mitglieder werden für eine Dauer von fünf Jahren ein Präsident und zwei Vizepräsidenten gewählt, sie bilden eine Art Geschäftsstelle bzw. Generalsekretariat (*bureau*). Die Funktion des Präsidenten ist inkompatibel mit jeglicher anderen beruflichen Tätigkeit oder öffentlichem Anstellungsverhältnis und jeder direkten oder indirekten Interessensbindung gegenüber einem Unternehmen des Sektors der elektronischen Dienstleistungen oder der Datenverarbeitung.

Die Versammlung der Mitglieder der CNIL erfolgt gem. Art. 15 LIFL grundsätzlich in Vollversammlung (*formation plénière*), es sei denn, es bestehen Zuständigkeiten des Sekretariats (*bureau*) oder der Teilversammlung (*formation restreinte*). Letztere setzt sich gem. Art. 13 Abs. 1 LIFL a.E. aus einem Präsidenten und fünf weiteren, aus den Mitgliedern der CNIL aus sich selbst heraus gewählten Mitgliedern, die aber nicht zugleich Mitglieder des Sekretariats sein dürfen, zusammen. Sie ist es auch, die nach Art. 17 LIFL für die Verhängung der in Kapitel VII vorgesehenen Sanktion gegenüber gegen die Vorgaben des LIFL verstoßenden verantwortlichen datenverarbeitenden Stellen zuständig ist.

Die Vollversammlung kann den Präsidenten oder seinen beauftragten Vertreter mit der Ausübung einzelner, in Art. 15 LIFL aufgelistete Zuständigkeiten betrauen. Andere Zuständigkeiten können nach Art. 16 LIFL dem Sekretariat übertragen werden.

bb) Aufgaben

Die Aufgaben (*missions*) der CNIL ergeben sich aus Art. 11 LIFL und lassen sich in vier Bereichsgruppen unterscheiden. Erstens obliegt ihr die Information jeglicher Betroffenen und jeglicher verantwortlichen Stellen über ihre jeweiligen Rechte und Pflichten.

Zweitens hat sie darauf zu achten, dass die Verarbeitung personenbezogener Daten in Einklang mit den Vorgaben des LIFL erfolgt. Das geschieht u.a. durch die Ausübung ihrer Funktionen im Rahmen des Anzeige- bzw. Genehmigungsverfahrens (Art. 11 Nr. 2 lit. a und b LIFL). Die CNIL bearbeitet zudem Beanstandungen (*réclamations*), Eingaben (*pétitions*) und Anzeigen (*plaintes*) in Hinblick auf die Durchführung der Datenverarbeitung (Art. 11 Nr. 2 lit. c LIFL) sowie aber auch Stellungnahmegesuche öffentlicher Stellen (*pouvoirs publics*) oder Gerichte (*juridictions*) und berät Personen oder Stellen, die eine automatische Verarbeitung personenbezogener Daten umsetzen oder dies beabsichtigen (Art. 11 Nr. 2 lit. d LIFL). Gerade im Bereich kommerzieller Werbung und der Ausübung des Rechts, sich nach Art. 38 LIFL der Datenverarbeitung zu widersetzen bzw. ihr zu widersprechen, gingen bei der CNIL in der Vergangenheit eine beträchtliche Anzahl an Beschwerden ein.[147] Aber auch Beschwerden über Google geben Anlass zur Tätigkeit der CNIL.[148] Außerdem informiert die CNIL unverzüglich nach Art. 40 des französischen Strafprozessgesetzbuchs, dem *Code de procédure pénal*, die Staatsanwaltschaft, wenn sie von Gesetzesverstößen Kenntnis erlangt hat, und kann Beobachtungen unter den in Art. 52 LIFL vorgesehenen Bedingungen bei Strafverfahren darlegen (Art. 11 Nr. 2 lit. e LIFL). Des Weiteren kann die CNIL eines oder mehrere ihrer Mitglieder oder den Generalsekretär damit beauftragen, die Überprüfung jeglicher Datenverarbeitung vorzunehmen oder durch Bedienstete vorzunehmen lassen und ggf. alle Dokumente und Unterlagen zu erlangen, die für die Wahrnehmung ihrer Aufgaben von Nutzen sind (Art. 11 Nr. 2 lit. f LIFL). Schließlich erstreckt sich die Aufgabe der CNIL, auf die Einhaltung der Vorgaben des LIFL zu achten, auch auf die Bearbeitung der Zugangsgesuche im Falle eines lediglich indirekten Zugangsrechts der Betroffenen bei besonderen Arten der Datenverarbeitung (Art. 11 Nr. 2 lit. h LIFL).[149]

Drittens zählt zu den Aufgaben der CNIL die Behandlung bestimmter Gesuche von Berufsorganisationen oder anderweitigen Zusammenschlüssen der verantwortlichen Stellen. So begutachtet die französische Datenschutzbehörde auf ihre Übereinstimmung mit den Vorgaben des LIFL hin ihr unterbreitete Berufsregeln, Produkte und Verfahren zum Schutz der Betroffenen bei Verarbeitung personenbezogener Daten oder zur Anonymisierung dieser Daten (Art. 11 Nr. 3 lit. a LIFL). Die CNIL gibt auch betreffend die Beachtung der Grundrechte Beurteilungen der durch die von ihr vorher als datenschutzrechtskonform erklärten Berufsregeln gebotenen Garantien ab (Art. 11 Nr. 3 lit. b LIFL). Darüber hinaus erteilt die CNIL ein Gütesiegel für den Schutz der Betroffenen bei Verarbeitung personenbezogener Daten anstrebende Produkte und Verfahren, nachdem sie diese vorher für mit dem französischen Datenschutzrecht konform erklärt hat (Art. 11 Nr. 3 lit. c LIFL). Für die Beurteilung können auch externe, unabhängige Personen herangezogen werden. Entstehende Kosten sind von dem das Gütesiegel beantragendem Unternehmen zu tragen.

Viertens ist es auch Aufgabe der CNIL, über die Entwicklung der Informationstechnologien informiert zu bleiben und ggf. ihre Einschätzung der sich daraus für die Ausübung der in Art. 1 LIFL erwähnten(Freiheits-)Rechte ergebenden Konsequenzen zu veröffentlichen. Dies umfasst die verpflichtende Konsultierung der CNIL bei jedem den Schutz der Betroffenen bei automatisierter Datenverarbeitung betreffendem Gesetzgebungsprojekt (Art. 11 Nr. 4 lit. a LIFL). Die CNIL macht der Regierung Gesetzgebungsvorschläge zur Anpassung des Schutzes der Freiheitsrechte an die Entwicklung der Informationsverfahren und –techniken (Art. 11 Nr. 4 lit. b LIFL). Daneben kann

147 *Vulliet-Tavernier*, Droit social 2004, 1055 (1058).

148 Hierzu *Mattatia*, RSC 2009, 317 (318 f.) sowie MMR-Aktuell 2010, 304953; ZD-Aktuell 2012, 02791; ZD-Aktuell 2013, 03465

149 Ausführlicher oben.

die CNIL auf Gesuch anderer unabhängiger Verwaltungsbehörden einen Beitrag zum Datenschutz leisten (*apporter son concours en matière de protection des données*) (Art. 11 Nr. 4 lit. c LIFL). Die CNIL kann des Weiteren auf Gesuch des *Premier ministre* bei internationalen Verhandlungen im Bereich des Schutzes personenbezogener Daten an der Vorbereitung und Festlegung der französischen Position beteiligt werden und bei der französischen Vertretung in auf diesem Gebiet federführenden internationalen und europäischen Organisationen mitwirken (Art. 11 Nr. 4 lit. d LIFL).

c. Befugnisse der Datenschutzbehörde

Einige Befugnisse der CNIL werden bereits im Zusammenhang mit den ihr obliegenden Aufgaben in der diese aufführenden Liste des Art. 11 LIFL mitgeregelt.[150] Dazu zählen beispielsweise die Befugnis zur Überprüfung von Datenverarbeitungsvorgängen und zur Erlangung aller zur Wahrnehmung der Aufgaben der CNIL nützlichen Dokumente und Unterlagen oder die Heranziehung externer, unabhängiger Sachverständiger. Darüber hinaus bekräftigt Art. 11 LIFL a.E., dass die CNIL zur Erfüllung ihrer Aufgaben jegliche Art von Empfehlung aussprechen und sowohl Einzelentscheidungen als auch Entscheidungen allgemeinverfügenden Charakters (*décisions individuelles ou réglementaires*) in den im LIFL vorgesehenen Fällen treffen kann.

Weitere Befugnisse finden sich in einem eigenständigen Kapitel VI des LIFL über Kontrolle der Datenverarbeitungsumsetzung.[151] Hierbei ergeben sich bei vorheriger Information des zuständigen Staatsanwalts gem. Art. 44 Abs. 1 LIFL für die Zeit zwischen 6 und 21 Uhr Zugangsrechte der CNIL zu allen Örtlichkeiten, Räumlichkeiten, Anlagen, Niederlassungen und Einrichtungen (*lieux, locaux, enceintes, installations ou établissements*), die der Durchführung der Verarbeitung personenbezogener Daten dienen und im gewerblichen bzw. beruflichen Gebrauch stehen, ausgenommen den als private Wohnstätte bestimmten Teilen. Dem Inhaber der Räumlichkeiten steht grundsätzlich ein Widerspruchsrecht zu, über das er zu informieren ist. Macht er von seinem Widerspruchsrecht Gebrauch, sind die Zugangsrechte der CNIL von einer richterlichen Erlaubnis abhängig. Ausnahmen sind vorgesehen im Falle besonderer Dringlichkeit oder Schwere der zu Last gelegten datenschutzrelevanten Verstöße sowie bei Gefahr der Zerstörung oder Verdunkelung von Dokumenten. Es können gem. Art. 44 Abs. 3 LIFL auch die Übermittlung aller zur Erfüllung der Kontrollaufgaben der CNIL notwendigen Dokumente verlangt werden sowie der Erhalt jeglicher Information, Belege und Zugangsrechte zu allen Informationsverarbeitungsprogrammen und Daten etc. Bei Bedarf dürfen externe Sachverständige hinzugezogen werden. Insbesondere medizinische Daten können nur durch einen Mediziner angefordert werden. Beschränkungen der Kontrollbefugnisse der CNIL bestehen darüber hinaus nur in bestimmten, die Staatsicherheit betreffenden Fällen.

Außerdem finden sich Befugnisse der CNIL in diversen Einzelvorschriften. U.a. enthält Art. 8 Abs. 3 LIFL die Befugnis der CNIL unter Berücksichtigung des Zwecks der Datenverarbeitung für den Fall eines kurzfristig vorzunehmenden Anonymisierungsverfahrens eine Genehmigung einzelner Arten der eigentlich nach Art. 9 Abs. 1 LIFL untersagten Verarbeitung der dort genannten personenbezogenen Daten zu erteilen. Nach Art. 21 Abs. 3 kann die CNIL bei Gesetzesverstößen dem Datenschutzbeauftragten die bei dessen Einrichtung eigentlichen entfallende Anzeigepflicht auferlegen.

---

150 Im Einzelnen s.o.

151 Ausführlicher zu den Grenzen der Kontrollbefugnisse der CNIL bei lediglich anzeigepflichtigen Datenverarbeitungsvorgängen *Combrexelle*, Les limites du contrôte de la Commission nationale de l'informatique et des libertés dans le régime de la déclaration, RFD adm. 13, 551.

Hinzu kommen Befugnisse im Rahmen des Anzeige- bzw. Genehmigungsverfahrens.
Die CNIL hat schließlich auch die Möglichkeit zur Verhängung von Sanktionen bei Nichteinhaltung der Vorgaben des französischen Datenschutzgesetzes.

d. Sanktionsmöglichkeiten

Die Sanktionsmöglichkeiten der CNIL sind überwiegend in einem eigenen Kapitel VII geregelt.[152] Zuständig für die Verhängung der dort vorgesehenen Sanktionen ist die Teilversammlung (*formation restreinte*)[153] der Mitglieder der CNIL.
Nach Einräumung der Möglichkeit zur Beibringung einer Gegendarstellung kann die CNIL gem. Art. 44 Abs. 1 LIFL im Falle einer Missachtung der sich aus dem LIFL ergebenden Pflichten durch eine verantwortliche Stelle dieser eine Verwarnung erteilen. Dieser Verwarnung wird gesetzlich ausdrücklich Sanktionscharakter zugeschrieben („*Cet avertissement a le caractère d'une sanction.*"). Die CNIL kann die verantwortliche Stelle zudem auffordern, die festgestellte Pflichtverletzung innerhalb einer vorgegebenen Frist einzustellen. Bei Dringlichkeit kann die Frist auf fünf Tage begrenzt sein. Wenn die für die Datenverarbeitung verantwortliche Stelle der Aufforderung nachkommt, erklärt der Präsident der CNIL den Abschluss des Verfahrens. Andernfalls kann die Teilversammlung nach erneuter Anhörung Sanktionen aussprechen: Sie kann gem. Art. 44 Abs. 1 Nr. 1 LIFL (außer in den Fällen, in denen die Datenverarbeitung durch den Staat erfolgt) eine Geldstrafe erteilen oder gem. Art. 44 Abs. 1 Nr. 2 LIFL die Anordnung zur Einstellung der Datenverarbeitung erteilen, sofern diese unter die bloße Anzeigepflicht nach Art. 22 LIFL fällt, oder die unter Anwendung des Art. 25 erteilte Genehmigung zurückziehen. Nach Art. 47 LIFL ist die Geldstrafe an der Schwere des Verstoßes und den daraus gezogenen Vorteile auszurichten. Bei erstmaligem Verstoß dürfen 150.000 Euro nicht überschritten werden, im Wiederholungsfall in den fünf darauffolgenden Jahren dürfen 300.000 Euro bzw. bei Unternehmen fünf Prozent des Umsatzes nach Steuern, jedoch maximal ebenfalls 300.000 Euro nicht überschritten werden. Diese Geldbuße ist jedoch auf eine durch den Strafrichter aufgrund gleicher Tatsachen oder zusammenhängender Tatsachen verhängte Geldstrafe anrechenbar. Verhängt wurde beispielsweise eine solche Geldbuße der CNIL i.H.v. 100.000 Euro gegenüber Google wegen unredlicher Datenerhebung.[154]
Führt die Datenverarbeitung oder die Auswertung der verarbeiteten Daten jedoch zu einer Verletzung der in Art. 1 LIFL genannten Rechte und Freiheitsrechte, so kann nach Einräumung der Möglichkeit zur Gegendarstellung ein Eilverfahren eingeleitet werden um über eine Unterbrechung der Datenverarbeitung für eine Dauer von maximal drei Monaten zu entscheiden (Art. 45 Abs. 2 Nr. 1 LIFL), die oben genannte Verwarnung auszusprechen (Nr. 2), über eine Sperrung einiger verarbeiteter personenbezogener Daten für eine Dauer von ebenfalls maximal drei Monaten zu entscheiden (Nr. 3) und/oder den Premierminister zu informieren, damit er die zur Einstellung der festgestellten Verletzung notwendigen Maßnahmen trifft (Nr. 4).
Im Falle einer schwerwiegenden und gegenwärtigen Beeinträchtigung der in Art. 1 LIFL genannten Rechte und Freiheitsrechte kann der Präsident der CNIL im Wege eines gerichtlichen Eilverfahrens die Anordnung jeglicher zum Schutz dieser Rechte notwendigen Sicherheitsmaßnahmen, ggf. unter Zwang, beantragen.

---

[152] Zu den Entwicklungen im Bereich der Sanktionsmöglichkeiten der CNIL aufgrund der Umsetzung der Datenschutzrichtlinie *Forest*, Pouvoirs de sanction de la CNIL : le réveil soudain de la belle endormie, D. 2007, 94.

[153] Näheres zur Teilversammlung (*formation restreinte*) s.o.

[154] Délibération n°2011-035, 17 mars 2011. Abrufbar unter http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/D2011-035.pdf .

Gem. Art. 46 hat die CNIL zudem die Möglichkeit, verhängte Sanktionen zu veröffentlichen.
Betrachtet man die durch die CNIL verhängbaren Geldbußen als Bußgeld für Verstöße mit Ordnungswidrigkeitencharakter, lassen die Vorschriften des LIFL erkennen, dass die CNIL selbst keine strafrechtlichen Sanktionen verhängen kann. Ein Strafverfahren kann sie nur dadurch forcieren, indem sie dem Staatsanwalt ihr bekannt gewordene strafrechtlich relevante Verstöße mitteilt und eigene Beobachtungen dann im Strafverfahren darlegt, vgl. Art. 11 Nr. 2 lit. e LIFL.[155] Unterschieden werden müssen demnach behördliche Sanktionen der CNIL einerseits und strafrechtliche Sanktionen durch die klassischen Strafverfolgungsbehörden wie sie zum Teil im LIFL selbst, aber auch im Code pénal vorgesehen sind.

e. Spielräume für eigene Politik

Nicht nur im Rahmen ihrer Stellungnahmen[156], vielfältigen präventiven Aufklärungsarbeit und Informationstätigkeit sowie in ihrem jährlichen Bericht hat die CNIL Spielräume für eigene Politik. Eben auch bei der thematischen Auswahlfreiheit macht sich auch die Ausgestaltung der CNIL als keinen Weisungen unterliegende unabhängige Sonderbehörde bemerkbar. Ihren Aufgaben nach Art. 11 LIFL muss sie allerdings verpflichtend nachkommen. Beispielsweise muss sie auf Beanstandungen (*réclamations*), Eingaben (*pétitions*) und Anzeigen (*plaintes*) in Hinblick auf die Durchführung der Datenverarbeitung reagieren und deren Verfasser über daraus entstandenen Konsequenzen informieren. Die Verleihung von Gütesiegel an datenverarbeitende Stellen spielt in diesem Kontext ebenfalls eine Rolle. Zu erwähnen sind darüber hinaus die Möglichkeit Entscheidungen allgemeinverfügenden Charakters zu treffen sowie Gesetzesänderungen zu initiieren und bei Gesetzesprojekten gehört bzw. konsultiert zu werden.

f. Besonderheiten bei grenzüberschreitender Durchsetzung

Maßgeblich für die Anwendbarkeit französischen Rechts und damit des LIFL ist nach Art. 5 LIFL zunächst die Niederlassung der verantwortlichen Stelle auf dem französischen Staatsgebiet.[157] Jedoch kann die CNIL von ihren Kontrollbefugnissen nach Art. 44 LIFL und überwiegend auch von ihren Sanktionsmöglichkeiten nach Art. 45 LIFL auch dann Gebrauch machen, wenn die verantwortliche Stelle zwar keine Niederlassung auf französischen Staatsgebiet hat, die Datenverarbeitung aber – ganz oder teilweise – auf französischen Staatsgebiet erfolgt.
Für die Übertragung personenbezogener Daten in Staaten außerhalb der Europäischen Union enthält das LIFL daneben einige Sondervorschriften.[158] Insbesondere ist die Übertragung bei fehlendem ausreichenden Schutzniveau gem. Art. 68 LIFL untersagt bzw. nur in Ausnahmefällen möglich. Eine wichtige Ausnahme stellt das Vorliegen einer Erlaubnis der CNIL dar. Dies muss dann jedoch durch die CNIL der Europäischen Kommission sowie den Kontrollbehörden der anderen Mitgliedstaaten zu Kenntnis gebracht werden.
Des Weiteren kann die CNIL gem. Art. 49 LIFL auch auf Gesuch einer anderen, ausländischen (Datenschutz-)Behörde eines anderen EU-Mitgliedstaats mit analog ausgestalteten Kompetenzen kontrollierend und sanktionieren tätig werden bzw. mit dieser anderen Behörde Informationen austauschen.

---

155 S.o.

156 Zur Pflicht der CNIL, Stellungnahmen über Gesetzgebungsprojekte in Vollversammlung zu verabschieden näher *Pastor*, La CNIL doit statuer en formation plénière pour émettre un avis sur les projets de décrets, AJDA 2007, 1438.

157 Ausführlicher s.o.

158 Ausführlicher s.o.

4. Für den behördlichen Schutz des Urheberrechts zu behandelnden Sachfragen

a. Grundverständnis der Behörde

Der CPI enthält, vor den Kapiteln V und VI zu den repressiven und präventiven Maßnahmen, im Kapitel I („*Dispositions générales*“) allgemeine Bestimmungen, darunter auch die Vorschriften des Abschnitts III über die *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* (HADOPI-Behörde). Diese ist eine durch die HADOPI 1 und 2 Gesetze geschaffene, unabhängige Sonderbehörde, der wichtige Funktionen bei der Bekämpfung von Urheberrechtsverstößen im Internet, insbesondere durch illegales Filesharing, zukommen.[159] Die HADOPI-Behörde übernimmt zugleich die Aufgaben der früheren Behörde zur Regulation technischer Maßnahmen (*Autorité de régulation des mesures techniques* – ARMT) und ersetzt diese.[160]
Die HADOPI-Behörde ist gem. Art. L. 331-12 CPI eine unabhängige staatliche Behörde und aus diesem Grund als juristische Person mit eigener Rechtspersönlichkeit ausgestattet.

b. Behördenstruktur und Ausgestaltung der Zuständigkeiten

aa) Zusammensetzung und Organisationsstruktur

Nach Art. L. 331-15 CPI setzt sich die HADOPI-Behörde aus einem Kollegium („*collège*“) und einer Kommission („*commission de protection des droits*“) zusammen. Der Präsident des Kollegiums ist zugleich auch der Präsident der HADOPI-Behörde selbst. Die HADOPI-Behörde verfügt darüber hinaus über einen eigenen Beamtenapparat. Details zu Organisationstruktur, Personal, Budget, etc. werden durch die Art. L. 331-19 bis L. 331-22 und die Art. R. 331-2 ff. CPI geregelt.
Einschließlich des Präsidenten besteht das Kollegium aus neun Mitgliedern, die für die Dauer von sechs Jahren per Dekret benannt werden, Art. L. 331-16 CPI. Ein Mitglied wird vom Vizepräsidenten des die Regierung beratenden obersten französischen Verwaltungsgerichts (*Conseil d'État*) aus dessen Geschäftsbereich benannt, eines vom ersten Präsidenten des mit dem BGH vergleichbaren französischen Kassationsgerichtshofs (*Cour de cassation*) aus dessen Geschäftsbereich und eines vom ersten Präsidenten des französischen Rechnungshofs (*Cour des comptes*) aus dessen Geschäftsbereich. Durch das Kollegium wird eines dieser drei Mitglieder zum Präsidenten gewählt. Hinzu kommen ein Mitglied aus dem übergeordneten Rat für das Eigentum an literarischen und künstlerischen Werken (*Conseil supérieur de la propriété littéraire et artistique*), das von dessen Präsident benannt wird, drei qualifizierte Persönlichkeiten auf gemeinsamen Vorschlag der für elektronische Kommunikation, Verbraucherangelegenheiten und Kultur zuständigen Minister, und schließlich noch zwei je durch den Präsidenten des französischen Parlaments (*Assemblée nationale*) und den Präsidenten des französischen Senats (*Sénat*) benannte qualifizierte Persönlichkeiten.
Die Kommission besteht – wiederum einschließlich ihres Präsidenten – aus drei Mitgliedern, die ebenfalls für die Dauer von sechs Jahren per Dekret benannt werden, Art. L. 331-17 CPI. Tauglichkeit und Benennungsmodalitäten entsprechen denen für die ersten drei Kandidaten des Kollegiums, jedoch sind die Ämter nicht kompatibel. Überhaupt bestehen nach Art. L. 331-18 CPI gewisse Inkompatibilitäten nicht nur während der Funktion als Mitglied der HADOPI-Behörde, sondern auch für die drei dieser Funktion vorausgehenden Jahre als auch nach Beendigung der Zugehörigkeit.

---

159 *Geiger* , Recueil Dalloz 2011, S. 776; *Sirinelli et al.*, *Commentaire* zu Section III vor Art. L. 331-12.

160 Vgl. *Kerr-Vignale*, RIPIA 2010, S. 74; *Marino*, Recueil Dalloz 2010, S. 163.

bb) Aufgaben

Zur Aufgabe hat die HADOPI-Behörde nicht nur den Schutz der dem Urheber- oder einem verwandten Schutzrecht unterfallenden Werke und Gegenstände vor Beeinträchtigungen in zur Erbringung von öffentlich zugänglichen Internetdiensten benutzten elektronischen Kommunikationsnetz(werk)en (Art. L. 331-13 Abs. 1 Nr. 2 CPI). Dabei bedient sich die Behörde der in Art. L. 331-24 bis L. 331-30 CPI beschriebenen Verfahren und Mittel – unter anderem der *réponse graduée*. Zu den Aufgaben der HADOPI-Behörde gehören zudem die Förderung legaler Angebote und die Beobachtung des rechtmäßigen und unrechtmäßigen Gebrauchs besagter geschützter Werke und Gegenstände in zur Erbringung von öffentlich zugänglichen Internetdiensten benutzten elektronischen Kommunikationsnetz(werk)en (Art. L. 331-13 Abs. 1 Nr. 1 CPI). Wie dies im Einzelnen geschieht, wird in Art. L. 331-23 CPI geregelt. Der HADOPI-Behörde kommt darüber hinaus eine Regulierungs- und Überwachungsaufgabe im Bereich der technischen Maßnahmen zum Schutz und zur Identifikation der durch Urheberrecht oder ein verwandtes Schutzrecht geschützten Werke und Gegenstände zu (Art. L. 331-13 Abs. 1 Nr. 3 CPI). Hierfür enthalten die Art. L. 331-1 bis L. 331-37 konkretere Vorgaben. Neben ihrer Rolle im Verfahren der *réponse graduée* kommen der HADOPI-Behörde in Hinblick auf das illegale Filesharing mithin insbesondere Präventivfunktionen zu.[161]

c. Befugnisse und Verfahrensweisen

aa) Kompetenzausübung im Allgemeinen

Nach Art. L. 331-13 Abs. 2 CPI kann die HADOPI-Behörde – neben der Vornahme bestimmter Maßnahmen zur Ausübung ihrer Aufgaben – jegliche Gesetzes- oder Verordnungsmodifikation empfehlen. In ihrem Aufgabenbereich empfangen weder das Kollegium noch die Rechteschutzkommission Weisungen irgendeiner anderen Behörde, Art. L. 331-15 Abs. 2 CPI.

Soweit in anderen Vorschriften nichts Gegenteiliges bestimmt ist, werden gem. Art. L. 331-15 CPI die Aufgaben der HADOPI-Behörde grundsätzlich durch das Kollegium wahrgenommen. Für das Verfahren der *réponse graduée* nach Art. L. 331-25 CPI bei Verletzung der Pflicht aus Art. L. 336-3 CPI durch den Internetanschlussinhaber ist allerdings gem. Art. L. 331-17 Abs. 1 CPI ausdrücklich die Kommission zuständig.

bb) Verfahren der réponse graduée[162]

Im Rahmen des Verfahrens der *réponse graduée* wird die Kommission nicht auf eigene Initiative tätig.[163] Ersucht werden kann sie entweder durch vereidigte und zugelassene Bevollmächtigte der ordnungsgemäß gebildeten beruflichen Schutzorganisationen (*organismes de défense professionnelle régulièrement constitués*), der Gesellschaften für Wahrnehmung und Verteilung von Rechten (*sociétés de perception et de répartition des droits*) oder des nationalen Filmkunstzentrums (*Centre national de la cinématographie*).[164] Vertreten werden die Rechteinhaber in Frankreich beispielsweise durch die SPPF (*Société civile des Producteurs de Phonographe en France*) und das SNEP (*Syndicat National de l'Édition Phonographique*), die nach Verteilung der Rechte

---

161 Vgl. *Binctin*, Rn. 1201.

162 Schaubildübersicht zu den drei Stufen der *réponse graduée* bei *El Sayegh*, Hadopi: année zero, Revue internationale de la propriété industrielle et artistique 118 (2010), S. 89-96 (89).

163 *Kerr-Vignale*, RIPIA 2010, S. 71-81 (75).

164 Schaubildübersicht zum Ablauf der Befassung der HADOPI-Behörde bei *Kerr-Vignale*, RIPIA 2010, S. 71-81 (77).

an Werken die entsprechend entfallenden Beiträge einziehen.[165] Die Kommission kann ebenfalls auf Basis von ihr durch den französischen Oberstaatsanwalt (*procureur de la République*) übermittelten Daten tätig werden, vgl. Art. R. 331-24 CPI. Die Voraussetzungen und Bedingungen der Befassung der Kommission regeln die Art. R. 331-35 ff. CPI. Das Gesuch muss insbesondere die für eine Verfolgung notwenigen personenbezogenen Daten und Informationen, also die IP-Adresse, und eine ehrenwörtliche Erklärung zum Beleg der Befähigung im Namen des Rechteinhabers zu handeln enthalten. Zur Lösung datenschutzrechtlicher Probleme ist es dann der HADOPI-Behörde vorbehalten, durch Einholung entsprechender Informationen beim Internetprovider die betreffende IP-Adresse einem Anschlussinhaber zuzuordnen.[166]

d. Verfahren der réponse graduée[167]

aa) Stufe 1: Erste Empfehlung

Ist die Kommission mit einem Sachverhalt befasst, der dazu geeignet ist, einen Verstoß gegen die in Art. L. 336-3 CPI festgelegte Pflicht des Internetanschlussinhabers darzustellen, so kann die Kommission dem anhand der verwendeten IP-Adresse ermittelten Anschlussinhaber gem. Art. 331-25 Abs. 1 CPI unter ihrem Siegel und auf eigene Kosten, auf elektronischem Wege (also per E-Mail) und mittels seinem Internetprovider eine Empfehlung (*recommandation*) zusenden, mit der er an seine Pflichten aus Art. L. 336-3 CPI erinnert und vor den Sanktionen nach den Art. L. 335-7 und L. 335-7-1 gewarnt werden soll. Dadurch soll ein Bewusstsein für die Unrechtmäßigkeit von Urheberrechtsverletzungen durch illegales Filesharing im Internet geschaffen und auf deren Einstellung hingewirkt werden.[168] Zugleich wandelt sich die in Bezug auf den eigenen Internetanschluss bestehende Überwachungspflicht des Art. L. 336-3 CPI faktisch zur Sicherungspflicht.[169] Mit dieser ersten Empfehlung wird der Anschlussinhaber zudem über das legale Angebot an kulturellen Inhalten im Internet, über das Bestehen von Sicherungsmitteln, mit denen Verstöße gegen die Pflicht aus Art. L. 336-3 CPI verhindert werden können, sowie über die Gefährdung des innovativen künstlerischen Schaffens und des Wirtschaftssektors Kultur durch die Missachtung des Urheberrechts und verwandter Schutzrechte informiert.

Art. L. 331-25 Abs. 3 CPI sieht vor, dass die Empfehlung das Datum und die Uhrzeit angibt, zu denen der Sachverhalt, der dazu geeignet ist, einen Verstoß gegen die in Art. L. 336-3 CPI festgelegte Pflicht des Internetanschlussinhabers darzustellen, konstatiert wurden. Hingegen muss nicht der Inhalt der durch den Verstoß betroffenen geschützten Werke oder Gegenstände offen gelegt werden. Anzugeben sind noch die telefonischen, postalischen und elektronischen Kontaktdaten, mittels derer der Empfänger der Empfehlung auf seinen Wunsch Bemerkungen (also eine Gegenvorstellung) gegenüber der Kommission anbringen und mittels derer er auf sein ausdrückliches Verlangen hin genauere Informationen hinsichtlich des Inhalts der durch den ihm zur Last gelegten Verstoß betroffenen geschützten Werke oder Gegenstände erlangen kann.

---

165 *Solmecke/Sebastian/Sahuc*, MMR-Aktuell 2011, 316298.

166 *Nérisson* , GRURInt 2010, 637-639 (638); *Strowel*, The 'Graduated Response' in France: Is It the Good Reply to Online Copyright Infringements?, in: Stamatoudi (Hrsg.), Copyright Enforcement and the Internet, Wolters Kluwer: Alphen aan den Rijn (Niederlande) 2010, S. 1147-161 (149).

167 Schaubildübersicht zu den drei Stufen der *réponse graduée* bei *El Sayegh*, Hadopi: année zero, Revue internationale de la propriété industrielle et artistique 118 (2010), S. 89-96 (89).

168 Vgl. *Gesmann-Nuissel/Wünsche*, GRURInt 2012, 231.

169 *Marino*, Recueil Dalloz 2010, 162.

bb) Stufe 2: Zweite Empfehlung

Liegt innerhalb einer Frist von sechs Monaten ab Zusendung der Empfehlung nach Art. L. 331-25 CPI erneut ein Sachverhalt vor, der dazu geeignet ist, einen Verstoß gegen die in Art. L. 336-3 CPI festgelegte Pflicht des Internetanschlussinhabers darzustellen, kann die Kommission gem. Art. L. 331-25 Abs. 2 CPI eine erneute Empfehlung mit den gleichen Informationen wie in der vorherigen auf elektronischem Wege unter den in Art. L. 331-25 Abs. 1 CPI vorgesehenen Bedingungen verschicken. Für diese zweite Empfehlung genügt ein bloßes Versenden per E-Mail jedoch nicht. Sie hat zusätzlich mit einem gegen Unterschrift auszuhändigend Brief (eine Art Übergabeeinschreiben) oder jedem anderen Mittel zu erfolgen, das zum Nachweis des Vorlagezeitpunkts dieser Empfehlung geeignet ist.
Die in diesem Empfehlungsschreiben zu machenden Angaben bestimmen sich ebenfalls nach Art. L. 331-25 Abs. 3 CPI (s.o.).

cc) Stufe 3: Sanktion

Wurde der Internetanschluss innerhalb eines Jahres nach dem Zeitpunkt der Vorlage der zweiten Empfehlung wieder zu Zwecken des illegalen Fileharings benutzt (vgl. Art. R. 335-5 Abs. 2 CPI), droht seinem Inhaber im Falle einer nachweisbaren *négligence caractérisée* (s.o.) die Sperrung des Internetanschlusses gem. Art. L. 335-7-1 CPI. Während die Sperrung in der ursprünglichen Fassung des HADOPI 1 Gesetzes noch verwaltungsrechtlich durch die HADOPI-Behörde angeordnet werden konnte, steht sie nun als strafrechtliche Zusatzstrafe (*peine complémentaire*) unter Richtervorbehalt.[170] Nach Art. 398-1 Abs. 1 Nr. 10 des französischen Strafprozessgesetzbuchs (*Code de procédure pénale*) wird die Entscheidung durch einen Einzelrichter getroffen, wobei dies gegebenenfalls im dem Strafbefehl ähnlichen vereinfachten Anordnungsverfahren (*ordonnance pénale*) gem. Art. 495-6-1 des französischen Strafprozessgesetzbuchs erfolgen kann.[171] Dieses Verfahren wird in Frankreich z. B. üblicherweise bei Geschwindigkeitsüberschreitungen und Falschparken angewandt.[172] Legt der Anschlussinhaber innerhalb von 45 Tagen Einspruch ein, so kommt es zur Hauptverhandlung nach herkömmlichem Prozessrecht.[173]

dd) Verteidigungsmöglichkeiten

Der Inhaber des der IP-Adresse zugeordneten Internetanschlusses hat nach Art. L. 331-25 Abs. 3 CPI die Möglichkeit, auf die Empfehlungen der Kommission mit einer Gegenvorstellung zu reagieren und Details der in Rede stehenden Urheberrechtsverletzung zu erfragen. Die Kommission ist zur Anhörung des betroffenen Anschlussinhabers nicht nur berechtigt, sondern auf sein Verlangen hin sogar verpflichtet.[174] Kritisiert wird aber, dass bereits die Vermutung eines Verstoßes gegen Art. L. 336-3 CPI für ein Tätigwerden der HADOPI-Behörde ausreicht und nicht immerhin einen solchen Verstoß begründende konkrete Tatbestände vorliegen müssen; daraus würde sich eine unzumutbare Beweislastumkehr zum Nachteil des Anschlussinhabers ergeben.[175] Gerade der Nachweis, dass die Urheberrechtsverletzung durch einen Dritten vorgenommen wurde, obwohl der Internetzugang ordnungsgemäß gesichert wurde, ist in der Regel aufgrund einge-

---

170 Näheres zu Voraussetzungen und Durchsetzung s.o.

171 *Pritzkow* (Fn. 5), MR-Int 2010, S. 53.

172 *Solmecke/Sebastian/Sahuc* (Fn. 5), MMR-Aktuell 2011, 316298.

173 *Nérisson* (Fn. 37), GRURInt 2010, S. 638.

174 *Pritzkow*, MR-Int 2010, 53.

175 *Solmecke/Sebastian/Sahuc*, MMR-Aktuell 2011, 316298.

schränkter technischer Möglichkeiten und Fähigkeiten eines durchschnittlichen Anschlussinhabers kaum zu erbringen.[176] Die HADOPI-Behörde bietet hierzu zwar eine von ihr geprüfte und zertifizierte Software an, die das Nutzerverhalten protokolliert.[177] Allerdings bedeutet dies eine erhebliche Beeinträchtigung der Privatsphäre und Persönlichkeitsrechte der Betroffenen und unter Umständen eine Ungleichbehandlung bei Inkompatibilität mit dem Betriebssystem des Anschlussinhabers.[178]

[176] Vgl. *Benabou*, S. 177; *Gesmann-Nuissel/Wünsche*, GRURInt 2012, 231; *Marino*, Recueil Dalloz 2010, 163.

[177] *Gesmann-Nuissel/Wünsche*, GRURInt 2012, 231.

[178] *Solmecke/Sebastian/Sahuc*, MMR-Aktuell 2011, 316298.

II. Länderbericht zur „Übersicht über die Regulierung des Datenschutzes und des Urheberrechts in der digitalen Welt in Schweden“

1. Regelungsstruktur der materiellen Standards im Datenschutz- und Urheberrecht

a. Struktur des Datenschutzrechts

In Schweden ist das Recht auf Privatsphäre in Kapitel 2 Artikel 6 Absatz 2 der Regierungsform[1], einem der vier Verfassungsgesetze in Schweden, verankert. Schweden setzte die 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 (im Folgenden „Datenschutzrichtlinie“) 1998 um, indem das Datenschutzgesetz[2] erlassen wurde.
Das Datenschutzgesetz ersetzte das zuvor in Schweden geltende Schwedische Datengesetz[3] von 1973, das vor allem auf Computer Registrierungen und nicht die Datenverarbeitung insgesamt gerichtet war.

Das Datenschutzgesetz regelt die Verarbeitung personenbezogener Daten und deren Genehmigungsvoraussetzungen. Da diese Vorschriften die alltägliche Verarbeitung personenbezogener Informationen in der elektronischen Kommunikation erschweren könnten, wurde das Gesetz 2007 geändert und gesonderte Regeln für die unstrukturierte Datenverarbeitung wurden eingeführt (mehr dazu unten). Neben diesen Sondervorschriften für die unstrukturierte Verarbeitung folgt das Datenschutzgesetz dem Aufbau der Datenschutzrichtlinie und umfasst Voraussetzungen für die Verarbeitung persönlicher Daten, Vorschriften über sensible persönliche Informationen, den Auskunftsanspruch sowie Transfer personenbezogener Daten in Drittstaaten.

Die Beschränkung auf natürliche Personen schließt Daten über juristische Personen aus, es sei denn, es handelt sich um einen Einzelunternehmer. Da die Registrationsnummer des Einzelunternehmers aus der persönlichen Nummer des Inhabers des Unternehmens besteht, wird sie als persönliche Information bewertet.[4]

In einer Entscheidung aus 2005 sahen sowohl die Schwedische Behörde für Dateninspektionen(*Datainspektionen*) als auch das Berufungsgericht für Verwaltungssachen in Stockholm(*Kammarrätt*) die IP-Nummern, die von einer schwedischen Anti-Piraten Organisation verwendet wurden, als personenbezogene Daten an.[5]

Im Zusammenhang mit Abschnitt 5 des Datenschutzgesetzes gelesen, bedeutet Verarbeitung jede Verwendung personenbezogener Daten mit automatischen oder halbautomatischen Mitteln.

---

[1] Regeringsform (1974:152).

[2] Personuppgiftslag (1998:204).

[3] Datalag (1973:289).

[4] Siehe dazu die Entscheidung des Berufungsgerichts Svea hovrättvom 31. Aug. 2004, nr B 4151–04.

[5] Entscheidung der Behörde für Dateninspektionen vom 8. Jun. 2005, nr 593–2005; und Entscheidung des Berufungsgericht für Verwaltungssachen in Stockholm vom 8. Jun. 2007, nr 285–07.

Sobald personenbezogene Daten einmal digitalisiert sind, unterliegt jede Art der Wiedergabe dieser Informationen dem Gesetz. Es ist, mit Ausnahme des Abschnittes 5a, nicht erforderlich, dass die Daten strukturiert sind; jede Art der automatischen Verarbeitung fällt unter die Definition. Typische Beispiele der Verarbeitung sind das Sammeln persönlicher Informationen bei der Registrierung von Kunden, die Weitergabe von Details von Angestellten an die Steuerbehörde sowie die Verbreitung persönlicher Informationen in Wort oder Bild auf einer Website.[6] In dieser Hinsicht ist das schwedische Recht zum Datenschutz stark auf eine digitale Perspektive ausgerichtet. Die rein handschriftliche Verarbeitung von Daten fällt nicht unter das Datenschutzgesetz.[7]

Die Abschnitte 9 und 10 des Datenschutzgesetzes entsprechen den Artikeln 6 und 7 der Datenschutzrichtlinie und legen die allgemeinen Voraussetzungen für die Verarbeitung von Daten und deren Zulässigkeit fest. Im Bereich der sensiblen Daten enthält das Datenschutzgesetz neben den allgemeinen Vorschriften der Abschnitte 9 und 10 noch zusätzliche Voraussetzungen: Abschnitt 13 enthält ein generelles Verbot der Verarbeitung von sensiblen Daten. Abschnitt 14 lässt jedoch eine Verarbeitung zu, wenn der Betroffene darin eingewilligt hat oder wenn es aus bestimmten Gründen notwendig ist.[8]

Im Jahr 2007 führte Schweden das „Missbrauchsmodell“ vor dem Hintergrund der „unstrukturierten Verarbeitung“ personenbezogene Daten ein. Wenn derartige Daten unstrukturiert verarbeitet werden, finden die meisten Vorschriften des Datenschutzgesetzes keine Anwendung und die Verarbeitung ist nur dann rechtswidrig, wenn die Persönlichkeitsrechte der betroffenen Person verletzt sind.[9] Ziel war es, die tägliche Datenverarbeitung in der elektronischen Kommunikation und das gewöhnliche Abfassen von Texte zu erleichtern[10] und eine Abkehr vom traditionellen Modell der Regulierung von Datenverarbeitung hin zu einem missbrauchsorientierten Ansatz zu erreichen.[11]

Abschnitt 5a definiert strukturierte Datenverarbeitung als die Strukturierung einer Sammlung personenbezogener Daten, sodass deren Durchsuchung und Zusammenstellung erleichtert wird. Wie bereits Definition und Bezeichnung ausdrücken, ist die Strukturierung des Materials und nicht die Art oder das Format der Informationen der entscheidende Faktor. Beispiele für unstrukturierte Datenverarbeitung sind etwa die Erwähnung persönlicher Informationen in einem linearen Text, das Versenden von E-Mails, welche persönliche Details beinhalten, die Veröffentlichung persönlicher Informationen auf einer Website sowie Bilder oder Tonaufnahmen, welche Personen darstellen.[12]

Wird die Verarbeitung für unstrukturiert erachtet, sind unter anderem die Abschnitte 9 und 10, die

---

[6] Christine Kirchberger, *Cyber Law in Sweden*, Kluwer, 2011, § 376.

[7] Abschnitt 5 des Datenschutzgesetzes, in Übereinstimmung mit der Datenschutzrichtlinie.

[8] Christine Kirchberger, *Cyber Law in Sweden*, Kluwer, 2011, § 394.

[9] Abschnitt 5a des Datenschutzgesetzes.

[10] Regierungsvorlage (*Entwurf*) 2005/06:173, ‘Översyn av personuppgiftslagen’.

[11] Sören Öman, *Implementing Data Protection in Law*, in Scandinavian Studies in Law, vol. 47 IT Law, Stockholm Institute for Scandinavian Law, 2004, unter 392.

[12] Regierungsvorlage (*Entwurf*) 2005/06:173, unter 58.

Abschnitte 13-19 über sensible Daten und die Abschnitte 23-26 über Informationen an den Betroffenen nicht anwendbar. Das heißt, der Datenverarbeiter bedarf keiner Genehmigung für die Verarbeitung personenbezogener Daten und es findet keine Unterscheidung zwischen sensiblen und nicht-sensiblen Daten statt. Die Abschnitte 31 und 32, die Sicherheitsmaßnahmen behandeln und die Abschnitte 48 und 49, die Schadensersatz und Sanktionen regeln, sind jedoch trotzdem anwendbar.

Um zu ermitteln, ob die Privatsphäre einer Person verletzt wurde, sollten folgende Gesichtspunkte beachtet werden:[13]
– der Zusammenhang, in dem die personenbezogenen Daten verwendet wurden;
– der Zweck, zu dem die Daten verarbeitet wurden;
– das Ausmaß der Verbreitung der Informationen.

Darüber hinaus ist das schwedische Strafrecht, etwa bei Ehrverletzungen, anwendbar, sodass das Missbrauchsmodell nur im Hinblick auf die Verarbeitung personenbezogener Daten anwendbar ist.

Gemäß der Datenschutzrichtlinie gibt es einige Ausnahmen für den Anwendungsbereich des Datenschutzgesetzes. Abschnitt 6 behandelt private Zwecke,[14] Abschnitt 7 regelt die Pressefreiheit. Letzterer schreibt vor, dass Zeitungen und andere geschützte Medien, die entweder unter das Gesetzes über die Pressefreiheit[15] oder das Verfassungsgesetz der Meinungsfreiheit[16] fallen, nicht an die Vorschriften des Datenschutzgesetzes gebunden sind. Eine Sondervorschrift im Verfassungsgesetz der Meinungsfreiheit gestattet es den Betreibern von Websites, ein „Zertifikat gegen die rechtliche Erschwernis von Veröffentlichungen“ (*utgivningsbevis*), das von der schwedischen Rundfunk- und Fernsehbehörde (*Radio- och TV-verket*) ausgestellt wird, zu beantragen, wenn bestimmte Voraussetzungen erfüllt werden. Zu den Voraussetzungen gehört unter anderem, dass ein rechtlich zuverlässiger Herausgeber (*utgivare*) bestimmt wird und die Rundfunk- und Fernsehbehörde davon in Kenntnis gesetzt wird und dass die Website keine interaktiven Elemente beinhaltet. Eine Zahl von Websitebetreibern hat ein solches Zertifikat erhalten und ist damit von den Vorschriften des Datenschutzgesetzes ausgenommen.

Die Abschnitte 33-55 des Datenschutzgesetzes enthalten bestimmte Vorschriften für den Transfer von Daten in Länder außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraumes (EWR). Gemäß dem Urteil des Europäischen Gerichtshofes aus 2003[17] ist die gewöhnliche Verbreitung von Informationen auf einer Website keine Übermittlung in ein drittes Land, es sei denn der Betreiber hat seinen Sitz außerhalb des EWR.

Verstößt ein Datenverarbeiter gegen die Vorschriften des Datenschutzgesetzes, so soll der Geschädigte den Schaden, der ihm durch die rechtswidrige Verarbeitung seiner Daten entstanden ist, nach Abschnitt 18 entschädigt werden. Bestimmte Arten der Datenverarbeitung können zudem

[13] Regierungsvorlage (*Entwurf*) 2005/06:173, unter 59.

[14] Artikel 3(2) der Datenschutzrichtlinie.

[15] Tryckfrihetsförordning (1949:105).

[16] Yttrandefrihetsgrundlag (1991:1469).

[17] Entscheidung C-101/01 Bodil Lindqvist [2003] ECR I-12971.

eine strafrechtliche Haftung nach Abschnitt 49 begründen. Bei einem Verstoß gegen die Abschnitte 13-21 droht eine Geldstrafe oder Freiheitsstrafe bis zu sechs Monaten. In dieser Hinsicht unterstützen Polizei und Rechtsprechung die Vorschriften des Datenschutzrechts. Zuständige Behörde für den Bereich des Datenschutzes ist die Schwedische Behörde für Dateninspektionen (*Datainspektionen*)[18].

Elektronische Kommunikation

Im Hinblick auf die elektronische Kommunikation hat Schweden 2003 das Gesetz über Elektronische Kommunikation[19] erlassen, auch um die 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 (im Folgenden „Datenschutzrichtlinie für elektronische Kommunikation“) umzusetzen.

In Umsetzung der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (Richtlinie über die Vorratsspeicherung von Daten) wurde das schwedische Gesetz über die Elektronische Kommunikation 2012 geändert. Kapitel 6 Abschnitt 16a-f wurde eingeführt. Es enthält Vorschriften über die Speicherung und Verarbeitung von Verkehrsdaten zum Zwecke der Untersuchung, Aufklärung und Verfolgung von Schwerkriminalität. Verkehrsdaten sind Daten, die darüber Auskunft geben, wer mit wem, zu welchem Zeitpunkt und an welchem Ort kommuniziert hat und welche Art der Kommunikation verwendet wurde (z.B. SMS oder Telefon). Nach Abschnitt 16d müssen Verkehrsdaten nach Ende der Kommunikation für sechs Monate gespeichert werden.

Kapitel 6 Abschnitt 18 des Gesetzes über Elektronische Kommunikation behandelt ausdrücklich Cookies und setzt Artikel 5(3) der Datenschutzrichtlinie für elektronische Kommunikation um. Elektronische Kommunikationsnetzwerke dürfen danach nur dazu benutzt werden, Zugang zu Informationen, die in Endgeräten des Benutzers gespeichert sind, zu erhalten oder diese zu speichern, wenn der Benutzer über den Zweck der Verarbeitung informiert wird und er vorher darin eingewilligt hat.

Gemäß Artikel 15(2) der Datenschutzrichtlinie für elektronische Kommunikation verweist Kapitel 6 Abschnitt 2 des Gesetzes über Elektronische Kommunikation auf das Datenschutzgesetz. Insbesondere werden Fragen zivilrechtlicher Haftung nach dem Datenschutzgesetz beantwortet. Kapitel 7 des Gesetzes über Elektronische Kommunikation enthält Vorschriften über die strafrechtliche Haftung, etwa bei einem Verstoß gegen die Geheimhaltungspflicht.

b. Struktur des Urheberrechts

Das schwedische Urheberrecht ist sowohl an die internationalen als auch an die europäischen

[18] Informationen über die Schwedische Behörde für Dateninspektionen sind abrufbar unter ihrer Website, www.datainspektionen.se.

[19] Lag (2003:389) om elektronisk kommunikation.

rechtlichen Rahmenbedingungen vergleichsweise gut angepasst. Schweden ist bereits seit 1885 Mitglied der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums (im Folgenden „Pariser Verbandsübereinkunft“) und trat 1904 der Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst (im Folgenden „Berner Übereinkunft“) bei und ratifizierte die letzten Änderungen. Schweden trat 1962 dem Rom Abkommen über den Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendeunternehmen (im Folgenden „Rom-Abkommen“) bei und unterzeichnete 1996 und ratifizierte dessen Nachfolger, den WIPO-Vertrag über Darbietungen und Tonträger (WPPT). Außerdem ist Schweden Mitglied der Welthandelsorganisation (WHO) und hat daher das Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums (TRIPS) unterzeichnet und ratifiziert.[20] Als Mitglied der EU seit 1995 ist Schweden zudem verpflichtet, den verschiedenen EU Richtlinien im Gebiet des geistigen Eigentums zu entsprechen.

Auf nationaler Ebene schützt Schweden das Urheberrecht in seiner Verfassung. Kapitel 2 der Regierungsform[21], welches grundlegende Rechte und Freiheiten enthält, erklärt in Artikel 16, dass „Autoren, Künstler und Fotographen das Recht an ihren Werken zusteht, so wie es durch Gesetz geregelt wird“.

Das ausführlichere materielle Urheberrecht in Schweden findet sich im Gesetz über das Urheberrecht in Literatur und künstlerischen Werken[22] (im Folgenden „Urheberrechtsgesetz“) von 1960. Kapitel 1 Artikel 1 dieses Gesetzes enthält eine weite Definition von literarischen und künstlerischen Werken, die alle Arten kultureller Produkte und Medieninhalte aber auch Werke von eher beschreibender Natur, wie Landkarten und Enzyklopädien umfasst. Trotzdem existiert in Schweden kein Urheberrecht der königlichen Krone; Gesetze und andere Vorschriften oder Verwaltungsentscheidungen unterfallen nach Kapitel 1 Artikel 9 des Urheberrechtsgesetzes nicht dem Schutz des Urheberrechts.

Der urheberrechtliche Schutz setzt gemäß Artikel 5(2) der Berner Übereinkunft mit dem Moment der Herstellung des Werkes ein. Der Schutz endet gemäß der Richtlinie 93/98/EWG des Rates vom 29. Oktober 1993 zur Harmonisierung der Schutzdauer des Urheberrechts und bestimmter verwandter Schutzrechte 70 Jahre nach dem Jahr des Todes des Urhebers. Leistungsschutzrechte erhalten einen 50 jährigen Schutz und Datenbanken werden fünfzehn Jahre geschützt.

Das schwedische Urheberrechtsgesetz gewährt den Urhebern von Literatur und künstlerischen Werken ökonomische und Urheberpersönlichkeitsrechte; diese werden in Kapitel 1 Artikel 2 respektive 3 geregelt. Auf ökonomische, nicht aber auf Urheberpersönlichkeitsrechte, kann gemäß Kapitel 3 Artikel 27 des Urheberrechtsgesetzes verzichtet werden, etwa durch Vertrag.

Kapitel 1 Artikel 2 gewährt zwei Arten von Exklusivrechten: das Recht, ein Werk zu vervielfältigen und das Recht, ein Werk öffentlich zugänglich zu machen. Diese Rechte werden wiederum durch Kapitel 2 des Urheberrechtsgesetzes beschränkt, der gemäß dem Dreistufentest in Artikel 9(2) der Berner Übereinkunft, Artikel 13 TRIPS und Artikel 5(5) der Urheberrechtsrichtlinie erlassen

[20] Christine Kirchberger, *Cyber Law in Sweden*, Kluwer, 2011, § 145.

[21] Regeringsform (1974:152).

[22] Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk.

wurde. Nach Kapitel 2 Artikel 11 stellen bestimmte Arten der Benutzung eines Werkes keine Verletzung des Urheberrechts dar, etwa zu Unterrichts- oder Archivierungszwecken, als Zitation, zur Bereitstellung in Bibliotheken etc. Auch private Kopien sind erlaubt. Sie werden in Kapitel 2 Artikel 12 des Urheberrechtsgesetzes geregelt.

aa) Regeln über die digitale Welt

Zu den Sonderregeln über die digitale Welt gehören ein erweitertes Recht, private Kopien zu erstellen, eine Neuregelung über temporäre Kopien und die Einführung von Regelungen zum Schutz technischer Maßnahmen. Das Recht in Artikel 12 des Urheberrechtsgesetzes, private Kopien zu erstellen, wurde im Lichte der digitalen Welt und als Resultat 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 (im Folgenden „Urheberrechtsrichtlinie") erweitert. Diesem Artikel wurde ein vierter Absatz hinzugefügt, der besagt: *„Dieser Artikel gewährt nicht das Recht, eine Kopie eines Werkes zu erstellen, wenn das Exemplar, das als Kopiervorlage dient, verändert wurde oder wenn es in Verletzung von Artikel 2 der Öffentlichkeit zugänglich gemacht wurde."*. Die Originalvorlage, die online zur Verfügung gestellt wurde, musste daher rechtmäßig veröffentlicht werden, damit die Ausnahme für private Kopien anwendbar ist.

Die Regeln über temporäre Kopien sind von dem exklusiven Recht der Vervielfältigung, das dem Inhaber des Urheberrechts zusteht, ausgenommen. Gemäß Artikel 5(1) der Urheberrechtsrichtlinie beschränkt Artikel 11a des Urhebergesetzes das Urheberrecht, indem es temporäre Kopien zulässt, vorausgesetzt, dass die *„Erstellung der Kopien ein wesentlicher und notwendiger Bestandteil eines technologischen Prozesses ist"* und dass die Kopien selbst nur *„vorübergehend sind oder nur eine untergeordnete Rolle in diesem Prozess spielen"*. Außerdem ist die Herstellung solcher Kopien nur dann zulässig, wenn der einzige Zweck entweder die, *„Übertragung in einem Netzwerk zwischen Dritten durch einen Vermittler […] oder […] ein rechtmäßiger Gebrauch […]"* ist. Diese Ausnahme von temporären Kopien ermöglicht es auch Einzelpersonen, das Internet zu benutzen, ohne eine Urheberrechtsverletzung zu riskieren. Die Vorschrift schützt auch die Anbieter von Dienstleistungen, auch wenn dieser Schutz umfassender und konkreter im Gesetz über den elektronischen Handel von 2002[23] geregelt wird, in dem Themen wie Catching und Hosting behandelt werden.

Eine weitere Sonderregel für die digitale Welt innerhalb des schwedischen Urheberrechts ist die des Schutzes von technischen Maßnahmen. Infolge der Umsetzung der Urheberrechtsrichtlinie sind technische Maßnahmen durch Kapitel 6 Artikel 52d des Urheberrechtsgesetzes geschützt und können danach nicht umgangen werden, ohne eine Strafe in Form eines Bußgeldes nach sich zu ziehen.[24] Es ist weiterhin nach Artikel 52g des Urheberrechtsgesetzes verboten, Informationen über die Digitale Rechteverwaltung, die im Zusammenhang mit einem urheberrechtlich geschützten Werk stehen, zu beseitigen oder zu verändern. Zuwiderhandlungen werden mit Geldstrafe oder mit Freiheitsstrafe bis zu sechs Monaten bestraft.[25]

[23] Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster.

[24] Artikel 57b Abs. 2 des Urheberrechtsgesetzes.

[25] Artikel 57b Abs.1 des Urheberrechtsgesetzes.

bb) Durchsetzung des Urheberrechts

Eine Verletzung des Urheberrechts kann in Schweden nach Kapitel 7 des Urheberrechtsgesetzes zivilrechtliche und strafrechtliche Haftung begründen. Eine Person, die die Verletzung von Urheberrecht geltend macht, muss vor Gericht die erforderlichen Beweise bringen. Artikel 53 regelt die strafrechtlichen Sanktionen in Form von Geld- und Freiheitsstrafe. Diese Sanktionen können verhängt werden, wenn die Urheberrechtsverletzung vorsätzlich oder grob fahrlässig begangen wurde. Die Höchstfreiheitsstrafe beträgt zwei Jahre. Artikel 54 regelt eine Schadensersatzzahlungen in Geld an den Inhaber des Rechtes, die der missbräuchlichen Nutzung des Werkes angemessen ist. Wurde die Handlung vorsätzlich oder fahrlässig ausgeführt, ist auch jeder kausal verursachte Schaden ersatzfähig.

Das schwedische Recht enthält im Strafgesetzbuch[26] auch Vorschriften, die die sekundäre Haftung von Urheberrechtsverletzungen betreffen. Kapitel 23 Abschnitt 4 sieht vor, dass auch derjenige bestraft wird, der die Straftat durch Rat oder Tat oder gefördert hat. Das Gesetz setzt nicht voraus, dass die Täter der Haupttat identifiziert sind, um jemanden wegen Beteiligung an dieser Tat zu bestrafen. Daher konnten etwa die Angeklagten im *Pirate Bay* Fall wegen Beteiligung an einer Urheberrechtsverletzung verurteilt werden, obwohl kein Haupttäter wegen einer Straftat verurteilt wurde.[27]

Schweden setzte die Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums (im Folgenden „Durchsetzungsrichtlinie“) um, indem das Urheberrechtsgesetz an einigen Stellen erweitert wurde. In Umsetzung von Artikel 8 der Durchsetzungsrichtlinie bietet Artikel 53c dem Inhaber eines Urheberrechts die Möglichkeit, eine „Anordnung zur Erteilung von Informationen“ zu beantragen. Diese Vorschrift verpflichtet Internet Provider, Informationen darüber zu erteilen, wo die IP-Adresse ihrer Nutzer verwendet wurde, als die Urheberrechtsverletzung stattfand.[28]

Seit diese Möglichkeit des Urheberrechtsinhabers, die Erteilung von Informationen gerichtlich zu beantragen im April 2009 in das schwedische Urheberrechtsgesetz eingeführt wurde,[29] gab es eine Reihe gerichtlicher Entscheidungen. Diese Entscheidungen behandelten größtenteils Streitigkeiten zwischen dem Rechtsinhaber und Service-Providern über die Übergabe von Nutzerinformationen, wobei einige Unternehmen sich weigerten, derartige Daten preiszugeben.

Im bekanntesten dieser Fälle, dem „E-Phone Fall“[30], wurde eine Reihe urheberrechtlich geschützter Hörbücher online zugänglich gemacht. Der Oberste Gerichtshof hat nach einem Vorabentscheidungsersuchen an den EuGH[31] entschieden, dass der Service-Provider verpflichtet war, dem Rechtsinhaber die Informationen zur Verfügung zu stellen, da diese Informationen die Untersuchung der Urheberrechtsverletzung erleichtern könnten.

---

[26] Brottsbalk (1962:700).

[27] Urteil desSvea Court of Appeal, B 4041-09 vom 26. November 2010.

[28] Regierungsvorlage (*Entwurf*) 2008/09:67, ‘Civilrättsliga sanktioner på immaterialrättens område – genomförande av direktiv 2004/48/EG’, 263.

[29] SieheArtikel 53c des Urheberrechtsgesetzes.

[30] Aktenzeichen Ö 4817-09, 21. Dezember 2012.

[31] Aktenzeichen C-461/10.

2. Matrix: Verbraucherschutz durch die öffentliche Verwaltung in der digitalen Welt

3. Ausrichtungen und Gegenstände der relevanten Verwaltungsbehörden

a. Verbraucherschutz durch öffentliche Verwaltung

Die Schwedische Verbraucheragentur (*Konsumentverket - KO*) ist die für den Verbraucherschutz zuständige nationale Behörde. Die KO stellt sicher, dass Unternehmen die einschlägigen Vorschriften über den Vertrieb und den Verkauf von Waren und Dienstleistungen einhalten. Verbraucher können sich mit Beschwerden an die Verbraucheragentur wenden. Die Agentur kann Unternehmen verbieten, gewisse Vertriebsformen oder Allgemeine Geschäftsbedingungen zu verwenden und kann den Verkauf von Waren und Dienstleistungen, von denen Gefahren für die Verbraucher ausgehen, untersagen. Die Agentur entscheidet jedoch keine eigentlichen Fälle; sie kann jedoch eine Zahl von Verbrauchern in Verbraucherrechtsstreitigkeiten vertreten. Die Agentur gibt einzelnen Verbrauchern keine Handlungsempfehlungen, außer dem auf der Website veröffentlichten Informationsmaterial. Wenn einzelne Verbraucher Beratung benötigen, können sie sich an den jeweiligen Verbraucherberater (*konsumentvägledare*) wenden, der für ihre Gemeinde zuständig ist.

Es gibt auch Beratungsbüros (*rådgivningsbyråer*), die von den Branchenverbänden finanziert werden aber von den öffentlichen Behörden mitverwaltet werden. Die Schwedische Telekommunikationsberatung (*Telekområdgivarna*)[32] etwa bietet Informationen und Unterstützung für Verbraucher zu Fragen, die Mobil- und Festnetztelefonie, Fernsehen und Internet betreffen.

Das Öffentliche Reklamationsamt (*Allmänna reklamationsnämnden* – ARN)[33] ist eine öffentliche Behörde, die sich mit Streitigkeiten zwischen Verbrauchern und Unternehmen beschäftigt. Es behandelt ausschließlich B2C Situationen, niemals B2B oder C2C. Die Entscheidung kann nicht angefochten werden, doch kann der Verbraucher dagegen vor den Zivilgerichten klagen. Das ARN trifft grundsätzlich keine Entscheidungen, wenn der Geschäftssitz des Unternehmens sich außerhalb von Schweden befindet.

b. Administration für die digitale Welt

Schweden hat keine allgemein zuständige Administration für die digitale Welt. Die vorgenannten Behörden behandeln den elektronischen Handel und online B2C. Außerdem ist die Schwedische Post- und Telekommunikationsbehörde (*Post- och telestyrelsen* - PTS)[34] die aufsichtführende Behörde für elektronische Kommunikation und, inklusive Telefonie, Internet und Radio und den Postsektor in Schweden. Die PTS gewährleistet Wettbewerb am Markt und dass Anbieter das Datenschutzrecht im Hinblick auf elektronische Kommunikation befolgen.

Die PTS nimmt Beschwerden von Verbrauchern an aber beschäftigt sich nicht mit den konkreten Beschwerden oder Streitigkeiten zwischen Verbrauchern und Anbietern. In diesen Fällen verweist

[32] Informationen über die Schwedische Telekommunikationsberatung sind abrufbar unter telekomradgivarna.se/.

[33] Informationen über das Öffentliche Reklamationsamt sind abrufbar unter www.arn.se/.

[34] Informationen über die Schwedische Post- und Telekommunikationsbehörde sind abrufbar unter www.pts.se.

sie die Verbraucher an die obengenannte Telekommunikationsberatung (*Telekområdgivarna*). Sie sammelt die Verbraucherbeschwerden lediglich, um abzuschätzen, mit welchem Problemen Verbraucher derzeit betroffen sind und in welchen Bereichen Informationen oder andere Maßnahmen notwendig sind.

Eine Delegation für eGovernment (*E-delegationen*)[35] wurde 2009 unter der Führung des Ministeriums für Wirtschaft, Energie und Kommunikation (*Näringsdepartementet*) eingerichtet. Die Aufgabe der Delegation für eGovernment ist die Entwicklung einer e-Verwaltung innerhalb des öffentlichen Sektors. Neben der Entwicklung digitaler Dienste beschäftigt sie sich außerdem etwa mit der Beurteilung der Einwirkung bestimmter Projekte auf die Bürger. Ihr Auftrag gilt bis 2014. Streng genommen behandelt sie nur Fragen der öffentlichen Verwaltung und keine verbraucherbezogenen Themen.

Der Schwedische Verbraucherverband (*Sveriges Konsumenter*)[36] ist eine NGO und einer seiner Hauptbeschäftigungsfelder betrifft IT und digitale Rechte. Der Verband hat keine offizielle Stellung, doch ist er in der Industrie und unter Verbrauchern sehr anerkannt.
Auch wenn sie keine Behörde ist, ist .SE (*Stiftelsen för Internetinfrastruktur*), die Schwedische Stiftung für Internetinfrastruktur, eine unabhängige Organisation, die für die schwedische Top-Level-Domain .se verantwortlich ist.

c. Organisation des verwaltungsrechtlichen Datenschutzes

Die Schwedische Behörde für Dateninspektionen (*Datainspektionen*) ist die aufsichtführende Behörde für den Bereich des Datenschutzes.[37] Sie gibt Richtlinien und Leitfäden heraus und führt auch Untersuchungen durch und bearbeitet Beschwerden.

Gemäß Abschnitt 2 der Verordnung über elektronische Kommunikation[38] ist die Schwedische Post- und Telekommunikationsbehörde (PTS) die zuständige aufsichtführende Behörde für Datenschutz innerhalb des elektronischen Kommunikationssektors. Die PTS überwacht die Anbieter von elektronischen Kommunikationsnetzwerken und stellt sicher, dass die Datenschutzbestimmungen des Gesetzes über Elektronische Kommunikation eingehalten werden. In seiner Funktion als Aufsichtsbehörde gibt die PTS Richtlinien über Datenschutz in der elektronischen Kommunikation heraus und kann, falls notwendig, Anordnungen und Bußgelder erteilen.

Die PTS und die Behörde für Dateninspektionen kooperieren in Fragen des Datenschutzes, da sich beide Zuständigkeitsbereiche in gewissem Umfang überschneiden.

d. Behördlicher Schutz des Urheberrechts

Es gibt keine eigenständige Behörde für den außergerichtlichen Schutz des Urheberrechts. Es gibt allerdings eine Zahl von Organisationen, die den Schutz des Urheberrechts in Schweden in Form von Verwertungsgesellschaften vollziehen. Diese Gesellschaften beschäftigen sich mit For-

[35] Siehe www.edelegationen.se.

[36] Siehe www.sverigeskonsumenter.se.

[37] Abschnitt 2 der Verordnung über persönliche Daten (Personuppgiftsförordning) (1998:1191).

[38] Förordning (2003:396) om elektronisk kommunikation.

men der Lizenzierung und der Nutzung urheberrechtlich geschützter Werke. Einige bekannte Beispiele und deren jeweilige Bereiche sind: STIM (Musik), Bonus Presskopia (Literatur), BUS (Kunstwerke), und Copyswede (Fernseh- und Radioprogramme).

Zusätzlich gibt es Organisationen, die das Urheberrecht und dessen Entwicklung fördern, etwa der SFU, der Schwedische Verband für Urheberrecht (*Svenska föreningen för upphovsrätt*).

e. Möglichkeit behördlichen Eingreifens zum Schutz vor übermäßiger Urheberrechtsdurchsetzung

Da die Durchsetzung des Urheberrechts den Gerichten obliegt, sind sie es, die die unterschiedlichen vorliegenden Interessen gegeneinander abwiegen und entscheiden, ob der Rechtsinhaber mit der Durchsetzung seines oder ihres Urheberrechts unverhältnismäßig handelt. Eine Person, die die Verletzung von Urheberrecht geltend macht, muss vor Gericht die erforderlichen Beweise bringen.

Wenn ein Antragsteller einen Anscheinsbeweis der Urheberrechtsverletzung gebracht hat, hat das Gericht zu entscheiden, ob ein Auskunftsanspruch[39] gewährt wird. Eine Verhältnismäßigkeitsprüfung wird vom Gericht gemäß Artikel 53d des Urheberrechtsgesetzes durchgeführt, bei der die unterschiedlichen vorliegenden Interessen gegeneinander abgewogen werden. Es liegt daher vollständig im Ermessend des Gerichts, zu entscheiden, ob die Durchsetzung eines Urheberrechts unverhältnismäßig ist.

4. Für die jeweilige Verwaltung zu behandelnden Sachfragen

Gemäß Kapitel 12 Artikel 2 der Regierungsform[40] ist die Verwaltung insoweit unabhängig, als weder die Regierung noch das Parlament vorschreiben kann, wie die Behörde in einem bestimmten Fall zu entscheiden hat.

Da der Großteil der relevanten Regelungen im Bereich des Verbraucherschutzes, Datenschutzes und Urheberrechts nur auf Rechtsträger anwendbar sind, die in Schweden angesiedelt sind, haben die jeweiligen Behörden keine gesonderten Befugnisse für die Durchsetzung von Vorschriften außerhalb Schwedens. Was etwa soziale Medien und Cloud Service Provider angeht, hat die Behörde für Dateninspektionen lediglich überprüft, wie Verwaltung und Unternehmen die sozialen Medien und Cloud Services in ihrer Arbeitsweise nutzen und nicht, in welchem Umfang die Anbieter selbst, etwa Facebook, Dropbox, usw. das Schwedische Datenschutzgesetz beachten müssen.[41]

a. Die Verbraucheragentur (Konsumentverket, KO)

[39] Siehe Artikel 53c des Urheberrechtsgesetzes und Artikel 8 der Durchsetzungsrichtlinie.

[40] Regeringsform (1974:152).

[41] Siehe außerdem www.datainspektionen.se/in-english/cloud-services/.

aa) Grundverständnis von der Behörde

Die Verbraucheragentur ist vor allem auf Verbraucher ausgerichtet. Die übergeordnete Zielvorstellung sind „aufmerksame und vorsichtige Verbraucher“ (*"medvetna och säkra konsumenter"*)[42], was bedeutet, dass Verbraucher die Fähigkeit und Möglichkeit haben, selbständige Entscheidungen zu treffen. Ihre drei Aufgaben sind zu stärken, zu unterdrücken und zu unterstützen: *Stärkung* der Position des Verbrauchers durch Informationen über Schwächen in verschiedenen Märkten; Unterdrückung unternehmerischer Zuwiderhandlungen durch aktive und effektive Aufsicht, um insgesamt ein hohes Verbraucherschutzniveau zu gewährleisten; Unterstützung, indem sichergestellt wird, dass die Informationen, die Verbraucher benötigen, unabhängig, zugänglich und auf die Zielgruppe zugeschnitten sind.

Die Aktivitäten der Behörde richten sich vor allem auf rechtlichen Schutz, Produktsicherheit und Informationen sowie zunehmendem Risikobewusstsein bei Einzelpersonen und Unternehmen. In diesem Sinne ist sie vor allem auf Prävention ausgerichtet, indem sie mit der Industrie zusammenarbeitet, um Vereinbarungen, etwa über Arten der Werbung oder Verbraucherverträge zu treffen. Sie unternimmt proaktive Maßnahmen, wie die Marktüberwachung und Produktkontrolle.

Obwohl sie nicht direkt Streitigkeiten zwischen Verbrauchern und Unternehmern bearbeitet, nimmt die Verbraucheragentur doch Beschwerden von Verbrauchern entgegen, die die Werbung oder die Vertragsbedingungen von Unternehmen betreffen. Diese Beschwerden können, gemeinsam mit der eigenen Überwachung durch die Behörde, die Grundlage für eine Untersuchung des Unternehmens bilden. Die Behörde nimmt Kontakt zum Unternehmen auf, um das Problem zu lösen. Wenn sich keine Lösung findet, hat die Behörde die Kompetenz, rechtliche Schritte vor Gericht gegen das Unternehmen einzuleiten.

Die Behörde gibt keine Ratschläge in Einzelfällen, doch arbeitet sie mit den Verbraucherberatern in den Gemeinden zusammen. An diese Berater sollten sich Verbraucher für persönliche Ratschläge wenden.

Die Behörde hat eine unabhängige Abteilung, den Europäischen Verbraucher (*Konsument Europa*)[43], die teilweise von der Europäischen Kommission und teilweise vom Netzwerk der Europäischen Verbraucherzentren finanziert wird. Diese Abteilung erteilt Ratschläge an Einzelpersonen, die etwas aus anderen EU Ländern kaufen und hat zum Ziel, die Vorteile des Europäischen Binnenmarktes für den Verbraucher zu erleichtern.

bb) Struktur und Zuständigkeit der Behörde

Die Verbraucheragentur wurde 1973 gegründet. Ihre Arbeitsweise wird durch eine Vorschrift, die ihre Pflichten und Zuständigkeit beschreibt[44], und in einer Geschäftsordnung, welche die Aufgaben und Zuständigkeit beschreibt, wie es bei Behörden üblich ist, geregelt.[45] Die Agentur wird auch von der Regierung angeleitet, die die Aufgaben, welche die Behörde nach ihrer Vorstellung

[42] Siehe www.konsumentverket.se/Om-oss/Uppdrag-och-mal/.

[43] Siehe www.konsumenteuropa.se.

[44] Förordning (2009:607) med instruktion för Konsumentverket, erweitert durch Förordning (2011:1218) om ändring i förordningen (2009:607) med instruktion för Konsumentverket.

[45] Myndighetesförordning (2007:515).

erfüllen soll, näher konkretisiert und die jährliche Finanzierung vorgibt.
Die Agentur ist in Karlstad angesiedelt, in der Mitte Schwedens, und hat circa 130 Mitarbeiter. Der Generaldirektor der Agentur ist gleichzeitig der Verbraucher Ombudsmann (*KO*). Die Behörde hat vier Abteilungen: Verbraucherschutz, Verbraucherunterstützung, Verwaltung und Personal/HR und eine Analyse Abteilung.[46]

cc) Befugnisse der Behörde und informelle Verfahrensweisen
Der Verbraucher Ombudsmann (*KO*) beobachtet den Markt und verteidigt die Interessen der Verbraucher gegen Unternehmen vor Gericht. Der KO kann, durch rechtliches Handeln, unter Aufsicht der Verbraucheragentur auf Unternehmen einwirken, die sich nicht an die gesetzlichen Vorgaben halten. In den meisten Fällen, in denen Rechtsverletzungen stattgefunden haben, leiten Unternehmen freiwillig die notwendigen Schritte ein, um die gesetzlichen Vorgaben einzuhalten. Wo dies nicht der Fall ist, kann jedoch der KO eine Anordnung erlassen oder bei Gericht Klage erheben. Welche rechtlichen Schritte eingeleitet werden, hängt davon ab, was die Rechtsverletzung des Unternehmens war.

Zusätzlich zu ihren eigenen Angelegenheiten kooperiert die Agentur mit verschiedenen Gremien und anderen Regierungsbehörden, um Wissen im Verbraucherbereich zu sammeln und zu teilen. Das Beratungsgremium (*Insynsrådet*) etwa hilft bei Themen, die die Arbeit der Verwaltung betreffen und der Wissenschaftsrat (*Vetenskapliga rådet*) analysiert und kommentiert die aktuellen Entwicklungen im Verbraucherbereich und gibt Einblicke in die aktuelle Forschung.

dd) Sanktionen, die die Behörde verhängen, beantragen oder sonst erlassen kann
Der KO kann Anordnungen gegen Unternehmen erlassen, die gegen das Marketinggesetz[47] oder das Gesetz über Vertragsbedingungen bei Verbraucherbezug[48] verstoßen. Zwei Arten von Anordnungen können erlassen werden: eine Unterlassungsanordnung, die es einem Unternehmen verbietet, eine bestimmte Werbung oder Vertragsbedingung zu verwenden; eine Auskunftsanordnung, die das Unternehmen verpflichtet, wichtige Informationen in seiner Werbung anzugeben. Wenn das Unternehmen die Anordnung akzeptiert, hat sie dieselbe Wirkung wie eine gerichtliche Anordnung. Akzeptiert das Unternehmen die Anordnung jedoch nicht oder handelt ihr zuwider, kann der KO eine Klage gegen das Unternehmen vor dem Amtsgericht (*tingsrätt*) einleiten. In Fällen, in denen die rechtliche Situation unklar ist, erlässt der KO keine Anordnungen, sondern reicht Klage vor dem Gericht für Markt- und Wettbewerbsangelegenheiten (*Marknadsdomstolen*) ein.

Die Behörde hat daher die Möglichkeit, gefährliche Produkt oder Dienstleistungen zu untersagen oder sicherzustellen, dass der Hersteller Informationen über die verbundenen Risiken erteilt.

Der KO kann Maßnahmen ergreifen, wenn irreführende Werbung oder Bezeichnungen stattgefunden haben, unzulässige Allgemeine Geschäftsbedingungen verwendet wurden, falsche Preisinformationen gegeben wurden oder wenn es um gefährliche Produkte und Dienstleistungen

[46] Ein detaillierteres Organigramm ist abrufbar unter www.konsumentverket.se/Global/Konsumentverket.se/om-oss/Dokument/organisation-chart-swedish-consumer-agency-2012.pdf.

[47] Marknadsföringslagen (2008:486).

[48] Lag (1994:1512) om avtalsvillkor i konsumentförhållanden.

geht.
Der KO kann auch Verbraucher vor Gericht vertreten. Der Ombudsmann kann einzelnen Verbrauchern in einem Streit mit einem Unternehmen in Form eines individuellen Verbrauchervertreters helfen. Er kann auch einer Gruppe von Verbrauchern, die in einem Streit mit einem Unternehmen stehen, in Form einer Verbandsklage zur Seite stehen.

ee) Spielräume der Behörde für eigene Politik; Verpflichtung, auf Begehren zu reagieren
Die Behörde hat einen gewissen Spielraum in Bezug auf die Wahl ihrer Tätigkeit. Sie ist nicht verpflichtet, Verbraucher vor Gericht zu vertreten – daher kann sie sich diejenigen Fälle aussuchen, in denen sie es für angemessen erachtet, einzugreifen. Da von der Agentur keine Einzelfälle behandelt werden, unternimmt sie einen eher übergeordneten Blick auf den Markt. Anträge von Einzelpersonen oder Verbänden können zwar zur Untersuchung eines Unternehmens führen, doch ist die Agentur nicht verpflichtet, auf jeden einzelnen Antrag zu reagieren.

b. Das Öffentliche Reklamationsamt (Allmänna reklamationsnämnden – ARN)

aa) Grundverständnis von der Behörde
Das vorrangige Ziel des Öffentlichen Reklamationsamts ist es, Streitigkeiten zwischen Verbrauchern und Unternehmen unparteiisch zu verhandeln, nachdem von einem Verbraucher eine Beschwerde eingelegt wurde. Das Amt behandelt ausschließlich B2C Verhältnisse, das heißt weder C2C noch B2B. Es funktioniert in etwa wie ein Gericht und gibt als solches keine Ratschläge über Einzelfälle. Das Verfahren vor dem Reklamationsamt geschieht unentgeltlich und dauert etwa sechs Monate von der Beschwerde bis zur Entscheidung.

Der Streit wird auf Grundlage der Informationen und Beweise entschieden, die die Parteien erbracht haben (es wird also keine eigenständige Beweiserhebung durchgeführt). Das Gremium betrachtet die vorgelegten Tatsachen und bewertet den Streit auf Grundlage der rechtlichen Rahmenbedingungen (Gesetze und Richterrecht).

Das Amt ist außerdem mit der Informierung von Verbrauchern und Unternehmen über seine Arbeitsweise und der Unterstützung der Bearbeitung von Verbraucherstreitigkeiten durch die kommunalen Verbraucherberater beauftragt.

bb) Struktur und Zuständigkeit der Behörde
Die Tätigkeiten des Reklamationsamts werden durch eine Vorschrift geregelt, die seine Rechte und Pflichten beschreibt.[49]

Das Amt hat einen Vorsitzenden und einen stellvertretenden Vorsitzenden, die beide erfahrene Richter sind und von der Regierung ernannt werden. Die Regierung ernennt auch eine Zahl von Richtern, um den verschiedenen Abteilungen vorzustehen. Das Amt hat 13 verschiedene Abtei-

[49] Förordning (2007:1041) med instruktion för Allmänna reklamationsnämnden.

lungen und ist unterteilt nach Produkten/Dienstleistungen. So gibt es etwa verschiedene Abteilungen für das Bankwesen, Elektronik, Möbel, Reise usw. Wenn ein Produkt oder eine Dienstleistung nicht unter eine dieser speziellen Abteilungen unterfällt, so gehört sie zur Abteilung für Allgemeines.

Zum Amt gehören auch eine Reihe assoziierter Mitglieder, die Kenntnis in einer speziellen Branche, der Industrie allgemein oder im Verbraucherrecht haben. Sie sind unabhängig und unterstützen weder Verbraucher noch Unternehmen in der Streitigkeit. Diese Mitglieder werden ernannt nach einem Vorschlag durch Behörden oder Verbraucher oder eines Branchenverbandes, der von der Regierung anerkannt wird. In Abteilungssitzungen müssen jeweils eine gleiche Zahl von der Verbraucher- und der Branchenseite anwesend sein. Auf diesen Sitzungen sind regelmäßig vier assoziierte Mitglieder, zwei von jeder Seite, anwesend.

Das Amt hat ein Sekretariat, das hauptsächlich aus zwei Anwälten besteht, die Fälle vorbereiten und die kommunalen Verbraucherberater unterstützen. Das Amt ist außerdem mit einem Beratungsgremium verbunden, das im Hinblick auf die Arbeit und die Transparenz des Amtes unterstützt.

cc) Befugnisse der Behörde und informelle Verfahrensweisen

Das Amt entscheidet Einzelfälle, leitet jedoch nicht eigenständig Verfahren ein. Seine Aufgaben umfasst keine übergeordnete Marktüberwachung und es ist ihm nicht gestattet, Fälle weiter zu untersuchen.

dd) Sanktionen, die die Behörde verhängen, beantragen oder sonst erlassen kann

Das Amt gibt Empfehlungen darüber ab, wie Streitigkeiten gelöst werden sollen, etwa dass ein Unternehmen ein mangelhaftes Produkt reparieren soll. Diese Empfehlungen sind zwar nicht bindend, doch werden sie von der Mehrheit der Unternehmen befolgt. 2012 wurden 76 % der Entscheidungen des Reklamationsamtes befolgt.[50]

ee) Spielräume der Behörde für eigene Politik; Verpflichtung, auf Begehren zu reagieren

Das Amt kann nicht über seine eigene Tätigkeit entscheiden, sondern reagiert lediglich auf die Fälle, die ihm vorgelegt werden. Wenn ein Fall in den Aufgabenbereich des Amtes fällt, ist es zum Tätigwerden verpflichtet. Es gibt Einschränkungen im Hinblick auf den Streitwert, Art der Streitigkeit etc. Das Amt kann Angelegenheiten zurückweisen, die es für unangemessen hält oder die nicht ausreichend untersucht werden können.[51]

c. Die Schwedische Post- und Telekommunikationsbehörde (Post- och telestyrelsen – PTS)

[50] Weitere Statistiken unter www.arn.se/Om-ARN/Statistik/.

[51] Siehe weiter www.arn.se/English/English/.

aa) Grundverständnis von der Behörde

Die PTS ist eine Behörde, die die elektronische Kommunikation und den Postsektor in Schweden überwacht. „Elektronische Kommunikation" beinhaltet Telefonie, das Internet und das Radio. Die PTS hat vier übergeordnete Ziele: langfristige ‚Vorteile für den Verbraucher, langfristig nachhaltiger Wettbewerb, effiziente Ressourcennutzung und sichere Kommunikation.

Die Behörde soll nur eingreifen, wenn der Markt nicht ordnungsgemäß funktioniert. Wo ein Eingreifen notwendig ist, soll die Behörde die Maßnahme mit dem geringsten Eingriffsniveau zur Erreichung des Ziels ergreifen.

Die PTS muss ihre Tätigkeiten immer im besten Interesse der Verbraucher ausführen. Sie führt an Verbraucher gerichtete Informationsmaßnahmen durch und ermöglicht, dass Beschwerden gegen Anbieter eingereicht werden können. Sie unternimmt Initiativen, um Verbraucher über die Sicherheit und Privatsphäre im Internet zu informieren. Aufgabe der PTS ist es, den Markt mit guten Rahmenbedingungen auszustatten, um Kommunikationsdienstleistungen zu erbringen. Dies beinhaltet nicht nur elektronische, sondern auch Postdienstleistungen. Die PTS zielt auch darauf ab, die Robustheit von Netzwerken zu erhöhen, um sichere Kommunikation zu gewährleisten. Außerdem finanziert die PTS Glasfaser-Netzwerkverbindungen, Mobilfunkbasisstationen, Reservekraftwerke usw.

bb) Struktur und Zuständigkeit der Behörde

Die Tätigkeiten der PTS werden durch eine Vorschrift geregelt, die ihre Rechte und Pflichten beschreibt[52] und in einer Geschäftsordnung, welche die Aufgaben und Zuständigkeit beschreibt, wie es bei Behörden üblich ist[53]. Die Behörde wird auch von der Regierung angeleitet, die die Aufgaben, welche die Behörde nach ihrer Vorstellung erfüllen soll, näher konkretisiert und die jährliche Finanzierung vorgibt. Die PTS berichtet dem Ministeriums für Wirtschaft, Energie und Kommunikation. Sie ist eine unabhängige Behörde; der Regierung ist es nicht gestattet, der PTS vorzugeben, wie sie eine bestimmte Handlung ausführen oder in einem bestimmten Fall, indem es um die Ausübung von Hoheitsmacht geht, entscheiden soll. Die PTS hat ein jährliches Budget, erhält Spenden und wird außerdem finanziert durch Bußgelder, die gegen Anbieter erhoben werden, die eine Lizenz, die unter die Aufsicht der PTS fällt, haben.

Die PTS besteht aus fünf Abteilungen (Wettbewerb, Verbrauchermarkt, Netzsicherheit, Spektrum und Postangelegenheiten) und vier unterstützenden Abteilungen (Verwaltung, Kommunikation, Personal und Rechtsangelegenheiten) sowie dem Büro des Generaldirektors. Die Aufgaben werden daher nach Sachgebieten aufgeteilt. Die Behörde hat einen Generaldirektor, der gleichzeitig Führungsvorstand ist, einem stellvertretenden Generaldirektor und ein Gremium von Direktoren, die durch die Regierung ernannt werden.[54] Die Behörde hat etwa 250 Angestellte und hat ihren Hauptsitz in Stockholm.

Die PTS vertritt Schweden in der Internationalen Fernmeldeunion (ITU).

---

[52] Förordning (2007:951) med instruktion för Post- ochtelestyrelsen.

[53] Myndighetesförordning (2007:515).

[54] Für weitere Details über den Aufbau der Behörde siehe www.pts.se/en-GB/About-PTS/Organisation/.

cc) Befugnisse der Behörde und informelle Verfahrensweisen
Die PTS kann Informationen über ein Problem beschreiben oder zur Verfügung stellen, beaufsichtigen und Anordnungen und Vorschriften erlassen. Die PTS löst Streitigkeiten zwischen Anbietern, führt Compliance Tätigkeiten in Bezug auf Anbieter durch und entscheidet über Lizenzen.

Das Gesetz über Elektronische Kommunikation von 2003 stattet die PTS mit der Befugnis aus, Rahmenbedingungen und Regeln für den Markt der elektronischen Kommunikation aufzustellen, um Wettbewerbsprobleme zu verhindern. Sie kann bestimmen, dass Anbieter bestimmte Dienstleistungen anbieten sollen, etwa solche, die sich an Menschen mit Behinderung richten. Dasselbe Gesetz verpflichtet die PTS auch, die Funktionsfähigkeit und Sicherheit der elektronischen Kommunikation zu überwachen.

Jedes Jahr gibt die PTS Berichte heraus, die den schwedischen Telekommunikationsmarkt, Entwicklung des Breitbandnetzes, Zustand des Wettbewerbs usw. beschreiben.

dd) Sanktionen, die die Behörde verhängen, beantragen oder sonst erlassen kann
Die PTS erlässt Vorschriften und kann innerhalb ihrer Aufsichtszuständigkeit Anordnungen treffen. Sie entscheidet weiterhin über Streitigkeiten zwischen den Anbietern von elektronischer Kommunikation. Die PTS kann Bußgelder verhängen, Lizenzen oder zuvor erteilte Genehmigungen entziehen und die Bedingungen einer Lizenz oder Genehmigung abändern. Kapitel 7 des Gesetzes über Elektronische Kommunikation setzt die verschiedenen Maßnahmen, die der PTS offen stehen, im Detail fest.

ee) Spielräume der Behörde für eigene Politik; Verpflichtung, auf Begehren zu reagieren
Innerhalb des Regelungsrahmens des Gesetzes über Elektronische Kommunikation kann die PTS über ihre Tätigkeiten und Maßnahmen entscheiden. Verbraucher können Beschwerden über die Anbieter von elektronischer Kommunikation bei der PTS einreichen, die dann entscheidet, ob die Beschwerde zu einer Untersuchung des betreffenden Anbieters führt. Die Verbraucher haben kein Recht, die PTS zur Einleitung einer Untersuchung zu zwingen.

d. Die Behörde für Dateninspektionen (Datainspektionen)

aa) Grundverständnis von der Behörde
Die Behörde für Dateninspektionen ist eine öffentliche Behörde, die den Schutz der Privatsphäre in Fällen der Bearbeitung persönlicher Daten zur Aufgabe hat. Dieses Ziel ist zu erreichen, ohne den Einsatz von Technologie unnötig zu verhindern oder zu erschweren. Der Aufgabenbereich der Behörde umfasst, neben anderen Vorschriften, vor allem das Gesetz über Persönliche Daten, das Gesetz über Kreditinformationen und das Gesetz über die Eintreibung von Forderungen.

Aufgabe der Behörde ist es, sicherzustellen, dass die Vorschriften über die Bearbeitung persönlicher Daten eingehalten werden. Sie ist in dieser Hinsicht die aufsichtführende Behörde, die selbst durch ihre eigenen Beobachtungen von Unternehmen, Behörden oder Organisationen sicherstellt, dass Gesetze und Vorschriften eingehalten werden, etwa im Bereich der Videoüberwachung. Sie

erteilt auch Lizenzen an Unternehmen, im Bereich der Forderungseintreibung und Kreditauskunft geschäftlich tätig werden zu dürfen.

Die Behörde zielt darauf ab, Bedrohungen für die Privatsphäre, vor allem in sensiblen Bereichen, neuen Erscheinungsformen und Bereichen, in denen das Missbrauchsrisiko besonders hoch ist, aufzudecken und zu verhindern. Um diese Ziele zu erreichen, verbreitet sie Achtsamkeit, regt Diskussionen an, warnt vor Risiken, vermittelt Wissen, bietet Rat und Unterstützung, verhindert Fehler und Missbrauch und kommentiert Gesetzesentwürfe der Regierung, die den Bereich des Datenschutzes und der Privatsphäre betreffen.

bb) Struktur und Zuständigkeit der Behörde

Die Arbeitsweise der Behörde für Dateninspektionen wird geregelt durch eine Vorschrift, die ihre Pflichten und Zuständigkeit beschreibt[55] und in einer Geschäftsordnung, welche die Aufgaben und Zuständigkeit beschreibt, wie es bei Behörden üblich ist.[56]

Die Behörde hat vier Abteilungen: die Abteilung für das Gesundheitswesen, Forschung und Bildung; die Abteilung für Industrie, die Abteilung für Behörden und das Arbeitsleben; und Verwaltungsabteilung. Der Generaldirektor ist der Vorstand der Behörde; seit 2008 hat die Behörde kein Gremium von Direktoren mehr, allerdings hat sie ein Beratungsgremium, das die Arbeit der Behörde verfolgt. Die Behörde wurde 1973 eingerichtet und hat etwa 40 Beschäftigte, wovon zwei Drittel Anwälte sind.

Die Behörde für Dateninspektionen ist die nationale Regulierungsbehörde für die Verarbeitung von persönlichen Daten unter dem Schengener Abkommen, dem Abkommen über das zentrale Informationssystem für den Europäischen Zoll und dem Beschluss des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol). Die Behörde ist Teil der Artikel 29 Datenschutzgruppe, der Arbeitsgruppe, die sich mit der Anwendung der Datenschutzrichtlinie in diversen Mitgliedstaaten beschäftigt.

cc) Befugnisse der Behörde und informelle Verfahrensweisen

Die Behörde unternimmt Untersuchungen und bearbeitet Fragen und Beschwerden von Einzelpersonen. Sie erlässt Vorschriften im Bereich des Datenschutzes sowie generelle Ratschläge und Empfehlungen.

Die Behörde legt großen Wert auf die Vorbeugung durch Information. Ratschläge und Unterstützung von Datenschutzbeauftragten/Privacy Officern haben Vorrang. Die Behörde erlässt Vorschriften und Richtlinien und bietet Berichte über Untersuchungen und Gesetzesvorschläge. Die Behörde verfolgt und beschreibt die Entwicklung des IT Sektors in Bereichen, die die Privatsphäre und neue Technologien betreffen.

Gemäß Paragraph 43 des Datenschutzgesetzes hat die Behörde für Dateninspektionen das

[55] Förordning (2007:975) med instruktion för Datainspektionen

[56] Myndighetesförordning (2007:515).

Recht, auf persönliche Daten, die innerhalb einer Organisation verarbeitet werden und Informationen und Dokumentationen über die Verarbeitung dieser Daten und die Sicherheit dieser Verarbeitung zuzugreifen. Die Behörde hat auch das Recht, die Geschäftsräume, die für eine Untersuchung vorgesehen sind, mit oder ohne Ankündigung zu betreten.

dd) Sanktionen, welche die Behörde verhängen, beantragen oder sonst erlassen kann

Eine Organisation kann aufgefordert werden, jedwede Unzulänglichkeiten, die sich aus einer Überwachung gemäß Paragraph 43 des Datenschutzgesetzes ergeben, zu beheben. Wenn die Mängel schwerwiegend sind, müssen sie innerhalb einer bestimmten Frist behoben werden, anderenfalls ist die Organisation verpflichtet, ein Bußgeld zu zahlen.

ee) Spielräume der Behörde für eigene Politik; Verpflichtung, auf Begehren zu reagieren

Die Behörde für Dateninspektionen hat die Kompetenz, Vorschriften innerhalb des Regelungsbereichs des Datenschutzgesetzes zu erlassen. Sie nutzt diese Befugnis nur in einem absolut notwendigen Maß, um einfache Regeln zu gewährleisten.[57]

Die Behörde für Dateninspektionen kann sich entscheiden, die Verarbeitung persönlicher Daten innerhalb durch einen bestimmten Industriesektor oder eine bestimmte Behörde zu untersuchen. Die Behörde führt auch Untersuchungen in den Geschäftsräumen verschiedener Organisationen durch. Bestimmte Beschwerden von Einzelpersonen können auch zu Untersuchungen gegen eine bestimmte Organisation, Unternehmen oder Behörde führen. Einzelpersonen haben jedoch kein Recht, die Behörde für Dateninspektionen zum Tätigwerden zu zwingen. [58]

e. Die Internet Infrastruktur Stiftung

aa) Grundverständnis von der Behörde

Obwohl sie keine öffentliche Behörde ist, ist .SE (*Stiftelsen för Internetinfrastruktur*), die Internet Infrastruktur Stiftung, eine unabhängige Organisation, die die Entwicklung des Internets in Schweden fördert. .SE ist zuständig für die schwedische Top-Level-Domain .se, die Registrierung von Domains und den administrativen und technischen Betrieb des nationalen Domainnamenregisters, indem sie von der ICANN ernannt wurde. Seit September 2013 bearbeitet .SE auch den administrativen und technischen Betrieb der Top-Level-Domain .nu.
Hauptaufgabe von .SE ist es, den technischen Betrieb von .se und .nu zu verwalten und zu leiten. Außerdem strebt .SE die positive Entwicklung des Internets in Schweden durch zahlreiche Initiativen an, die durch Einnahmen aus dem Domain-Name Geschäft finanziert werden.

Einige dieser Initiativen sind an Verbraucher und Internetnutzer gerichtet. So bietet .SE etwa ein Hilfsmittel für Verbraucher an, den „Breitband Check“ (*"Bredbandskollen"*), der es den Nutzern von Breitbandnetzen erlaubt, ihre Internetverbindung sowohl auf stationären als auch mobilen

[57] Jahresbericht 2012, unter 10, www2.datainspektionen.se/bt/ladda-ner-a-bestaell?page=shop.product_details&flypage=produktsida.tpl&product_id=156&category_id=10.

[58] Mehr dazu im Jahresbericht 2012, unter 20.

Geräten zu überprüfen und zu bewerten. .SE gibt auch Internet Ratgeber heraus, um die Verbreitung von Wissen über Internetbereiche wie die Funktionsweise des Internets, Web Publikationen, Urheberschutz, Privatsphäre, E-Commerce, Internetnutzung durch Kinder usw. zu vergrößern.

.SE arbeitet auch auf eine digitale Integration hin, indem sie sich mit anderen Organisationen und Behörden zusammenschließt und unabhängige Projekte finanziert. .SE fördert nicht-kommerzielle Projekte, die das Internet in Schweden weiterentwickeln, durch die Internet Stiftung. Die Stiftung organisiert einen Schülerwettbewerb "Web Star" (*"Webbstjärnan"*), der Schüler animieren soll, eine Website aus einem Schulprojekt zu entwickeln. Das Ziel ist es, Kinder zu ermutigen, das Internet zu benutzen und ihre digitalen Fähigkeiten zu verbessern aber auch die Nutzung von IT als pädagogische Maßnahme im Unterricht zu fördern.
.SE sammelt und präsentiert Material über das Wachstum des Internets in Form von Berichten, Forschung und Analyse aus zuverlässigen Quellen auf der Website
www.internetstatistik.se.

bb) Struktur und Zuständigkeit der Behörde

Die Arbeitsweise und Aufgaben von .SE werden durch das Gesetz über die Nationalen Top-Level-Domains für Schweden im Internet geregelt.[59] Die PTS, die Schwedische Post- und Telekommunikationsbehörde, ist die aufsichtführende Behörde für .SE, die sicherstellt, dass das schwedische Domain-Name System zuverlässig funktioniert.

Durch ständige Überwachung der Qualität der Internet Infrastruktur in Schweden, möchte .SE ein hohes Niveau von Funktionalität und Verfügbarkeit des Internets in Schweden sicherstellen. Sie möchte auch dort, wo es notwendig ist, die Aufmerksamkeit auf Unzulänglichkeiten und problematische Bereiche lenken.

cc) Befugnisse der Behörde und informelle Verfahrensweisen

N/A

dd) Sanktionen, die die Behörde verhängen, beantragen oder sonst erlassen kann

N/A

ee) Spielräume der Behörde für eigene Politik; Verpflichtung, auf Begehren zu reagieren

.SE veranstaltet jeden Herbst eine jährliche Internet Tag Konferenz. Dort können Themen, die Technologie, Sicherheit, digitale Medien, Gesellschaft usw. betreffen, behandelt werden. Als Veranstalter kann .SE den Schwerpunkt auf bestimmte Themen legen, die sie für wichtig hält.

[59] Lag (2006:24) om nationella toppdomäner för Sverige på Internet.

III. Länderbericht zur „Übersicht über die Regulierung des Datenschutzes und des Urheberrechts in der digitalen Welt in Großbritannien“

Dieser Bericht soll eine Übersicht über Datenschutz und Urheberrecht geben, besonders hinsichtlich der digitalen Welt und Verbraucherschutz. Die Gesetze, gesetzliche Rahmen, Aufsichtsbehörden und Durchsetzungsmechanismen werden diskutiert, im Besonderen mit Analyse der verschiedenen Behörden und ihrer Arbeit bezüglich des Verbraucherschutzes. Wie in vielen anderen Ländern, gibt es in Großbritannien kein übergreifendes System, das spezifisch für „Verbraucherschutz in der digitalen Welt“ verantwortlich ist – besonders, weil „digitale Welt“ eine sehr weitreichende Definition ist. Von daher gibt es viele verschiedene gesetzlichen Rahmen und öffentliche sowie private Behörden, die teilweise verantwortlich für Verbraucherschutz in der digitalen Welt durch ihre eigenen fachspezifischen Aufgaben sind.

1. Regelungsstruktur des Datenschutz- und Urheberrechts

a. Struktur des Datenschutzrechts

Großbritannien hat die “*European Parliament and Council Directive 95/46/EC 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 (the ‘Data Protection Directive’)*” mit dem “*Data Protection Act 1998 (the ‘DPA’)*” durchgesetzt. Das *DPA* bleibt immer noch das wichtigste Gesetz, das sich mit dem persönlichen Datenschutz in Großbritannien beschäftigt. Der “*Freedom of Information Act 2000*” hat das *DPA* bezüglich der Funktionsweise der öffentlichen Behörden geändert und der *Durant* Fall hat die Bedeutung von „*personal data*“ erklärt.[1]

Die *DPA* schützt alle Daten über lebende und identifizierbare Individuen, aber anonymisierte oder aggregierte Daten werden nicht einbezogen, solange die Anonymisierung oder Aggregation unumkehrbar ist.[2] Das Gesetz umfasst nur Daten, die auf einem Rechner (*„equipment operating automatically in response to instructions given for that purpose*“) oder in einem *„relevant filing system*“ gespeichert werden. Die *DPA* schafft Rechte für Verbraucher und Pflichten für Menschen, Firmen oder Behörden, die solche Daten sammeln, verarbeiten oder übermitteln. Die Individuen, deren Daten verarbeitet werden, haben das Recht, die Daten zu sehen; per „*subject access request*“[3] eine Kopie davon zu erhalten und zu fordern, dass falsche Daten korrigiert werden. Wenn der “*data controller*” dies ignoriert, kann ein Gericht befehlen, dass die Daten zerstört werden müssen (das Gericht kann hier ferner Schadenersatz gewähren);[4]

---

[1] "What is personal data? Information Commissioner updates guidance", *Out-Law*, Pinsent Masons, 30 August 2007; online verfügbar; http://www.out-law.com/page-8427 “*In the case involving Michael Durant he sought information held on him by the Financial Services Authority. The Court of Appeal ruled that just because a document contained his name it was not necessarily defined as personal data. This changed the perception of how wide a definition of personal data could be.*"

[2] Art 26 *Data Protection Directive*

[3] *Subject access code of practice*, ICO, online verfügbar; http://www.ico.org.uk/for_organisations/data_protection/subject_access_requests/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject-access-code-of-practice.PDF

[4] Section 10(4), *Data Protection Act 1998*

oder verlangen, dass die Daten nicht zu Ungunsten des Verbrauchers[5] oder nicht für Direktmarketing benutzt werden.[6] Wichtige „*Schedules*“ im *DPA* stellen die zentralen Prinzipien des britischen Datenschutzes und die "gerechte" Verarbeitung von Daten dar. Besonders wichtig sind „*Schedule 1 – The Data Protection Principles*“[7] und “*Schedule 2*”,[8] das *consent* und *necessary processing* definiert.

Beispiele für die Verarbeitung sind sowohl das Sammeln von persönlichen Daten in Verbindung mit der Registrierung von Kunden, als auch die Übermittlung von Arbeitnehmerinformationen an Steuerämteroder die Veröffentlichung von persönlichen Informationen online. Fast alle Verarbeitungen werden vom *DPA* umfasst, außer einigen wichtigen Ausnahmen, ganz

---

[5] *Ibid* Section 10(1)

[6] *Ibid* Section 11

[7] *Ibid* Schedule 1: The Data Protection Principles;

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
  I. at least one of the conditions in Schedule 2 is met, and
  II. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. About the rights of individuals e.g. personal data shall be processed in accordance with the rights of data subjects (individuals).[7]
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Auch online verfügbar; http://www.legislation.gov.uk/ukpga/1998/29/schedule/1

[8] *Ibid* Schedule 2: Conditions Relevant for Purposes of the First Principle: Processing of Any Personal Data;

1. The data subject has given his consent to the processing.
2. The processing is necessary—
  a) for the performance of a contract to which the data subject is a party, or
  b) for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary—
  a) for the administration of justice, **[F1**(aa)for the exercise of any functions of either House of Parliament,**]**
  b) for the exercise of any functions conferred on any person by or under any enactment,
  c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
  d) for the exercise of any other functions of a public nature exercised in the public interest by any person.
6. **(1)**The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2) The **[F2** Secretary of State**]** may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Auch online verfügbar; http://www.legislation.gov.uk/ukpga/1998/29/schedule/2

besonders; *Section 28* – Nationale Sicherheit; *Section 29* – Strafrecht und Steuerrecht; und *Section 36* – häusliche persönliche Zwecke.

Das Gesetz schafft auch neue Straftaten und Untersagungen im Bereich des Datenschutzes; *Sub-section 21(1)* – verbietet, Daten ohne Registrierung nach *Section 17(1)* zu verarbeiten;[9] *Sub-section 21(2)* – macht es strafbar, die Meldevorschriften nach *Section 20(1)* nicht zu folgen;[10] *Section 55* – bestraft das widerrechtliche Sammeln von Daten ohne Einwilligung des *data controllers*, aber mit Ausnahmen für Kriminalitätsverhütung, dies liegt zum Beispiel bei Hackern vor; *Section 56* – bestraft es, eine „*Subject Access Request*" auf eigene persönliche Daten für einen Arbeitnehmer erforderlich zu machen. Diese Vorschrift wurde durch das *Data Protection Act 1998 (Commencement No. 2) Order 2008* eingeführt.[11]

Elektronische Kommunikationen

Großbritannien hat die "*Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector ('e-Privacy Directive')"* durch die *"Privacy and Electronic Communications (EC Directive) Regulations 2003*" umgesetzt. Die "*Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC ('Data Retention Directive')*" war problematischer und erregte Widerstand bei einigen Parteien,[12] wurde aber letztendlich durch die "*Data Retention (EC Directive) Regulations 2009*" umgesetzt. Großbritannien hat letzlich das "*Directive 2009/136/EC (the Cookie Directive)*" durch die "*Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 No.1208, ('PECR')*", die am 26. Mai 2011 in Kraft trat. Diese *Regulations* bessern vorherige Regelungen nach - die "*Privacy and Electronic Communications Regulations 2003 No.2426*" bezüglich des Datenschutzes und Verbraucherschutzes gegenüber Netzbetreibern und Telekom-Netzwerken.

Die Definition des Begriffs der Einwilligung im *e-Privacy Directive* kommt von der Definition im *Data Protection Directive*. Einwilligung persönlicher Datenverarbeitung muss freiwillig, spezifisch und informiert ("*freely given, specific and informed*")[13] gegeben werden. Dies muss nicht immer ausdrücklich erfolgen, sofern nicht die Daten als "*sensitive*" kategorisiert wurden. Die neue EU- "*Article 29 Data Protection Working Party guidance*"[14] regelt die Voraussetzungen

[9] Section 21, *Data Protection Act 1998*, Part III (Notification by Data Controllers), online verfügbar; http://www.legislation.gov.uk/ukpga/1998/29/section/21

[10] *Ibid*

[11] *Statutory Instrument 2008 No. 1592 (C. 71)*, online verfügbar; http://www.legislation.gov.uk/uksi/2008/1592/contents/made

[12] "Transposition of Directive 2006/24/EC", Open Rights Group Wiki, online verfügbar; https://wiki.openrightsgroup.org/wiki/Transposition_of_Directive_2006/24/EC

[13] *The conditions for processing*, ICO Webseite, online verfügbar; http://www.ico.org.uk/for_organisations/data_protection/the_guide/conditions_for_processing und Art 2(h) *The Data Protection Directive (EU Directive 95/46/EC)*

[14] *Working Document 02/2013 providing guidance on obtaining consent for Cookies*, online verfügbar; http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

der Einwilligung in Cookies: Danach müssen die Kunden zunächst einmal Informationen ("*specific information*") über die bestimmte Zwecke ("*exact purpose*") der Cookie-Einstellungen besitzen. Ferner muss die Einwilligung in die Nutzung vor der tatsächlichen Nutzung der Cookie-Einstellungen erfolgen und auf aktives Handeln ("*active behaviour*") der Kunden basiert sein. Zuletzt muss den Kunden die freie Wahl bleiben, die Einwilligung abzugeben oder nicht.[15]

Das "*ICO (Information Commissioner's Office)*" hat neue Richtlinien ausgegeben, die Firmen informieren, wie sie die "PECRs" befolgen können, und hat auch klargestellt, dass eine gültige Einwilligung auch durch nicht-ausdrückliche Möglichkeiten gesammelt werden kann.[16] Sie wollten damit klarstellen, dass eine konkludente Einwilligung ebenfalls oft zulässig sein kann:

> *Implied consent has always been a reasonable proposition in the context of data protection law and privacy regulation and it remains so in the context of storage of information or access to information using cookies and similar devices […] While explicit consent might allow for regulatory certainty and might be the most appropriate way to comply in some circumstances this does not mean that implied consent cannot be compliant.*[17]

Akteure der Musik- und Filmindustrie haben, frustriert durch die Verspätungen eines gesetzlichen Rahmens („*online piracy code*"), unter dem „*Digital Economy Act 2010 (DEA)*"[18] versucht, Hilfe von Internetdienstanbietern (IDA, auf Englisch; *ISPs*) im Kampf gegen online begangene Urheberrechtsverletzungen auf einer freiwilligen Basis zu bekommen (was auch stark opponiert wird)[19]. Vorgeschlagen wird eine Datenbank von mutmaßlichen Verletzern, aber Verbraucher und IDA sind besorgt, ob solche Maßnahmen nicht die Unschuldsvermutung und Beweislast umkehren. TalkTalk vermutet, dass diese Pläne den *Data Protection Act* verletzen könnten, indem Virgin die Pläne als unausführbar ("*unworkable*") beschreiben hat.[20] Allerdings finden andere, dass die Sorgen unbegründet sind.[21]

---

[15] "New cookies guidance highlights intra-EU differences on data protection definitions, says expert", *Out-Law*, Pinsent Masons, 17 Oktober 2013; online verfügbar; http://www.out-law.com/en/articles/2013/October/new-cookies-guidance-highlights-intra-eu-differences-on-data-protection-definitions-says-expert-/

[16] *Guidance on the rules on use of cookies and similar technologies*, ICO, downloadbare PDF; http://www.ico.gov.uk/news/blog/2012/~/media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.ashx

[17] "ICO publishes new guidance on 'implied consent' to cookies", *Out-Law*, Pinsent Masons, 25 Mai 2012; online verfügbar; http://www.out-law.com/en/articles/2012/may/ico-publishes-new-guidance-on-implied-consent-to-cookies/

[18] "Ofcom anti-piracy code delayed until 2015", *Out-Law*, Pinsent Masons, 10 Juni 2013; online verfügbar; http://www.out-law.com/en/articles/2013/june/ofcom-anti-piracy-code-delayed-until-2015/

[19] M Leiser, "BPI to meet with David Cameron in attempt to resurrect controversial Digital Economy Act", *The Drum*, 2 September 2013; online verfügbar; http://www.thedrum.com/news/2013/09/02/bpi-meet-david-cameron-attempt-resurrect-controversial-digital-economy-act

[20] K Fiveash, "Brit music body BPI lobbies hard for 'UK file-sharers database': Virgin Media brands plan 'unworkable', TalkTalk says 'our customers come first'", *The Register*, 2 September 2013; online verfügbar; http://www.theregister.co.uk/2013/09/02/voluntary_letters_from_isps_to_subscribers_where_illegal_file_sharing_is_detected/

[21] Siehe "ISPs data protection fears about database of suspected online copyright infringers unfounded", *Out-Law*, Pinsent Masons, 20 Sep 2013; online verfügbar; http://www.out-law.com/en/articles/2013/september/isps-data-protection-fears-about-database-of-suspected-online-copyright-infringers-unfounded/

b. Struktur des Urheberrechts

Die aktuelle Basis des britischen Urheberrechts ist der „*Copyright, Designs and Patents Act 1988 (CDPA).“* Großbritannien ist Mitglied der Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst, mit nationaler Wirkung seit 5. Dezember 1887. Es ist mit nationaler Wirkung seit 18. Mai 1964 in das Rom-Abkommen über den Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendeunternehmen eingetreten, und hat auch den Nachfolger, den WIPO-Vertrag über Darbietungen und Tonträger vom 20. Dezember 1996, unterschrieben und ratifiziert, aber mit nationaler Wirkung erst ab 2010.[22]
Großbritannien ist auch Mitglied der Welthandelsorganisation und hat das Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums (TRIPS-Übereinkommen) ebenso ratifiziert. Als EU-Mitglied seit 1973 muss Großbritannien auch die verschiedenen EU-Richtlinien bezüglich des Urheberrechts realisieren.

Formen des unautorisierten Downloadens und daneben die noch komplizierten Fragen über „*Streaming Media*“, sind wahrscheinlich die wichtigsten Problemen im Bereich des Urheberrechts in der digitalen Welt. Filesharing, besonders über Peer-to-Peer-Netze, ist die bedeutendsten Form des unautorisierten Downloadens, weshalb dagegen die meisten Entwicklungen in Politiken und Gesetzen erfolgen. Filesharing wird weitreichend im *DEA 2010*, „*Communications Act 2003*“ (*Section 124* vom *DEA* verbessert), und *CDPA 1988* besorgt.
Normalerweise ist das Downloaden widerrechtlich, wenn es nicht autorisiert ist. Streaming Media anzuschauen wird normalerweise nicht als Kopieren gesehen, also erfolgt auch kein unautorisiertes Downloaden. Der *Digital Economy Act* wurde nach dem „*2009 Digital Britain Report*“ geschaffen, auch auf Druck der Industrie-Akteure wie beispielsweise der „*Britisch Phonographic Industry (BPI)*“. Er trat im Juni 2010 in Kraft[23] und versucht, online begangene Urheberrechtsverletzungen zu regulieren, besonders Filesharing.

aa) Regelungen für die “Digitale Welt”

Der *DEA* verbessert und erweitert frühere Gesetze, speziell für Entwicklungen der digitalen Welt, wie zum Beispiel sowohl die CDPA Schuldfähigkeit für Verletzungen als Ergebnis des Geschäftsverlaufs bis zu £50.000 erhöhen,[24] als auch den *Communications Act 2003 Section 124* mit *Sections 3-18 DEA* verbessern, um die „*enforcement letters*“, Ofcom, „*3-strikes-policy*“, usw, besser zu regulieren. Der *DEA* hat auch eine wichtige fachspezifische Behörde in diesem Telekom-Gebiet, Ofcom, restrukturiert (ursprünglich im "*Office of Communications Act 2002*“ geschaffen) und die kompletten Befugnisse vom *Communications Act 2003* bekommen, sodass die Abschwächung oder Blockierungen von Internetanschlüssen gegen mutmaßliche Verletzer erlaubt wurde.

Die Durchsetzung des Urheberrechts in diesem Gebiet wird also durch den *DEA* und Ofcom reguliert. Dies erfolgt dadurch,, dass die Rechteinhaber („*rightsholders*“) die IP-Adressen der mutmaßlichen Verletzer sammeln und dann einen „*copyright infringement report*“ an den IDA schicken. Dieser Bericht enthält den Verdacht auf die und die Beschreibung der Verletzung, Beweismittel dafür und die relevante IP-Adresse. Dabei müssen die Beweismittel innerhalb eines Monats nach Sammeln der Beweismittel an den IDA geschickt werden.[25] Der IDA muss

[22] *WIPO Performances and Phonograms Treaty (Geneva, 1996) Status on October 14, 2013*, downloadbare PDF; http://www.wipo.int/export/sites/www/treaties/en/documents/pdf/wppt.pdf

[23] Einige Vorschriften sind am 8. April in Kraft getreten, aber die Anderen erst danach durch Rechtsverordnungen.

[24] Section 42, *Digital Economy Act 2010*

[25] Section 124A(3), *Communications Act (amended by Section 3 DEA)*

den mutmaßlichen Verletzern auch eine schriftliche Androhung rechtlicher Schritte (*enforcement letters*) zukommen lassen, was innerhalb eines Monats nach Empfang des *copyright infringement reports* erfolgen muss. Dieser *enforcement letter* muss klarstellen, dass er nach *Section 124A(6)(4) Communications Act (amended by DEA)* geschickt wird und weiterhin den Namen des Rechteinhabers, eine Beschreibung der anscheinenden Verletzung, die Beweismittel, IP-Adresse und den Zeitraum der Sammlung beinhalten. Ferner müssen Informationen über Berufung und Berufungsbegründung über das Urheberrecht und seine Zwecke und darüber enthalten sein, wie man Hilfe im Falle der unautorisierten Nutzung einer IP-Adresse findet.[26] Die Rechteinhaber könnten danach eine "*copyright infringement list*" von den IDA verlangen, eine Liste aller Kunden, die die Schwelle des *Ofcom-Codes* und *3-strikes-policy* erreicht haben.[27] Danach dürfen die Rechteinhaber vor Gericht gehen, um eine Verfügung zur Identifikation zu bekommen, und schließlich um einen Wiederholungstäter anzuklagen.

Der *DEA* bestimmt aber einige Berufungsgründe:
Diese liegen vor, wenn die anscheinende Verletzung nicht wirklich eine Verletzung des Urheberrechts ist;[28] wenn die IP-Adresse der Verletzungszeit sich nicht auf die IP-Adresse des *enforcement letters* bezieht,[29] oder andere angemessene Gründe ("*or any other reasonable grounds*") im Sinne dieses "*draft codes*" vorliegen.[30] Dies ist beispielsweise der Fall, wenn der Verbraucher angemessene Maßnahmen ergriffen hat, andere von der Nutzung der IP-Adresse auszuschließen.[31]
Erlaubt ist dabei, die Berufungen in einem außergerichtlichen Verfahren zu bearbeiten (unter „*Section 6* und *13 DEA)*. Anders als bei gerichtlichen Berufungen gibt es in diesen Fällen eine Unschuldsvermutung.[32]
Die höchste Durchsetzungsmethode des Urheberrechts (normalerweise eher verbraucherfeindlich als verbraucherfreundlich, weil die Internet-User in diesen Fällen normalerweise Verbraucher wären und nicht andersherum) ist in *Section 17 (Power to make provisions about injunctions preventing access to locations on the Internet)* und *Section 18 (Consultation and parliamentary scrutiny) DEA* zu finden. *Section 17* erlaubt die Blockierungsunterlassungsurteile, die sogenannte "*blocking injunctions*", die Internetzugriff auf eine IP-Adresse blockieren können. Die sollen normalerweise nach drei Warnungen von der IDA kommen, daher der

---

[26] Section 124A(6), *Communications Act (amended by Section 3 DEA)*

[27] Section 124B and 124C, *Communications Act (amended by Sections 4 and 5 DEA)*

[28] Section 124K(3)(a), *Communications Act (amended by Section 13 DEA)*

[29] Section 124K(3)(b), *Communications Act (amended by Section 13 DEA)*

[30] "Ofcom asked not to include general right to appeal under Digital Economy Act code", *Out-Law*, Pinsent Masons, 5 September 2011; online verfügbar; http://www.out-law.com/en/articles/2011/september/ofcom-asked-not-to-include-general-right-to-appeal-under-digital-economy-act-code/ und *Online Infringement of Copyright and the Digital Economy Act 2010 Draft Initial Obligations Code*, Ofcom, Mai 2010; online verfügbar; http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf

[31] Section 124K(6), *Communications Act (amended by Section 13 DEA)*

[32] Section 124K(5), *Communications Act (as amended by Section 13 DEA);*

"The code must provide that an appeal on any grounds must be determined in favour of the subscriber unless the copyright owner or internet service provider shows that, as respects any copyright infringement report to which the appeal relates or by reference to which anything to which the appeal relates was done (or, if there is more than one such report, as respects each of them)—

(a)the apparent infringement was an infringement of copyright, and

(b)the report relates to the subscriber's IP address at the time of that infringement."

Name „*3-Strikes-Policy*“ - der aber noch nicht benutzt wird und noch immer sehr umstritten ist.[33]

Im Moment soll der Einsatz solcher Maßnahmen nur in extremen Fällen, in denen das Gericht glaubt, dass sehr viele Urheberrechtsverletzungen passieren könnten, benutzt werden.[34] Das Gericht muss auch die Maßnahmen der IDA und Rechteinhaber, “*any representations made by a Minister of the Crown*”, die Interessen der Verbraucher und die Meinungsäußerungsfreiheit in Betracht ziehen.[35] Es gibt eine maximale Geldstrafe i.H.v. £250.000 für IDA oder Rechteinhaber,[36] die ihre Pflichten an Ofcom (wegen Notifizierungen usw.) [37] nicht erfüllen.

bb)Schwierigkeiten des aktuellen Systems

Es gibt eine Menge Schwierigkeiten mit den aktuellen Systemen; z.B. wird angeführt, dass diese zu verbraucherfeindlich seien oder ein zu niedriges Beweisniveau forderten, besonders, wenn es zu einer strafrechtlichen oder zivilrechtlichen Schuldvermutung oder der Abgabe von persönlichen Daten führen könnte.[38] Andererseits wird vertreten, dass es zu wenig parlamentarische Überprüfung und Kontrolle gäbe, und oftmals wird auch eine Reform des Gesetzes verlangt.[39] Eine gerichtliche Überprüfung von *Sections 3-18* wurde von IDA, BT und TalkTalk, verlangt. Die Anfechtungsklage ist gescheitert, aber die Berufung wurde am 7. Oktober 2011 zugelassen. Die Berufung im “*Court of Appeals*” wurde im März 2012 letztendlich verloren, aber es wird noch immer an einer klareren Gesetzesreform gearbeitet[40] und es stellt sich weiterhin die Frage, ob europarechtlich noch alles in Ordnung ist.[41] Es wurde argumentiert, dass das Gesetz unklare Prinzipien und kein konkretes Recht einführe oder die Verantwortungen und Befugnisse der IDA und Rechteinhaber nicht völlig klar seien.[42] Andere Industrie-Akteure (außer IDA) argumentieren, dass die Maßnahmen, also die „*3-strikes*“, zu langsam seien und dass nicht genug getan werde, um die Urheberrechtsverletzungen zu vermindern.[43]

---

[33] G Moody, “Warning Letters Under UK's Three Strikes Plan Unlikely To Be Sent Out Before 2016 -- If Ever”, TechDirt, 19 Juni 2013; online verfügbar; http://www.techdirt.com/articles/20130608/03355523371/warning-letters-under-uks-three-strikes-plan-unlikely-to-be-sent-out-before-2016-if-ever.shtml

[34] Section 17(4), *Digital Economy Act 2010*

[35] Section 17(5), *Digital Economy Act 2010*

[36] Section 124L(2), *Communications Act*, *(amended by Section 14 DEA)*

[37] Section 124G(6), *Communications Act (amended by Section 9 DEA)*; “*Internet service providers and copyright owners must give OFCOM any assistance that OFCOM reasonably require for the purposes of complying with any direction under this section*”

[38] D Mendis, “Digital Economy Act 2010: fighting a losing battle? Why the ‘three strikes’ law is not the answer to copyright law's latest challenge”, *International Review of Law, Computers & Technology*, Vol. 27 (1-2), (2013)

[39] “Digital Economy Act to be reviewed by courts and Parliament”, *Out-Law*, Pinsent Masons, 10 November 2010; online verfügbar; http://www.out-law.com/page-11538

[40] K Fiveash, “BT, TalkTalk lose final appeal against Digital Economy Act”, *The Register*, 6 März 2012; online verfügbar; http://www.theregister.co.uk/2012/03/06/bt_talktalk_lose_final_appeal_against_digital_economy_act/

[41] M Sweney, J Halliday, “BT and TalkTalk given last chance to challenge Digital Economy Act: Lord Justice Lewison grants UK's two biggest ISPs permission to appeal against their failed challenge to the act”, *The Guardian*, 7 Oktober 2011; online verfügbar; http://www.theguardian.com/technology/2011/oct/07/bt-talktalk-digital-economy-act?INTCMP=ILCNETTXT3487

[42] J Kiss, “Digital Economy Act is proving hard to follow with real progress”, *The Guardian*, 9 Mai 2011; online verfügbar; http://www.theguardian.com/media-tech-law/digital-economy-act-progress

[43] Oben erwähntes Datenbank-Schema

Es gibt auch praktische Schwierigkeiten in dem System, wie die Schwierigkeiten, einen Verletzer zu verfolgen, weil sie leicht zu einer neuen P2P Gruppe wechseln können. Auch problematisch ist, dass dieser *Ofcom-Code* nur IDA mit mehr als 400.000 Kunden erfasst, also können die Verletzer ganz leicht zu einer kleineren IDA wechseln. Dass die IP-Adresse nicht genau den Täter, sondern nur den Ort bestimmt, kann problematisch sein, wenn mehrere Leute eine IP-Adresse benutzen – was sehr schwierig für WGs, Schulen und Universitäten wäre. Verletzer wechseln oft auch zu spezifischen Webseiten, wo direkte Downloade möglich sind, was nur effektiv mit der extremen Lösung der Seitenblockierung bekämpft werden kann.[44] Ofcom stellt diese Schlupflöcher klar; "*for all blocking methods circumvention by site operators and internet users is technically possible and would be relatively straightforward by determined users*."[45]

Anderseits gibt es bestimmte Probleme bezüglich der Grundrechte und Freiheiten. Warnbriefe könnten effektiv sein, aber in diesen Fällen muss der IDA sowohl Richter als auch Jury sein. Der IDA weiß aber anfangs nicht, ob eine mutmaßliche Verletzung auch wirklich eine Verletzung ist und mussvermuten, dass alle *copyright infringement reports* gültig sind, wodurch die Rechteinhaber eine erhebliche Macht besäßen. Das kann leicht zur Leitungsunterbrechung der Kunden ohne fairen Prozess führen. Auch vermutet ist, dass die Kunden die Kosten der Durchsetzung tragen werden. Weitere Probleme bezüglich britischer Urheberrechtssystemen (die auch für den Datenschutz wichtig sind) sind der Konflikt zwischen die Meinungsäußerungsfreiheit nach dem „*Human Rights Act 1998 (HRA)*" und das Urheberrechtrecht nach dem *CDPA 1988*. Solche Beschränkungen der Meinungsäußerungsfreiheit sind nicht unbedingt nötig oder „*necessary in a democratic society*".[46] Schutz des öffentlichen Interesses („*public interest defence*") oder eine Unvereinbarkeit mit dem HRA 1998 könnte auch für solch ein System problematisch sein.[47]

2. Öffentliche Verwaltung der digitalen Welt

Wie oben diskutiert, geht die allgemeine Tendenz hin zu einem verbraucherfreundlicheren System, wenn es sich um Verbraucherverträge mit Dienstleistungen oder digitalen Waren (besonders IDA- Und Telekoms-Dienstleistungsverträge) handelt. Allerdings ist die Tendenz weniger verbraucherfreundlich, wenn es um die Durchsetzung des digitalen Urheberrechts geht, weil die Wertungen und Maßnahmen ziemlich pro-Industrie und rechteinhaberfreundlich sind und mit weniger Betonung auf Unschuldsvermutung, Datenschutz und Privatheit der Internet-User erfolgen.

Der Verbraucherschutz ist also in Großbritannien eine Mischung aus direkten staatlichen Interventionen auf legislativen ministeriellen Ebenen, öffentlichen Behörden, besonders quasi-selbstständige ‚*quangos*';[48] aber auch völlig privaten verbraucher- oder bürgerrechtlichen Organisationen, wie z.B. OpenRightsGroup.org.

Wie in vielen Ländern gibt es in Großbritannien keine weitreichende, zentralisierte Verwaltungsbehörde der digitalen Welt, teilweise auf Grund der unklaren und vielfältigen Bereiche,

---

[44] *"Site Blocking" to reduce online copyright Infringement: A review of sections 17 and 18 of the Digital Economy Act*, Ofcom, Mai 2010; downloadbare PDF; http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf

[45] *Ibid*, Seite 5.

[46] Article 10, Freedom of expression, *Human Rights Act 1998*

[47] M David, *Peer to Peer and the Music Industry: The Criminalisation of Sharing*, (2010) Sage Publications: London

[48] "Quasi-autonomous non-governmental organisations"

die unter den Namen „digitale Welt“ fallen könnten. Viele Fragen, die direkt mit der Bereitstellung von und dem Zugriff auf Internetanschlüssen gestellt werden, werden durch die Gesetze bezüglich der IDA und Ofcom als Telekommunikationsübersicht geregelt. Außerdem werden viele Fragen über digitales Urheberrecht und E-Commerce auch direkt von der Verwaltung des Telekoms-Sektors beeinflusst. Natürlich sind auch die Wettbewerbs- und Verbraucherschutzbehörden, wie z.B. „*the Office of Fair Trading (OFT)*“in diesem Bereich sehr wichtig. Fast alles, was mit E-Commerce zu tun hat, wird von den Systemen und rechtlichen Rahmen des Wettbewerbsrechts auch geregelt. Sowohl aktuelle Aspekte als auch neue Entwicklungen in der digitalen Welt werden in diesen Systemen durch robuste sekundäre Rechtsvorschriften oder legislative Revisionen integriert.

Datenschutz in Großbritannien ist durch das „*Information Commissioner’s Office (ICO)*“ ziemlich stark zentralisiert. Auf das ICO wird in den späteren Überschriften ausführlicher eingegangen. In diesem Bereich gab es spezifische legislative Entwicklungen, auf EU- und nationaler Ebene, die spezifisch mit Datenschutz in der digitalen Welt zu tun haben.

Die unregistrierte Natur des Urheberrechts macht es schwierig, umfangreich und zentralisiert zu verwalten – ein Problem, das man nicht wirklich im Bereich des Patentrechts oder Markenrechts hat. Also wird das Urheberrecht oft eher durch private Organisationen wie Verbände der Urheber durchgeführt als durch öffentliche Behörden. Trotzdem gibt es einige Behörden, die teilweise für Urheberrecht, besonders für das digitale Urheberecht, verantwortlich sind, oder die zumindest den Urheberrechtsschutz ermöglichen – wie z.B. Ofcom mit der „3-strikes-policy“.

Es gibt einemangelhafte Einschränkung der Macht der Rechteinhaber und Verbände der Urheber in der Durchsetzung des Urheberrechts, obwohl diese oft übereifrig handeln können. Trotzdem gab es Fälle, in denen die potentiellen Rechteinhaber in Gewinnerzielungsabsicht handelten, indem sie eine Vielzahl von Anzeigen, in denen sie oft unberechtigt behaupteten, dass eine Urheberrechtsverletzung vorlag, an Kunden verschickten. Dies haben die Behörden oder Gerichte gestoppt.[49] Die Gerichte in Großbritannien übernehmen teilweise nur langsam den Urheberschutz von Pornographie, eine interessante Besonderheit, die auf hauptsächlich legislative-unterstützten, moralischen Gründen und öffentlichen Politik basiert.[50] Es gibt auch in Großbritannien Ausnahmen des Urheberrechts, die “*fair dealing*” Ausnahmen, die aber nicht so weitreichend wie „*fair use*“ in Amerika sind.[51] Die wichtigsten Ausnahmen liegen im Bereich der nicht geschäftlicher Forschung und Ausbildung oder der Kritik oder Berichterstattung. Besonderheiten für die digitale Welt sind, dass temporäre und nebensächliche Kopien, die aus technischen Gründen nötig sind, erlaubt sind.

---

[49] ”UK Phishing Scam Exploits Digital Economy Act”, *Bitdefender, Industry News*, 2 Juli 2012; online verfügbar; http://www.bitdefender.co.uk/security/uk-phishing-scam-exploits-digital-economy-act.html

[50] HL McQueen, C Waelde, G Laurie, A Brown, *Contemporary Intellectual Property: Law and Policy*, (2 Ed.) Oxford University Press, (2010), para 5.47

[51] Section 29

> (1) Fair dealing with a literary, dramatic, musical, etc, work, for the purpose of research for a non-commercial purpose, does not infringe any copyright in the work, provided it is accompanied by a sufficient acknowledgement of the source.

Section 30

> (1) Fair dealing with a work for the purpose of criticism or review, of that or another work, or of a performance of a work, does not infringe copyright in the work, provided it is accompanied by a sufficient acknowledgement, and provided the work has actually been made available to the public.

Wie bereits oben erwähnt, gibt es auch ab und zu strafrechtliche Maßnahmen, die die Gerichte oder Behörden nutzen können, die vielleicht auch in einigen Fällen erweitert werden.[52] Im Moment legt "*Section 55 of the Data Protection Act (DPA)*" fest, dass es widerrechtlich ist, Daten unautorisiert zu sammeln oder zu übermitteln. In diesem Fall könnten die strafrechtlichen Maßnahmen erweitert werden – nach dem "*Criminal Justice and Immigration Act (CJIA)*" darf der „*Secretary for Justice*" neue Regelungen für eine Gefängnisstrafe in diesen Fällen einsetzen, die aber noch nicht eingeführt wurden. Manche glauben, dass solche Regelungen wirklich nötig sind;

> Data protection law expert Kathryn Wynn of Pinsent Masons, the law firm behind Out-Law.com, previously said that it is "perverse that organisations and individuals guilty of accidental breaches of personal data can be issued with monetary penalty notices of up to £500,000 for those breaches, but organisations and individuals guilty of a criminal offence of deliberately invading privacy and misleading others can escape with a relatively minor punishment".[53][54]

3. Relevante Behörden

a. Information Commissioner's Office (ICO)

aa) Schwerpunkt und Ziel der Behörde

Der „*Data Protection Act 1984*" hat die Stelle „*Data Protection Registrar*" geschaffen, in dem sich die Datenverarbeiter registrieren mussten. Nach der Umsetzung der *Data Protection Directive* durch den *Data Protection Act 1998* wurde der Name in „*Data Protection Commissioner*" und später in „*Information Commissioner*" geändert. Das ICO wurde oben als primäre Datenschutzbehörde Großbritanniens erwähnt. Die erklärte Mission der Organisation besteht darin, die Informationsrechte und das öffentliche Interesse zu schützen. Sie bietet Leitfäden und Beratung für Verbraucher und Organisationen, verwaltet relevante Beschwerden und ergreift angemessene Maßnahmen, wenn gegen die Gesetze verstoßen wird. Die Natur der Behörde – Datenschutz und Informationsfreiheit – bedeutet, dass die Mehrheit von Aufgaben ziemlich verbraucherorientiert gestaltet sein können.

Mission

---

[52] "Jail sentence penalties for data breaches will be consulted on despite Government's skepticism", *Out-Law*, Pinsent Masons, 11 Oktober 2013; online verfügbar; http://www.out-law.com/en/articles/2013/October/jail-sentence-penalties-for-data-breaches-will-be-consulted-on-despite-governments-scepticism/

"*In a letter to the chairman of Parliament's Home Affairs Committee Keith Vaz, Justice Secretary Chris Grayling called for a public consultation on whether there should be new custodial penalties for breaches of Section 55 of the Data Protection Act (DPA)*." Die Briefe können auch online gelesen werden; http://www.parliament.uk/documents/commons-committees/home-affairs/Private%20investigators%20follow-up%20written%20evidence%20-%20131008.pdf

[53] "Watchdog bemoans insufficient punishment for data blagging offences", *Out-Law*, Pinsent Masons, 28 Februar 2012; online verfügbar; http://www.out-law.com/en/articles/2012/february/watchdog-bemoans-insufficient-punishment-for-data-blagging-offences/

[54] "Jail sentence penalties for data breaches will be consulted on despite Government's skepticism", *Out-Law*, Pinsent Masons, 11 Oktober 2013; online verfügbar; http://www.out-law.com/en/articles/2013/October/jail-sentence-penalties-for-data-breaches-will-be-consulted-on-despite-governments-scepticism/

> The ICO's mission is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
>
> **Our vision**
> To be recognised by our stakeholders as the authoritative arbiter of information rights, delivering high-quality, relevant and timely outcomes, responsive and outward-looking in our approach, and with committed and high-performing staff – a model of good regulation and a great place to work and develop.[55]

Das ICO ist Großbritanniens selbstständige öffentliche Behörde für Informationsrechte Aus diesem Grund überwachen sie die folgenden Gesetze: *Data Protection Act 1998*; *Freedom of Information Act 2000*; *Privacy and Electronic Communications Regulations 2003*; *Environmental Information Regulations 2004*; und *INSPIRE Regulations 2009*. Sie ist für Datenschutz in England, Schottland, Wales und Nordirland verantwortlich, hat aber auch internationale Verantwortungen.

Die Verantwortungen sind sowohl die Überwachung der Industrie und Industrie-Akteure aber auch die Publikation von Leitlinien und Informationen, dazu auch die Durchsetzung relevanter Gesetze durch Warnungen, Geldstrafen und Strafverfolgungen. Das ICO kontrolliert, ob die Organisationen die „*freedom of information requests*" und andere relevante datenschutz- und privatrechtliche Regeln befolgen. Es überwacht auch, ob die Organisationen den *Freedom of Information Act* und die „*Environmental Information Regulations*" gut beachten.[56] Das ICO kontrolliert ferner, ob Organisationen das ICO-Veröffentlichungsschema („*model publication scheme*") beachten – dieses Schema sollte ab 1. Januar 2009 adoptiert werden und erfordert, dass alle relevante Organisationen und Behörden ein Handbuch anfertigen müssen, das genau erklärt, was sie mit den Daten tun und welches leicht für die Allgemeinheit erreichbar ist. Das Handbuch soll weiterhin regelmäßig aktualisiert werden.

Die internationalen Verantwortungen enthalten Zusammenarbeit mit ähnlichen Behörden überall in Europa, mit der Europäischen Kommission und mit anderen Ländern. Das ICO ist verpflichtet, mit anderen europäischen und internationalen Partnern zusammenzuarbeiten, einschließlich Informationsaustausch, Hilfe bei Beschwerden und Zusammenarbeiten, um ein besseres Verständnis des Datenschutzes und der gemeinsamen Politiken zu generieren. Auf europäischer Ebene ist sie Mitglied des *Article 29 Working Party*, das aus 27 Vertreter der nationalen Datenschutzbehörde und Norwegen, Island, Liechtenstein und der „*European Data Protection Supervisor*" besteht. Das ICO avisiert auch jene, die Daten außerhalb der EU übermitteln wollen.[57]

---

[55] Der 2013-16 Plan kann auch online herunterladen werden; *'Information rights in the spotlight' ICO plan 2013-16, Final version 3.0.0*, ICO, 25 Februar 2013; http://www.ico.org.uk/about_us/plans_and_priorities/~/media/documents/library/Corporate/Detailed_specialist_guides/ico_corporate_plan_2013-16.ashx

[56] *Monitoring compliance*, ICO Webseite, online verfügbar; http://www.ico.org.uk/what_we_cover/monitoring_compliance

[57] *Can I send personal data overseas?,* ICO, online verfügbar; http://www.ico.org.uk/for_organisations/data_protection/overseas

bb) Behördenstruktur

Der "Information Commissioner" wird von der Königin berufen und ist gegenüber dem Parlament verantwortlich. Er/sie wird vom „Management Board" unterstützt. Die primäre Funktion des „Management Board" ist, den langfristigen strategischen Plan des „Commissioner" zu unterstützen und durchführen.[58] Die organisatorische Struktur besteht aus „directorates" und „departments", mit einem „Executive Team Member" für jedes „directorate" verantwortlich. Jedes Department besteht aus verschiedenen Teams. Der „Director of Corporate Services" ist für "Corporate Affairs, Finance, Information Technology, Information Governance and Organisational Development" verantwortlich. Der "Deputy Commissioner and Director of Freedom of Information (FOI)", ist, unter anderem, für die "Policy Delivery" verantwortlich. Der "Deputy Commissioner and Director of Data Protection" ist speziell für "Strategic Liason" verantwortlich. Letzlich ist der "Director of Operations" sehr wichtig und relevant für den Verbraucherschutz, weil er für „*Good Practice, Customer Contact, Complaints Resolution, Enforcement and the regional offices*" verantwortlich ist.[59]

Das "*Ministry of Justice*" ist das "*sponsoring department*" des ICOs innerhalb der Regierung. Das ICO hat formelle Vereinbarungen mit „*the National Archives, the Office of Fair Trading (OFT), the Parliamentary and Health Service Ombudsman's Office, the Financial Ombudsman Service, The Keeper of Public Records, as well as the Secretary of State for Constitutional Affairs*."[60] Es veröffentlicht "*Annual Reports*", die die Arbeit des vorherigen Jahres beschreiben und die Ziele für das nächste Jahr aufzeigen. Zum Beispiel wurde im Juni 2013 Folgendes veröffentlicht:

> … the report reflects on a year which saw the ICO impose civil monetary penalties of over £2.6 million on 23 data controllers and organisations for serious breaches of the Data Protection Act and Privacy and Electronic Communications Regulations. The ICO also played a key role in important national issues, including the post-legislative scrutiny of the Freedom of Information Act, the Leveson Inquiry and the proposed revision of the EU data protection regime.[61]

Das Hauptbüro findet sich in Winslow, Cheshire, aber es gibt drei regionale Büros in Nordirland, Schottland und Wales, die besonders wichtig sind, wenn die Verwaltungsstruktur oder Gesetze etwas unterschiedlich besagen. Das ICO enthält ein „*register of data controllers*" – die DPA 1998 verlangt von allen Datenverarbeitern eine Registrierung beim ICO (abgesehen von einigen Ausnahmen).[62] Eine Unterlassung dieser Pflicht stellt eine Straftat dar. Es gibt mehr als 370.000 Datenverarbeiter und das ICO veröffentlicht die Namen aller Datenverarbeiter und eine Beschreibung ihrer Arbeit. Das ICO besorgt auch die Beschwerden von Mitgliedern der Öffentlichkeit, darunter ungefähr 2.500 Informationsfreiheitbeschwerden („*freedom of information complaints*") pro Jahr – einige werden informell behandelt andere aber brauchen

---

[58] *Management Board*, ICO Webseite, online verfügbar; http://www.ico.org.uk/about_us/our_organisation/management_board

[59] *Ibid*

[60] Weitere Informationen zu diesen Vereinbaren können online gefunden werden; *Working with other bodies*, ICO Webseite; http://www.ico.org.uk/about_us/how_we_work/other_bodies

[61] *Annual Reports* sind auf der ICO Webseite verfügbar; http://www.ico.org.uk/about_us/performance/annual_reports

[62] Sections 19 and 17, *Data Protection Act 1998*

ein „*formal decision notice*“,[63] das weiter an die relevanten Organisationen oder Behörden geschickt wird. Das ICO bekommt auch ungefähr 5.000 formelle Beschwerden von Mitgliedern der Öffentlichkeit über persönlichen Daten pro Jahr.[64]

cc) Übersicht und Regelung des Markts

Das ICO kann einigermaßen neue Regelungen produzieren und veröffentlichen, wie den „*Data Sharing Code of Practice*“ von 2012.[65] Das ICO kann auch direkt in den Markt eingreifen Dies erfolgt durch ‚sanfte' Durchsetzung, Leitlinien und Beratung für die Datenverarbeiter wie auch für die Kunden und Verbraucher. Es gibt drei primäre Methoden, durch die das ICO der Markt sanft reguliert:

(1) “Audits” (Überprüfungen)

Diese freiwilligen Überprüfungen sind für große Organisationen, die wahrscheinlich ein ziemlich gutes Verständnis des Datenschutzrechts haben und selbst Politiken und Leitlinien haben, aber die gezielte Hilfe auch nützlich finden könnten. Das ICO gibt diesen Organisationen eine Bewertung, die Vorschläge und Kritiken über die Datenschutzpolitiken der Organisationen enthält.[66] In spezifischer Weise kann das ICO überprüfen, wie die Organisationen die *freedom of information requests* besorgen und Verbesserungen vorschlagen. Sie können danach (aber müssen nicht immer) ein „*follow up report*“ veröffentlichen.

(2) “Advisory Visits” (Beratungsbesuche)

Die Beratungsbesuche sind für mittelgroße oder kleine Organisationen, die ihre Pflichten und Verantwortungen z.T. schwer verstehen und somit hauptsächlich praktische Beratung brauchen. Dies erfolgt normalerweise in Form eines eintägigen Besuchs, bei welchem das ICO die Stärken und Schwächen der Organisationen identifiziert und einen kurzen Bericht dazu schreibt.[67]

(3) “Self Assessment” (Selbstbeurteilung)

Das ICO nutzt diese gezielten Selbstbeurteilungen, mit dem Zweck, bewährte Datenschutz-Verfahrensweise zu fördern, normalerweise für kleinere Organisationen. Der Fokus liegt somit auf Aufklärungskampagnen in Industrien und Schulen und der Förderung eines besseren Verständnisses des Datenschutzrechts.[68]

---

[63] *Decision notices*, ICO Webseite, online verfügbar; http://search.ico.org.uk/ico/search/decisionnotice

[64] *Handling complaints*, ICO Webseite, online verfügbar; http://www.ico.org.uk/what_we_cover/handling_complaints

[65] J Burn-Murdoch, “New code of practice to minimise privacy risks in anonymised data”, *The Guardian*, 21 November 2012, online verfügbar; http://www.theguardian.com/news/datablog/2012/nov/21/anonymised-data-protection-code-freedom-of-information Data sharing code of practice auch online verfügbar; http://www.ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

[66] *Audits*, ICO Webseite, online verfügbar; http://www.ico.org.uk/what_we_cover/audits_advisory_visits_and_self_assessments/audits

[67] *Advisory Visits*, ICO Webseite, online verfügbar; http://www.ico.org.uk/what_we_cover/audits_advisory_visits_and_self_assessments/advisory_visits

[68] *Self Assessments*, ICO Webseite, online verfügbar; http://www.ico.org.uk/what_we_cover/audits_advisory_visits_and_self_assessments/self_assessments

Das ICO bestellt auch Berichte und Forschung, um ein besseres Verständnis des Datenschutzes und der Informationsfreiheit zu entwickeln. Die Details der Berichte für das Parlament werden online auf der ICO-Webseite veröffentlicht.[69] Es analysiert auch die Ergebnisse öffentlichen Konsultationen, („*public consultations*") die auch online verfügbar sind.[70]

dd) Sanktionen und Durchsetzungsmechanismen

Es gibt eine Menge von Instrumenten, die das ICO nach dem "*Freedom of Information Act, Environmental Information Regulations, INSPIRE Regulations and associated codes of practice*" nutzen kann, um das Verhalten der Individuen und Organisationen, die persönliche Informationen sammeln, verarbeiten und speichern, zu ändern. Beispiele sind Strafverfahren, außerstrafrechtliche Durchsetzung und obligatorische Überprüfungen. Der/die *Information Commissioner* darf auch Geldstrafen an *data controllers* verhängen. Das ICO kann in extremen Fällen auch das Parlament informieren, wenn ein großes Datenschutzrisiko besteht. Eine Liste die Befugnisse des ICO findet man online:

> The main options are:
> - serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
> - issue undertakings committing an organisation to a particular course of action in order to improve its compliance;
> - serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
> - conduct consensual assessments (audits) to check organisations are complying;
> - serve assessment notices to conduct compulsory audits to assess whether organisations processing of personal data follows good practice (data protection only);
> - issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010, or serious breaches of the Privacy and Electronic Communications Regulations occurring on or after 26 May 2011;
> - prosecute those who commit criminal offences under the Act; and
> - report to Parliament on data protection issues of concern.[71]

Zulassungen der Berufungen werden von einem "*First–tier Tribunal (Information Rights), part of the General Regulatory Chamber (GRC)*" entschieden, das die Berufungen gegen "*enforcement notices*", "*decision notices*" und "*information notices*", die vom *Information Commissioner* stammen, hört. Das GRC hat vormals verschiedene *tribunals* zusammengebracht. Das ICO ist auch sehr proaktiv bezüglich Beschwerden im Informationsrecht wie „*spam texting, marketing calls and cookies.*"[72]

Das ICO hat die Befugnis, Geldstrafen bis zu £500.000 zu verhängen, nach den PECR im Mai 2011 bekommen und zum ersten Mal gegen unerwünschte Direktmarketing-Anrufe in Novem-

[69] *Research and Reports*, ICO Webseite, online verfügbar; http://www.ico.org.uk/about_us/research

[70] *Consultations*, ICO Webseite, online verfügbar; http://www.ico.org.uk/about_us/consultations

[71] Liste aus; *Taking action: data protection and privacy and electronic communications*, ICO Webseite, online verfügbar; http://www.ico.org.uk/what_we_cover/taking_action/dp_pecr

[72] *What action have we taken?*, ICO Webseite, online verfügbar; http://www.ico.org.uk/enforcement/action

ber 2012 i.H.v. £440,000 gegen Christopher Niebel und Gary McNeish wegen „*millions of unlawful spam texts*“ eingesetzt.[73] Weitere Beispiele dieser strafrechtlichen Sanktion sind auch online verfügbar:[74]

> **8 October 2013**
> A pay day loans company based in London and its director have been prosecuted after failing to register that the business was processing personal information. Hamed Shabani, the sole director of First Financial, was convicted under section 61 of the Data Protection Act at City of London Magistrates Court.[75]
> **25 September 2013**
> A former Barclays Bank employee has been fined after illegally accessing the details of a customer's account. In one case the employee, Jennifer Addo, found out the number of children the customer had and passed the details to the customer's then partner, who was a friend of Ms Addo.[76]
> **15 August 2013**
> A probation officer who revealed a domestic abuse victim's new address to the alleged perpetrator has been fined £150 following a prosecution bought by the ICO.[77]
> **23 May 2013**
> A former manager of a health service based at a council-run leisure centre in Southampton has been prosecuted under section 55 of the Data Protection Act for unlawfully obtaining sensitive medical information relating to over 2,000 people.[78]

ee) Selbstständigkeit und Pflichten der Behörde

Das ICO ist relativ selbstständig und arbeitet eher ‚mit' der Regierung als ‚für' die Regierung. Es setzt die Gesetze und Regelungen durch, schafft aber auch neue Regelungen und Leitlinien und avisiert das Parlament. Es darf auf Politik-Ebene, aber auch mit individuellen Beschwerden und Fällen arbeiten. Es ist nicht nur eine informationelle Behörde, sondern hat auch Durchsetzungsmöglichkeiten und weitere Befugnisse – also kann das ICO sich mit kleineren Fällen beschäftigen oder auch größere strafrechtliche und zivilrechtliche Verfolgungen gegen größere Industrie-Akteure durchführen. Damit es nicht alle Fälle individuell bearbeiten muss, veröffentlicht es Leitlinien und fördert Selbsturteilungen.

---

[73] “ICO serves first fines for unlawful spam text messages by marketing firm”, *Out-Law*, Pinsent Masons, 30 November 2012; online verfügbar; http://www.out-law.com/en/articles/2012/november/ico-serves-first-fines-for-unlawful-spam-text-messages-by-marketing-firm/

[74] Siehe *Prosecutions*, ICO Webseite, online verfügbar; http://www.ico.org.uk/enforcement/prosecutions

[75] *Pay day loans company and its director prosecuted for failing to register, News release: 8 October 2013*, ICO Webseite, online verfügbar; http://www.ico.org.uk/news/latest_news/2013/pay-day-loans-company-and-its-director-prosecuted-for-failing-to-register-08102013

[76] *Barclays Bank employee prosecuted for illegally accessing customer's account, News release: 25 September 2013*, ICO Webseite, online verfügbar; http://www.ico.org.uk/news/latest_news/2013/barclays-bank-employee-prosecuted-for-illegally-accessing-customer-account-25093013

[77] *Probation officer prosecuted for leaking victim's details to alleged culprit, News release: 15 August 2013*, ICO Webseite, online verfügbar; http://www.ico.org.uk/news/latest_news/2013/probation-officer-prosecuted-for-leaking-victims-details-to-alleged-culprit-15082013

[78] *Leisure centre employee prosecuted for unlawfully obtaining health information of over 2,000 people, News release: 23 May 2013*, ICO Webseite, online verfügbar; http://www.ico.org.uk/news/latest_news/2013/leisure-centre-employee-prosecuted-for-unlawfully-obtaining-health-information-23052013

Das ICO arbeitet eng mit ausländischen, im Besonderen mit europäischen, Behörden zusammen, um grenzüberschreitende Probleme zu lösen. Es kontrolliert dabei die Übermittlungen von Daten, welche die EU verlassen. Wenn das Zielland dann keine angemessenen Datenschutzregeln hätte, könnte das ICO eingreifen, soweit es das britische Recht erlaubt.

b. The Office of Fair Trading (OFT)

aa) Schwerpunkt und Ziele der Behörde

Das "*Office of Fair Trading (OFT)*" ist eine der wichtigsten Behörden in Großbritannien im Bereich des Lauterkeitsrechts und auch teilweise im Bereich des Wettbewerbsrechts und besonders im Bereich von Kaufverträgen und Dienstleistungsverträgen mit Verbrauchern. Es wurde ursprünglich nach dem „*Fair Trading Act 1973*" gegründet, aber jetzt auf Basis des „*Enterprise Act 2002*" verbessert. Es wurde auch „*CPC enforcer*" nach *Part 8* des *Enterprise Act´s*, spezifisch *Section 213(5A),* genannt – ein EU-basierter Rechtsdurchsetzer des Verbraucherrechts nach "*EU Regulation 2006/2004 on Consumer Protection Cooperation*".[79] Die Befugnisse des OFT wurde von den „*Consumer Protection from Unfair Trading Regulations 2008 (the CPRs)*" auch erweitert. Es versucht, sowohl Verbraucherschutz als auch Wettbewerbsrecht durchzusetzen und zu verbessern. Das Ziel des OFT ist es, den Markt zu beaufsichtigen und darauf zu achten, dass er wettbewerbsfähig und frei von unlauteren Handlungen wie „*rogue trading*", „*scams*" und „*cartels*" ist. Das OFT analysiert den Markt, setzt Verbraucherrecht und Wettbewerbsrecht durch, kontrolliert Unternehmenszusammenschlüsse;, fördert Lizenzierung und Übersicht sowie den Erhalt von Informationen und etabliert Bildungsprogramme und Kampagnen für Verbraucher und Firmen.

> ***Mission***
> *The OFT's mission is to make markets work well for consumers. Markets work well when businesses are in open, fair and vigorous competition with each other for the consumer's custom. Our job is to make sure that consumers have as much choice as possible across all the different sectors of the marketplace. When consumers have choice they have genuine and enduring power.*[80]

Das OFT beaufsichtigt, ob die Märkte zugunsten der Kunden und Verbraucher funktionieren. Wenn nötig, können diese Analysen zu „*market investigation references*" zur „*Competition Commission (CC)*" geleitet werden und so zu Durchsetzungsmaßnahmen, zu verbraucherorientierten Werbe-, Informations- und Aufklärungskampagnen, oder zu Vorschlägen für die Regierung führen. Es fördert Selbstregulierung, kann aber auch entschlossen gegen „*hardcore or flagrant offenders*" handeln.[81] Das OFT hat keine spezifische „digitale Welt"-Abteilung als Schutzgebiet, aber alles was mit der digitalen Welt zu tun hat, kann normalerweise zu schon existierenden Industrie-Kategorien zugeordnet werden und fällt somit in den Schutzbereich. Trotzdem gibt es viele aktuelle Fragen und Probleme, die das OFT bearbeitet, welche bestimmt mit E-Commerce und digitalen Waren zu tun haben, besonders in einem hochtechnologischen Markt, der von großen internationalen Firmen beherrscht ist.

---

[79] *The OFT's coordination role*, OFT Webseite, online verfügbar; http://www.oft.gov.uk/about-the-oft/legal-powers/legal/enterprise-act/part8/role#.UnEMunCkq68

[80] *What we do*, OFT Webseite, online verfügbar; http://www.oft.gov.uk/about-the-oft/what/;jsessionid=7CC88776D0BF5410E3ED6B8CBB2406A4#.UmZ-03Cnq68

[81] *Ibid*

Allerdings werden sich die genauen Pflichten und Befugnisse des OFT bald ändern, weil das „*Department for Business Innovation and Skills (BIS)*“ bekanntgegeben hat, dass in Großbritannien wegen Reformen Verbraucherschutz- und Wettbewerbsschemata und damit das OFT und CC am 1. April 2014 abgeschafft werden. Ihre Befugnisse werden in einer neuen Behörde, dem „*Competition and Markets Authority (CMA)*“, das nach dem „*Enterprise and Regulatory Reform Act 2013 (ERRA13)*“[82] gegründet wurde, zusammengefügt.[83] Trotzdem hat die Regierung zugesagt, dass die entscheidenden verbraucherrechtlichen Befugnisse und Pflichten noch immer wichtig für die neue Behörde wären;

> … the Government recognises and values the close relationship between competition problems and consumer activities and that the CMA “will therefore have the OFT and Competition Commission’s full competition toolkit and consumer protection enforcement powers. It will have the power to tackle practices and market conditions that make it difficult for consumers to exercise choice in an otherwise competitive market.”[84]

Die Regierung will dabei weiterhin ein “*strong, sustainable and balanced growth that is more evenly shared across the country and between industries*”, fördern, besonders wenn diese Industrien auf dem “*Plan for Growth*” vom Budget-2011 basieren. Das OFT hat auch binnen 40 Tagen ein "*invitation to comment*" für interessierte Individuen und Parteien veröffentlicht.

bb) Behördenstruktur

Das OFT ist eine gemeinnützige non-ministerielle staatliche Behörde in Großbritannien. Der *Enterprise Act 2002* hat sowohl das OFT, als auch “*all UK trading standards departments and the Department of Enterprise, Trade and Investment of Northern Ireland*” als Durchsetzungsbehörden („*General Enforcers*”)[85] etabliert. Der „*Secretary of State*“ darf auch andere *enforcers* benennen, wie z.B. der *Information Commissioner* (s.o.) und der *„Director General of Telecommunications*“. Ergo gibt es oft eine Überlappung zwischen Verantwortungen des OFT und anderer noch speziellerer Behörden, die gelegentlich zusammenarbeiten müssen.

Der Vorstand („*Board*”) enthält den Vorsitzender („*Chairman*”), den Geschäftsführer („*Chief Executive*“), zwei Exekutivdirektoren („*executive directors*“) und sieben nicht leitende Mitglieder („*non-executive members*“).[86] Das OFT ist gegenüber dem Volk und dem Parlament sowohl in Westminster als auch durch Untersuchungen („*investigations by select committees*”) verantwortlich. Das OFT muss auch den Jahresabschluss am „National Audit Office“ abgeben um ihre Ressourcen zu rechtfertigen. Die Entscheidungen des OFT zum Wettbewerbsrecht

[82] „OFT + CC = CMA“, Field Fischer Waterhouse, 19 Juli 2013; online verfügbar; http://www.ffw.com/publications/all/alerts/cma.aspx

[83] "Press Release: Chief Executive Designate appointed to the Competition and Markets Authority". *Department for Business, Innovation and Skills*, 8 January 2013; online verfügbar; https://www.gov.uk/government/news/press-release-chief-executive-designate-appointed-to-the-competition-and-markets-authority

[84] *Ibid*

[85] Section 213, *Enterprise Act 2002*

[86] *OFT structure*, OFT Webseite, online verfügbar; http://www.oft.gov.uk/about-the-oft/oft-structure/#.UmZ6R3Cnq68 das Organigramm ist auch online verfügbar; http://www.oft.gov.uk/shared_oft/about_oft/Organisation-chart.pdf

sind auch vor dem „*specialist Competition Appeal Tribunal*“, (ein selbstständiges Gericht nach dem *Enterprise Act* gegründet)[87] anfechtbar.

Die Struktur des OFT wird eher nach Märkten als nach dem Gesetz aufgebaut, unter anderem mit einer „*Services, Infrastructure and Public Markets*“ Gruppe und einer „*Goods and Consumers*“ Gruppe.[88] Die verschiedenen, spezialisierten Gruppen arbeiten eng miteinander zusammen, wodurch das OFT den ganzen Markt leichten überwachen kann. Das OFT benutzt das Instrument der verbraucherrechtlichen und wettbewerbsrechtlichen Durchsetzung sowie Marktstudien, Bildung und Kommunikation in verschieden Kombinationen, um die Ziele zu erreichen. Es versucht, eine umfangsreiche Überwachung sowohl des Verbraucherrechts als auch des Wettbewerbsrechts zu garantieren, weil gerade das Wettbewerbsrecht so wesentlich für einen wettbewerbsfähigen und verbraucherfreundlichen Markt ist.[89]
Bevor sie das OFT direkt kontaktieren, werden Verbraucher informiert, dass das OFT viele häufige gestellte Fragen im Internet veröffentlicht hat. Deshalb wird ihnen empfohlen, zuerst die FAQ-Seite zu lesen. Das OFT informiert den Verbrauchern auch, dass der „*Citizens Advice consumer service*“ eine kostenlose, vertrauliche und objektive Beratung online unter www.adviceguide.org.uk anbietet, oder empfiehlt auch, das „*Citizens Advice consumer helpline*“ unter der Nummer 08454 04 05 06 anzurufen.[90]

Das Hauptbüro des OFT findet man in der *Fleet Street* in der Nähe der Blackfriarstreet Station in London. Andere Behörden und Organisationen, die vom *Secretary of State* gewählt werden, können nach *Section 11* des *Enterprise Act´*s eine „*Super Complaint*“ vor dem OFT vorbringen wenn irgendeine Eigenschaft eines Markts für Waren oder Dienstleistungen gefährlich verbraucherfeindlich sein könnte.[91] Die Liste dieser Behörden umfasst:

The Campaign for Real Ale Limited (CAMRA)
The Consumer Council for Water
The Consumers' Association (trading as "Which?")
The General Consumer Council for Northern Ireland (GCCNI)
The National Association of Citizens Advice Bureaux (NACAB)
The National Consumer Council (trading as "Consumer Focus")

Das OFT arbeitet auch in Kooperation mit lokalen, nationalen und internationalen Behörden wie zum Beispiel “*the Competition Commission, the Department of Health Cooperation and*

[87] *Accountability,* OFT Webseite, online verfügbar; http://www.oft.gov.uk/about-the-oft/oft-structure/accountability/#.UmZ6ZXCnq68

[88] Die volle Liste enthält; *Goods and Consumer; Cartels and Criminal Enforcement; Services, Infrastructure and Public Markets; Mergers; Pipeline and Performance; Consumer Credit and Anti-Money Laundering; Finance and Enquiries; Human Resources; Business Services; General Counsel's Office; Communications; Chief Economist; Competition Policy; Executive Office; Procedural Adjudication*. Mehr Information dazu ist auch online verfügbar; http://www.oft.gov.uk/about-the-oft/oft-structure/structure/#.UmZ6S3Cnq68

[89] Why is competition policy important for consumers?, Europäische Kommission Webseite, online verfügbar; http://ec.europa.eu/competition/consumers/why_en.html ; siehe auch P Klemperer, “Competition when Consumers have Switching Costs: An Overview with Applications to Industrial Organisation, Macroeconomics and International Trade”, *Review of Economic Studies,* 62, 515-539, (1995)

[90] *Contact us*, OFT Webseite, online verfügbar; http://www.oft.gov.uk/contactus#.UmZ3mHCnq68

[91] *Super-complaints,* OFT Webseite, online verfügbar; http://www.oft.gov.uk/OFTwork/markets-work/super-complaints/#.UnoRYXCkq68

Competition Panel, the Financial Conduct Authority, the Trading Standards Services",[92] und ist auch Mitglied des "*European Competition Network (ECN)*", das das EU-Recht bezüglich der Artikeln 101 und 102 AEUV und EU-Wettbewerbsregeln durchsetzt.[93] Das OFT arbeitet auch mit dem „*International Competition Network (ICN), the International Consumer Protection Enforcement Network (ICPEN), and the OECD*".

cc) Übersicht und Regelung des Markts

Eine der wichtigsten Pflichten des OFT ist es, genauso wie es vormals beim ICO war, die Industrie-Akteure zu informieren und zu unterrichten, sodass diese als wichtigste Unternehmen und Organisationen ihre eigenen Pflichten verstehen und idealerweise wettbewerbsfähig und fair ohne großes Eingreifen des OFT arbeiten können. *Section 229(1)* des *Enterprise Act 2002* verpflichtet das OFT, Informationen über die Vorschriften des *Enterprise Act Part 8* zu veröffentlichen und klarzustellen wie diese Vorschriften befolgt werden sollen; "*how the OFT expects such provisions to operate*".[94] *Subsection 2* regelt ferner, dass das OFT diese Informationen regelmäßig aktualisieren muss.

Basiert auf den erweiterten Befugnissen aus dem *Enterprise Act 2002*, recherchiert das OFT, wie genau die verschiedenen Märkte funktionieren, um ein besseres Verständnis und weitere Verbesserungen für alle Märkte zu entwickeln. So kann es einen spezifischen Markt detailliert erforschen oder auch die Wirkung der allgemeinen Gesetze und Leitlinien in allen Märkte und Industrien analysieren. Die Ergebnisse solcher Recherchen werden danach veröffentlicht und helfen dem OFT, Pläne und Maßnahmen für einen besseren Verbraucherschutz in diesen Gebieten zu entwickeln. Dies klingt pauschal ziemlich abstrakt, jedoch wurde aufgrund der häufigen Recherche und der vielen Berichte des OFT eine fast vollständige Erfassung aller neuen technologischen Entwicklungen ermöglicht– besonders im Bereich des digitalen Urheberrechts und der Telekommunikationsindustrie und der Internetverbindungen. Das OFT kann, sowohl für spezielle Industrien oder Bereiche wie auch allgemein, stärkere Regelungen oder auch reine Informationskampagnen für Verbraucher vorschlagen. Es kann auch entscheiden, keine Eingriffe vorzuschlagen, muss dann aber klar und öffentlich erklären, warum keine Maßnahmen benötigt werden. Das OFT muss auch die Regeln der Behörden, die vor ein Gericht gehen dürfen, überprüfen und den „*Lord Chancellor*" informieren, wenn diese Regeln wettbewerbsrechtlich oder verbraucherrechtlich problematisch sein könnten.[95]

Das OFT veröffentlicht jedes Jahr einen ausführlichen Geschäftsbericht, welcher online zu finden ist und den allgemeinen, aktuellen Stand des Verbraucherschutzes und der Durchsetzungseffektivität, eine Liste der durchgeführten Maßnahmen, eine Liste der Strafverfolgungen sowie eine Marktanalyse enthält. Das OFT veröffentlicht gemäß *Section 3(1)* des *Enterprise Act´s 2002*, auch einen „*Annual Plan*", der die Hauptziele und Prioritäten der Behörde erklärt.

---

[92] *Partnership working*, OFT Webseite, online verfügbar; http://www.oft.gov.uk/about-the-oft/partnership-working/#.UmaCw3Cnq6-

[93] *International work*, OFT Webseite, online verfügbar; http://www.oft.gov.uk/about-the-oft/partnership-working/partnership-working-info/international/#.UmaCEnCnq68

[94] G Woodroffe, R Lowe, *Woodroofe & Lowe's Consumer Law and Practice*, (8 Ed.), Sweet & Maxwell: London, (2010), para 17.19

[95] Siehe *Application by the Bar Standards Board to Amend its Training Regulations : A report by the Office of Fair Trading to the Ministry of Justice on the likely competition effects of the Bar Standards Board modifying Regulation 25 of the Bar Training Regulations under Section 29 and Schedule 4 of the Courts and Legal Services Act 1990*, OFT, 2009, online verfügbar; http://www.oft.gov.uk/shared_oft/reports/professional_bodies/oft1086.pdf

Es hat jetzt den "*2013-14 Annual Plan*" und dazu eine Zusammenfassung der Konsultation-Reaktionen und deren Umsetzung veröffentlicht, was auch online verfügbar ist.[96] Dies war auch der letzte *Annual Plan* vor dem „*CMA merger*".

Das OFT soll sowohl Übersicht als auch Eingriffe nutzen, um die Märkte aktiv zu regulieren, besonders wenn eine Beeinträchtigung der Wettbewerbsfähigkeit droht. Aktuell hat das OFT beispielsweise Googles $1mrd Übernahme des "*travel mapping service Waze*" untersucht, weil diese wettbewerbsfeindlich sein könnte und die „*Federal Trade Commission (FTC)*" auch eine ähnliche Untersuchung vorgenommen hat.[97]

dd) Sanktionen und Durchsetzungsmechanismen[98]

Die primären Waffen des OFT sind Untersuchungen und Vorschläge, nicht aber eine starke Durchsetzung. Wenn eine solche benötigt wird, schickt das OFT den Fall normalerweise an die *Competition Commission (CC)* als „*market investigation reference*", nach *Part 4, Chapter 1 Enterprise Act 2002*,[99] oder direkt an die Gerichte weiter. Das OFT wird ziemlich oft wegen Ineffektivität kritisiert. Teils wird argumentiert, dass zu viele Untersuchungen zu keinen praktischen Ergebnissen oder Maßnahmen führen, vor allem im Vergleich zu ähnlichen Behörden in Amerika (*United States Department of Justice Antitrust Division*) und Europa (*Directorate-General for Competition*).[100] Das "*Public Accounts Committee*" kritisiert andererseits die Behörde, neue Märkte nicht richtig zu regulieren oder überhaupt zu verstehen und passiv auf die Beschwerden zu warten. [101]

Trotzdem kann das OFT in extremen Fällen stärkere Maßnahmen einsetzen oder auch selbstständiger arbeiten. Nach *Section 154* darf das OFT in besonderen Fällen, in denen es eine starke Verhinderung des Wettbewerbes und eine Unzuträglichkeit für Verbraucher gibt, anstatt einer Weitergabe des Problems an eine andere Behörde (nach *Section 121*) auch eine Zusage („*undertaking*") der angreifenden Partei akzeptieren.[102] Die Annahme einer Zusage bedeutet, dass es zunächst keine *market investigation reference* gibt,[103] diese jedoch nachträglich vorgenommen werden kann, wenn die Zusage gebrochen werden würde, oder die angegebenen Informationen falsch wären. Dabei obliegt es der Verantwortung des OFTs, die Einhaltung der Zusage zu beobachten.[104]

---

[96] *Annual Plan*, OFT Webseite, online verfügbar; http://www.oft.gov.uk/about-the-oft/annual-plan-and-report/annual/#.UmaDIXCnq68

[97] C Arthur, "Google acquisition of Waze traffic app sparks OFT inquiry", *The Guardian*, 27 August 2013; online verfügbar; http://www.theguardian.com/technology/2013/aug/27/google-waze-app-sparks-oft-inquiry

[98] *How we deal with Complaints: A guide for public authorities*, ICO, 9 September 2011; downloadbare PDF; http://www.ico.org.uk/about_us/~/media/documents/library/Corporate/Practical_application/complaints_guide_for_public_authorities.ashx

[99] Sections 131-138, *Enterprise Act 2002*

[100] L Armistead, "OFT 'ineffective and timid' in tackling payday lenders", *The Telegraph*, 31 Mai 2013; online verfügbar; http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/10089401/OFT-ineffective-and-timid-in-tackling-payday-lenders.html

[101] *Ibid*

[102] Section 154(2), *Enterprise Act 2002*

[103] Section 156(2), *Enterprise Act 2002*

[104] Section 162, *Enterprise Act 2002*

Ein Mitglied kann erstens nach dem "*Competition Act 1998*"[105] eine Geldstrafe in Höhe von bis zu 10% seines weltweiten Absatz bekommen. Zweitens ist es nach dem *Enterprise Act 2002* auch eine Straftat, Mitglied eines besonders starken Kartells zu sein. Die maximale Strafe ist eine fünfjährige Freiheitsstrafe und/oder eine Geldstrafe mit unbegrenztem Höchstwert. Wenn eine Firma ein Kartell beenden will und das OFT über das Kartell informiert, ist nach dem *Enterprise Act* eine Straffreiheit oder eine Reduktion der Geldstrafe möglich.[106]

Die Mehrheit der Durchsetzungsmechanismen des OFT sind im *Part 8* des *Enterprise Act´*s zu finden; genauer unter dem Begriff *enforcement order* für Verbraucherrecht. *Sections 210 (3)* und *(4)* definieren genau, was ein 'Verbraucher' ist und was die Voraussetzungen für beide Parteien sind. Eine *enforcement order* darf benutzt werden, wenn der Täter gegen nationale oder europäische Gesetze verstoßen hat.[107] Nur die Anwendung der *enforcement order* stammt von der Behörde, der Rest wird vom Gericht durchgeführt, sofern dieses feststellt, dass eine Rechtsverletzung vorlag oder dass eine große Chance besteht, dass eine Rechtsverletzung eintreten können wird.[108] *Section 217* berechtigt das Gericht, eine *enforcement order* durchzusetzen. Bei Nichtbefolgung durch das Unternehmen liegt eine Missachtung des Gerichts vor, was zu einer Freiheitsstrafe führen kann.[109]

Section 224 berechtigt das OFT, im Rahmen der Bearbeitung der Pflichten des OFT nach *Part 8 Enterprise Act 2002* ein Informationsverlangen („*notice requiring the provision of information*")[110] an ein Unternehmen zu senden. Das OFT kann auch ein Gericht anrufen, einen Betriebsleiter zu disqualifizieren, wenn das Unternehmen das Wettbewerbsrecht verletzt hat und sein Verhalten die Qualifikation ungeeignet erscheinen lässt. Das OFT kann auch in Kooperation mit dem „*Serious Fraud Office"* und dem „*Lord Advocate in Scotland"* Individuen strafrechtlich verfolgen. Es ist dabei in beiden Fällen eine gerichtliche Berufung möglich.[111] Viele dieser Maßnahmen und Befugnisse sollen bald dem CMA übergeben werden, dann aber mit stärkerem Fokus auf großen, systematischen Fällen und damit auf einem möglichen Scheitern des Systems und nicht auf kleineren Beschwerden:

---

[105] Siehe auch Art 101 AEUV

[106] *Cartels*, OFT Webseite, online verfügbar; http://www.oft.gov.uk/about-the-oft/legal-powers/Cartels/#.UmaFoXCnq68

[107] Section 215(1), *Enterprise Act 2002*

[108] Section 217, *Enterprise Act 2002*

[109] G Woodroffe, R Lowe, *Woodroofe & Lowe's Consumer Law and Practice*, (8 Ed.), Sweet & Maxwell: London, (2010), para 17.18

[110] Section 224, *Enterprise Act 2002*, OFT;

(1)The OFT may for any of the purposes mentioned in subsection (2) give notice to any person requiring the person to provide it with the information specified in the notice.

(2)The purposes are—

(a)to enable the OFT to exercise or to consider whether to exercise any function it has under this Part;

(b)to enable a designated enforcer to which section 225 does not apply to consider whether to exercise any function it has under this Part;

(c)to enable a Community enforcer to consider whether to exercise any function it has under this Part;

(d)to ascertain whether a person has complied with or is complying with an enforcement order, an interim enforcement order or an undertaking given under section 217(9), 218(10) or 219.

[111] *Accountability*, OFT Webseite, online verfügbar; http://www.oft.gov.uk/about-the-oft/oft-structure/accountability/#.UmZ6ZXCnq68

> Following changes to the consumer protection regime introduced by Government in April 2013, local authority Trading Standards Services have a greater role in the enforcement of consumer protection law at national level. The OFT retains (and from April 2014 the new Competition Markets Authority will inherit) all of its previous consumer enforcement powers but will now tend to use those powers where breaches of consumer protection law point to systemic failures in a market. This means cases will more often be taken against a number of firms in a market, rather than cases against individual firms, unless changing the behaviour of one firm would set a precedent or have other market-wide implications.[112]

Momentan funktioniert das OFT auch als Durchsetzer der „*Unfair Terms in Consumer Contracts Regulations 1999*“, aber diese Befugnisse werden mit der „*Trading Standards Services*“ geteilt. Weitere Beispiele der strafrechtlichen Durchsetzungsmaßnahmen gab es zwischen September 2009 und Januar 2010, als das OFT Strafverfolgungen gegen eine Menge von Individuen, die mit einem widerrechtlichen Pyramidensystem verbunden waren, betrieb. Die Informationszugang hierzu ist aber beschränkt, weil die Verfahren noch laufen.[113] Strafverfolgungen werden normalerweise von den “*local weights and measurements authorities in England and Wales*” geführt. Falls diese aber solch relevante Verfolgungen beginnen, müssen sie das OFT informieren und eine Zusammenfassung des Beweises abgeben.[114]

ee) Selbstständigkeit und Pflichten der Behörde

Die non-ministerielle Natur des OFT erlaubt ihm eine große Selbstständigkeit, besonders bei der Realisierung von Politiken, aber es muss die Befugnisse der relevanten Gesetze und Regulierungen rechtfertigen. Zum Beispiel nach *Section 229*: Dort geregelt ist die Pflicht, Form und Methode der Informationen und der Veröffentlichung vom OFT bezüglich der Wirkung des *Part 8* des *2002 Act*, sagt *Section 229(4)*besonders zu wählen (“*Advice or information published by the OFT under this section is to be published in such form and in such manner as it considers appropriate*.”).

Die *Super Complaints* nach *Section 11(2)*, müssen innerhalb von 90 Tagen beantwortet werden. Dabei zu nennen sind eine Erklärung, wie genau die Beschwerde behandelt wird und ob das OFT Maßnahmen einsetzen wird und, falls ja, so ist auch eine genaue Beschreibung der Maßnahmen nötig. *Subsection (3)* erklärt auch, dass das OFT eine Begründung für diese Entscheidungen geben muss. *Section 210*, welche von Durchsetzungsmaßnahmen handelt, erklärt in *subsection (5),* dass es für eine innerstaatliche Verletzung irrelevant ist, ob die Unternehmen oder Individuen einen Geschäftssitz in Großbritannien haben.(“*For the purposes of a domestic infringement it is immaterial whether a person supplying goods or services has a place of business in the United Kingdom*”).

c. The Office of Communications (Ofcom)

---

[112] *Relevant Legislation*, OFT Webseite; http://www.oft.gov.uk/about-the-oft/legal-powers/legal/#.UmaFlnCnq68

[113] *Prosecution of a number of individuals involved in an alleged unlawful pyramid scheme, Case reference: CE9062/08, Start date: September 2009, Next milestone: Trial ongoing at Bristol Crown Court*, OFT Webseite, online verfügbar; http://www.oft.gov.uk/OFTwork/consumer-enforcement/consumer-enforcement-current/pyramid/#.UmaGdnCnq68

[114] Section 230, *Enterprise Act 2002*

aa) Schwerpunkt und Ziel der Behörde

"*The Office of Communications*", oder "Ofcom", ist ein Beispiel der sehr fachspezifischen Natur der Behörden in Großbritannien, die für Verbraucherrecht in der digitalen Welt verantwortlich sind. Ofcom ist die staatlich-anerkannte regulatorische und wettbewerbsrechtliche Behörde des Telekommunikationssektors, welche verantwortlich für Rundfunk, Telekommunikation und Post ist. Besonders im Telekommunikationssektor reguliert Ofcom Verbraucher- und Datenschutzfragen, dabei ausdrücklich die Probleme der Urheberrechtsverletzungen und der illegalen Downloads. Jedoch können auch viele andere Aspekte der digitalen Welt für Ofcom relevant sein, weil Ofcom im Bereich der IDA-Kunden,Verhältnisse aufgrund eines Teils ihrer Überwachungspflichten aus dem Telekommunikationssektor viel Macht innehat. Ofcom hat eine gesetzliche Pflicht, die Interessen der Bürger und Verbraucher zu fördern und die Verbraucher vor gefährlichen Handlungen oder Inhalten zu schützen.

Ofcom wurde ursprünglich nach dem „*Office of Communications Act 2002*" gegründet, hat aber die volle Befugnis vom „*Communications Act 2003*" bekommen. Die Gründung der Ofcom wurde in der Thronrede im britischen Parlament im Juni 2001 angekündigt. Diese neue Behörde wurde als „super-regulator" gesehen und übernahm die Verantwortlichkeiten vieler verschiedener kleinerer Behörden. Dies hatte auch damit zu tun, dass aufgrund der zunehmenden Digitalisierung verschiedene Telekommunikationsmethoden mehr und mehr zusammenlaufen.[115] Ofcom hat am 29. Dezember 2003 die Verantwortlichkeiten der vorherigen; „*Broadcasting Standards Commission*"; „*Independent Television Commission*"; „*Office of Telecommunications (Oftel)*"; „*Radio Authority*"; und „*Radiocommunications Agency*" zu übernehmen.

Die Hauptpflichten von Ofcom werden nach *Section 3(1) Communications Act 2003* dargelegt. Sie fördern die Verbraucherinteressen im Bereich des Telekommunikationsmarktes und anderer relevanter Märkte, wenn nötig durch Wettberwerbsunterstützung. Eine der wichtigsten, und für die digitale Welt relevantesten, Pflichten ist zu gewährleisten, dass Großbritannien eine Vielzahl von elektronischen Kommunikationsdienstleistungen, inklusive schnelllaufenden Dienstleistungen wie Broadband, hat.[116] Sie lizenzieren auch alle Fernseh- und Radio-Dienstleistungen in Großbritannien. Die Sender müssen auch die Lizenzbestimmungen befolgen, denn Ofcom kann bei Nichtbefolgen der Bestimmungen die Genehmigung revozieren. Ofcom veröffentlicht auch einen „*Broadcasting Code*", dem alle Sender folgen müssen.[117]

Ofcom wird jedoch relativ oft kritisiert: Einerseits von der Telekommunikationsindustrie, weil sie zu streng oder vollmachtsüberschreitend handle; anderseits von der Öffentlichkeit oder dem Parlament, weil sie nicht streng genug seien oder mit der Telekommunikationsindustrie kollidieren würden. Am 1. Februar hat Ofcom eine interne Überprüfung abgeschlossen, um ihren finanziellen Aufwand stark zu reduzieren. Im Juli 2009 hat David Cameron gewarnt, dass er Ofcom zugleich mit anderen "*quangos*" schließen wolle, wenn das *Conservative Party* zur Macht käme. "*Ofcom, as we know it, will cease to exist*".[118] Trotzdem hat der *Conservative*

[115] "Queen announces media shake-up", *BBC News*, 20 Juni 2001; online verfügbar; http://news.bbc.co.uk/2/hi/entertainment/1398580.stm

[116] *What is Ofcom?*, Ofcom Webseite, online verfügbar; http://www.ofcom.org.uk/about/what-is-ofcom/

[117] *Broadcasting*, Ofcom Webseite, online verfügbar; http://stakeholders.ofcom.org.uk/broadcasting/

[118] L Holmwood, "Ofcom hits back at David Cameron", *The Guardian*, 6 Juli 2009; online verfügbar; http://www.theguardian.com/media/2009/jul/06/ofcom-david-cameron

Regierung Ofcom nicht so stark entmachtet und die Befugnisse nur teilweise nach dem „*Public Bodies Act 2011*“ abgeschwächt.[119]

Ofcom veröffentlicht jedes Jahr einen “Annual Plan”, der aktuellste für 2013/14 ist online abrufbar und intendiert, die Verbraucher besser zu informieren, Frequenzspektren besser zu regulieren und effizienter zu nutzen, die Politiken in diesem Bereich zusammen mit dem Parlament zu organisieren, und dies dabei transparent, fair und konsultativ zu realisieren:

> We will work for consumers and citizens by promoting effective competition, informed choice and the opportunity to participate in a wide range of communications services, including post. We will secure the optimal use of spectrum, through market mechanisms where possible and regulatory action where necessary. We will provide proportionate protection for consumers and help maintain audiences' confidence in broadcast content. We will contribute to public policy defined by Parliament, including high quality public service broadcasting and plurality of media ownership. To achieve these aims, we will be consultative, transparent and proportionate. We will be informed through high quality research and information, which we will share widely. We will be mindful of the diversity of the UK and its nations. We will aim to be innovative, responsive and effective in everything we do.[120]

bb) Behördenstruktur

Die durch die interne Überprüfung realisierten Einsparungen wurden durch eine Kombination von effizienteren Wirkungen, einer Reduktion der Personalkosten, verschiedener Rationalisierungsprozesse und durch das Beenden von einigen Aktivitäten erzielt. Nach einer weiteren kleinen Restrukturierung im Dezember 2012 enthält die Behörde jetzt; „*Competition Group*“; „*Content, Consumer and External Affairs Group*“; „*Legal*“; „*Operations*“; „*Spectrum Policy Group*“; „*Strategy, International*“, „*Technology*“ und „*Economists*”. Im Januar 2011[121] hat Ofcoms „*Chief Executive*“ Ed Richards die Änderungen und Restrukturierungen noch detaillierter erklärt.[122] Als „*Group Director*“ von Ofcoms „*Content, Consumer and External Affairs Group*“ ist Claudio Pollack sehr wichtig für den Verbraucherschutz. Seine Aufgaben sind die Förderung und der Schutz der Kunden in den Telekommunikations- und Post-Industrien. Ferner muss er sicherstellen, dass die Kunden Zugriff auf diese Dienstleistungen haben. Diese „*Content, Consumer and External Affairs Group*“ beschäftigt sich auch mit Marktforschung und Internet-Politik. Im Übrigen ist Claudio Pollack auch Ofcoms Vertreter beim „*Board of UKCISS, the UK Council for Child Internet Safety*”.[123]

Ofcoms primäres Entscheidungsorgan ist das „*Board*“, welches die strategische Ausrichtung der Behörde unterstützt. Es enthält einen „*Non-Executive Chariman*“, „*Executive Directors (in-*

---

[119] C Williams, “Ofcom top of Tory deathlist: Quangogeddon“, *The Register*, 6 Juli 2009; online verfügbar; http://www.theregister.co.uk/2009/07/06/cameron_ofcom/

[120] *Annual Plan 2013/14*, Ofcom Webseite, online verfügbar; http://www.ofcom.org.uk/about/annual-reports-and-plans/annual-plans/annual-plan-2013-14/

[121] *Oxford Media Convention. Speech by Ed Richards: January 24, 2011*, Ofcom Webseite, online verfügbar; http://media.ofcom.org.uk/2011/01/24/oxford-media-convention-speech-by-ed-richards/

[122] Siehe auch *Ofcom organisation chart by reporting structure, 10 Dezember 2012*, Ofcom Webseite, downloadbare PDF; http://www.ofcom.org.uk/files/2010/09/Org_chart.pdf

[123] *Claudio Pollack*, Ofcom Webseite, online verfügbar; http://www.ofcom.org.uk/about/how-ofcom-is-run/content-board/members/claudio-pollack/

cluding the Chief Executive)", und "*Non-Executive Directors*". Das *Executive* wird von der Behörde betrieben und muss sich vor dem Board verantworten. Das Board tritt mindestens einmal pro Monat (außer im August) zusammen und die Agenda, eine Zusammenfassung, Notizen und der Sitzungsbericht werden regelmäßig online veröffentlicht. Das „*Executive Committee (ExCo)*" ist das wichtigste exekutive Team, es tritt jeden Monat zusammen und ist für die Zielsetzung und allgemeine Betriebsführung der Behörde verantwortlich. Das „*Policy Executive (PE)*" trifft wöchentlich zusammen und ist für die Entwicklung Ofcoms gesamter Regulierungsabsicht verantwortlich. Es diskutiert dabei vorwiegend verschiedene Ansätze, hat aber auch teilweise Befugnisse, eigene Entscheidungen zu treffen. Das „*Operations Board*" administriert den Arbeitsbereich und spezifisch die „*Central Operations*", welche sich mit tausenden von Verbraucherbeschwerden pro Woche beschäftigen müssen.

In der Rolle des *Operations Board´s* ist es Ofcoms internationale Leistung, Einrichtungen wie zum Beispiel die *European Platform of Regulatory Authorities*)[124] zu unterstützen, zu betreuen, aber auch, herausfordern. Das *Operations Board* tagt zweiwöchentlich und muss sich vor dem *ExCo* verantworten. Das „*Content Board*" ist ein Ausschuss des primären Board, das neue Maßstäbe für Fernsehen und Rundfunk setzt und durchführt. Es enthält Mitglieder, die jedes Land im Vereinigten Königreich von Großbritannien und Nordirland vertreten, und hat durch weite vorhandene Laienmitglieder zugleich Mitglieder, die extensive Rundfunk-Erfahrung haben. Es soll die Interessen der Verbraucher (hier die Zuhörer und Betrachter) verstehen, analysieren und fördern.[125] Ofcom selbst erklärt, dass neben jährlichen Plänen und Zielen die regulatorischen Grundprinzipien („*foundational regulatory principles*") noch sehr wichtig bleiben.[126] Diese Prinzipien enthalten eine Tendenz gegen Eingriffe und sind dabei evidenzbasiert, proportional, konsistent und verantwortlich ; und derart ausgerichtet, die am wenigsten aufdringliche Durchsetzung einzusetzen:

- Ofcom will operate with a bias against intervention, but with a willingness to intervene firmly, promptly and effectively where required;
- Ofcom will strive to ensure that its interventions will be evidence-based,

proportionate, consistent, accountable and transparent in both deliberation and

outcome; and

- Ofcom will always seek the least intrusive regulatory mechanisms to achieve its policy objectives.[127]

Nach den aktuellen Entwicklungen im Bereich der Urheberrechtsverletzungen und dem „*Public Service Broadcasting Review*",[128] nimmt Ofcom, keine ‚spezifische' Prioritäten innerhalb ihres strategischen Ziels der Entwicklung und Durchsetzung öffentlicher und parlamentarischer Politiken ein. Das spiegelt die Tatsache wider, dass Ofcoms strategisches Ziel eher reaktiv und

[124] http://www.epra.org/

[125] *How Ofcom is run*, Ofcom Webseite, online verfügbar; http://www.ofcom.org.uk/about/how-ofcom-is-run/

[126] *Statutory Duties and Principles*, Ofcom Webseite, online verfügbar; http://www.ofcom.org.uk/about/what-is-ofcom/statutory-duties-and-regulatory-principles/

[127] *Ibid*

[128] A Petridis, "Public Service Broadcasting: Inform-Educate-Entertain – review", *The Guardian*, 2 Mai 2013; online verfügbar; http://www.theguardian.com/music/2013/may/02/public-service-broadcasting-inform-review

politikbasiert ist und sich mit wichtigen Problemen des Parlaments oder der Regierung identifiziert und deren Lösungen durchführt.[129] Der aktuellste Plan für 2014 legt vor, dass Ofcom ihre normalen Aufgaben effizient bearbeiten, neue Entwicklungen und Problemen analysieren und darauf reagieren wird und soll. Dabei soll in ganz Großbritannien der Zugriff auf Verbraucherschutz unterstützt werden. Erstmalig wurde dabei eine Liste möglicher wichtiger und relevanter Themen, die auch in den nächsten Jahren wachsen könnten, geschaffen:

> **1.12** As well as these priorities, we will undertake a range of other work as part of our 2013/14 programme (discussed in Section 5), reflecting our statutory duties and responsibilities. We will also continue to deliver other services to stakeholders, such as licensing access to the radio spectrum (detailed in Section 6). We will deliver these services in the most efficient and effective way possible.
>
> **1.13** We will also continue to remain responsive to new issues, emerging concerns that affect consumers across the UK and new government requests, focusing on those areas where we can make the most difference.
>
> **1.14** In addition to responding to requests from the Government and to help it to implement its policies in respect of communications matters, we will also aid government in the UK nations to ensure that consumer and citizen benefits are available across and within all the nations of the UK.
>
> **1.15** For the first time this year we include a list of areas of potential future relevance to Ofcom. These areas comprise possible future priorities for the organisation and emerging issues on which Ofcom may be required to have a view in the future. Both are areas over which Ofcom will continue to have a watching brief, but where it is too early to undertake work within next year's Annual Plan.[130]

Das Ofcom Hauptbüro findet man im Riverside House, Southwark Bridge Road in London. Für öffentliche Beratung gibt es eine „*advice page*", das wie eine FAQ Seite funktioniert.[131] Ofcom ist auch per Telefon unter 0300 123 3333 oder 020 7981 3040 erreichbar.

cc) Übersicht und Regelung des Markts

Ofcom nutzt sehr oft Konsultationen mit Industrien und der Öffentlichkeit, um besser informierte und evidenzbasierte Entscheidungen treffen zu können. Dieser Prozess beginnt mit der Veröffentlichung von Dokumenten auf Ofcoms Webseite, in welchen um Meinungen und Antworten gebeten wird. Für den Fall, dass die relevanten Konsultation-Dokumente zu lang oder kompliziert wären, sind auch einfache Zusammenfassungen dazu veröffentlicht. Es gibt danach einen zehnwöchigen Zeitraum, in dem interessierte Parteien, Unternehmen oder Organisationen ihre Antworten an Ofcom schicken können. Nach diesem Zeitraum veröffentlicht Ofcom die Antworten und Meinungen auf ihrer Webseite (abgesehen von persönlichen oder

---

[129] *Ofcom Annual Plan 2013/14*, Ofcom Webseite, 26 März 2013; downloadbare PDF; http://www.ofcom.org.uk/files/2013/03/annplan1314.pdf

[130] *Ibid*

[131] *Ask Us*, Ofcom Webseite, online verfügbar; http://ask.ofcom.org.uk/

vertraulichen Daten). Nach der Konsultation bereitet Ofcom eine Zusammenfassung der Antworten („*a summary of responses*“) vor, welche an die Regierung oder das Parlament geschickt und/oder als Basis für weitere Entscheidungen benutzt werden.[132]

Ofcom musste als Medien-Regulierungsbehörde („*Media Regulator*“) „*Regulatory Codes*“ für den *Digital Economy Act* schaffen, welche die Wirkungen des Gesetzes erklären können. Ofcom hat im Mai 2010 einen 74-seitige „*draft code*“ veröffentlicht, der den Prozess für die Identifizierung eines illegalen „*File-sharers*“ skizziert hat, um .Zivil- oder Strafprozesse, und so besonders die *3-strikes-policy,* möglich zu machen. Ferner dürfen Individuen und Organisationen Ofcom nur ein „*designated electronic communications network“* oder relevante Einrichtungen/ und Möglichkeiten zur Notifizierung bieten.[133] Dadurch ist die Regulierung aller Telekommunikationsnetzwerke sehr eng an die Ofcom-Übersicht verbunden.

In *Section 1(5)* sind die Befugnisse Ofcoms nach *subsection (3)* klar definiert als; (a) die Macht, Forschungen und Untersuchungen in Verbindung mit relevanten Funktionen von Ofcom zu unterfangen; und (b) die Macht, solche Forschungen oder Untersuchungen anderer zu unterstützen oder zu organisieren, sodass andere solcher Forschungen oder Untersuchungen ermöglicht werden können. Ofcom ist im Moment sehr mit der Umsetzung des 4G in Großbritannien beschäftigt, und verauktioniert sehr oft 4G Bandbreite. Ofcom erhöht auch die Gebühren für 2G Bandbreite, die jetzt von den Telekommunikations-Akteuren benutzt werden,[134] und versucht auch zu bewirken, dass Firmen ihre Bandbreite wirklich nutzen und nicht nur sammeln.[135]

Im Bereich Netzneutralität hat Ofcom ebenfalls eine relativ hohe Verantwortung. Auf EU-Ebene sind die Pflichten der IDA zur Bereitstellung von Informationen über Geschwindigkeit und Einschränkungen einer Internetleitung nicht komplett geklärt. Ferner gibt es viele Diskussionen darüber, wie viele Informationen genau dem Verbrauchern zuzukommen sind.[136] Ofcom hat einen „*wait and see*“ Ansatz gewählt (wie die Kommission, wenn es zur Netzneutralität kommt), und bis jetzt keine konkreten Regeln diesbezüglich gemacht, denn die Entscheidung, wie viel Information an den Verbrauchern gegeben werden muss, ist eine für die IDA. Fernergibt es dazu kein obligatorisches, standardisiertes System.[137] Es gibt jedoch ein freiwilliges System über Informationspflichten in den Ofcom Regelungen, aber diese sind oft nicht sehr transparent von der IDA eingeführt.[138]

---

[132] *How Will Ofcom Consult?*, Ofcom Webseite, online verfügbar; http://stakeholders.ofcom.org.uk/consultations/how-will-ofcom-consult

[133] Section 33, *Communications Act 2003*

[134] B Ray, “Ofcom, it's WAR! Mobe networks fire broadside over 2G spectrum pricing”, *The Register*, 11 Oktobre 2013; online verfügbar; http://www.theregister.co.uk/2013/10/11/network_operators_kick_off_pr_battle_over_2g_pricing/

[135] B Ray, “Ofcom sets out next DECADE of spectrum policy: Use it or lose it”, *The Register*, 3 Oktober 2013; online vefügbar; http://www.theregister.co.uk/2013/10/03/ofcom_sets_out_next_decade_of_spectrum_policy/

[136] Article 1(14) of *Directive 2009/136/EU of the European Parliament and of the Council, OJ 2009/L 337, p 11.,* Article 20 (1)(b), *Universal Services Directive.*

[137] *Approach to net neutrality*, Ofcom Webseite, para 1.14, 24 November 2011; downloadbare PDF; http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/statement/statement.pdf

[138] *Ibid,* para 3.15 und A1.5 - A1.13. Siehe auch D Read, “Net neutrality and the EU electronic communications regulatory framework”, *International Journal of Law and Information Technology*, Vol 20, 48, at 68, (2012), über BTs Webseite.

dd) Sanktionen und Durchsetzungsmechanismen

Ofcom beschäftigt sich primär mit Regulierung und Übersicht und hat auch sehr weitgehende Aufgaben, hat also normalerweise nicht viel mit individuellen Sanktionen zu tun. Ofcom ist dabei kein Mediator zwischen Verbraucher und Telekommunikationsunternehmen auf individuelle Basis::

> We are not responsible for regulating: disputes between you and your telecoms provider; premium-rate services, including mobile-phone text services and ringtones; the content of television and radio adverts; complaints about accuracy in BBC programmes; the BBC TV licence fee; or post offices; or newspapers and magazines.[139]

Sofern Ofcom überhaupt etwas mit Sanktionen zu tun hat, handelt es sich oftmals um Sanktionen *gegen* Verbraucher, weil Ofcom die Urheberrechts-Streite zwischen Kunden, IDA und Rechteinhaber beaufsichtigt. Nach dem „*Online Infringement of Copyright and the Digital Economy Act 2010*"-Konsultation[140] hat Ofcom die Maßnahmen gegen online Urheberrechtsverletzungen klarer gestellt und die neuen Ofcom Codes entwickelt. Die Mehrheit der kleineren Details der Urheberrechtsprovisionen im DEA wurde nicht klar definiert, dafür jedoch wurde Ofcom die Kompetenz gelassen, durch Codes zu regulieren.[141] Aufgrund von Verspätungen und Streitigkeiten über die genaue Wirkungen dieses Systems tritt dieses jedoch erst 2014 in Kraft.

Der Prozess, dass Rechteinhaber Anklagen gegen mutmaßliche Urheberrechtsverletzer erheben können, folgt der oben erwähnten[142] *3-strikes-policy* oder dem „*graduated response*" System. Dieses System enthält drei Warnbriefe von der IDA (auf Anforderung der Rechteinhaber) an den mutmaßlichen Urbeherrechtsverletzer, bevor die letzte Sanktion der Drossellung („*throttling*") oder Blockierung der Internetverbindung gewählt werden kann. Der mutmaßlicher Verletzer/Verbraucher hat aber die Möglichkeit, gegen diese Briefe Berufung einzulegen. Werden jedoch mehr als 3 Briefe zugestellt, ohne dass sie erfolgreich angefochten wurden, so werden die Verletzer schwarzgelistet, d.h. der Rechteinhaber kann ihn identifizieren oder die IDA kann ihn blockieren. [143]

Bei Erfüllung der Voraussetzung des *Section 33 Communications Act 2003* – dass Anbieter eines designierten elektronischen Kommunikationsnetzwerks (*designated electronic communications network*) Ofcom zuerst benachrichtigen müssen – kann Ofcom bei Vorliegen angemessener Gründe für die Annahme, dass jemand *Section 33* verletzt hat, dem Verletzer eine Benachrichtigung nach *Section 35* schicken und, bei ausbleibender Reaktion, eine Geldstrafe bis zu £10.000 nach *Section 37(6)* verhängen. Diese Geldstrafe wird direkt an Ofcom bezahlt. Nach *Section 1(3)* und *1(5)(c) Communications Act 2003* hat Ofcom auch weitere Befugnisse

---

[139] *What is Ofcom*, Ofcom Webseite, online verfügbar; http://www.ofcom.org.uk/about/what-is-ofcom/

[140] *Online Infringement of Copyright and the Digital Economy Act 2010: Draft Initial Obligations Code*, Ofcom Webseite, 28 Mai 2010; downloadbare PDF; http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf

[141] K Solomon, "ISP's 'three strikes' policy hitting pirates in 2014: Ofcom outlines how it will tackle copyright infringers", *TechRadar*, 26 Juni 2012; online verfügbar; http://www.techradar.com/news/internet/isp-s-three-strikes-policy-hitting-pirates-in-2014-1087016

[142] II. Struktur des Urheberrechts

[143] Section 124H, Obligations to limit Internet Access, *Communications Act 2003, (amended by Section 10 DEA)*

für Strafverfolgungen in England, Wales oder Nordirland, wenn sie relevant für Ofcoms Funktionen sind..

ee) Selbstständigkeit und Pflichten der Behörde

Ofcom ist eine der wichtigsten „*quangos*"(*quasi-autonomous non-governmental organisations*), die oft in Großbritannien und Irland gefunden werden. Ofcom bewahrt also ein Maß an Unabhängigkeit, bekommt aber im Endeffekt die Befugnisse und Verantwortlichkeiten via Gesetz und arbeitet eng mit der Regierung zusammen. So wurde beispielsweise in dem *Communications Act 2003* von Anfang an erklärt, dass Ofcom ermächtigt ist, absolut alles zu tun, was für ihre Aufgaben nebensächlich oder förderlich ist – auch Geld "leihen", aber nur mit Zustimmung des *Secretary of State*.[144] Nach *Section 1 – ‚Functions and general powers of OFCOM'*:

…

> **(3)** OFCOM may do anything which appears to them to be incidental or conducive to the carrying out of their functions, including borrow money.
>
> **(4)** OFCOM are not to borrow money except with the consent of the Secretary of State, or in accordance with a general authorisation given by him.
>
> **(5)** OFCOM's powers under subsection **(3)** include, in particular—
>
> > **(a)** power to undertake research and development work in connection with any matter in relation to which they have functions;
> >
> > **(b)** power to promote the carrying out of such research and development by others, or otherwise to arrange for it to be carried out by others;
> >
> > **(c)** power to institute and carry on criminal proceedings in England and Wales or Northern Ireland for an offence relating to a matter in relation to which they have functions; and
> >
> > **(d)** power, in such cases and in such circumstances as they may think fit, to make payments (where no legal liability arises) to persons adversely affected by the carrying out by OFCOM of any of their functions.

Hier sieht man, dass Ofcom eine Menge Verantwortung hat, die auch weiter im Part 1 gefunden werden können. Ofcom muss immer die Meinungen und Interessen der Kunden in relevanten Märkten und auch des breiten Publikums berücksichtigen. Anderseits muss Ofcom auch die Investition und Innovation in den relevanten Bereichen fördern.[145] Letztlich ist auch interessant, dass Ofcom berechtigt ist (ohne Rechtsschuld), Individuen Entgeld, d.h. Kompensationen, zu bezahlen, wenn dies für angemessen befunden wird, d.h. falls sie durch die Arbeit der Ofcom beschwert werden.[146]

d. Andere bemerkenswerte Behörden

aa) Ombudsman Services[147]

Die "*Ombudsman Services*" sind sehr informativ und praktisch. Aus der Verbraucherperspektive heraus betrachtet sind sie sehr wichtig, weil sie oft die erste Anlaufstelle sind, wenn es irgendein Verbraucherschutzproblem gibt. „*Communications, Energy, Property and Copyright*" sind die Hauptbereiche der *Ombudsman Services*, neben weiteren, spezielleren Kategorien

---

[144] Section 1(4), *Communications Act 2003*

[145] Section 3(4), *Communications Act 2003*

[146] Section 1(5)(c), *Communications Act 2003*

[147] http://www.ombudsman-services.org/

wie „*The Green Deal*“[148] über Energieeffizienz in Großbritannien, Beschwerde über reallymoving.com, Umzüge-Firmen oder über Geschäftsleute und Firmen nach dem “*Which? Trusted Traders scheme*“.[149] Bezüglich der digitalen Welt ist die wahrscheinlich wichtigste Kategorie die „*Copyright*“ Kategorie, weil sie sich mit Beschwerden über Rechteinhaber beschäftigt:

> Our job is to resolve complaints about bodies that either own or administer, on behalf of third parties, the licensing of copyright materials. These are called Collective Management Organisations or collecting societies.[150]

Diese *Ombudsman Services* sind für Verbraucher kostenlos. Dabei sind sie völlig unabhängig von Regulierungsbehörden, der Urheberrechtindustrie und anderen Verbraucherschutzorganisationen. Sie arbeiten als Mediator und versuchen, eine einfache Lösung zwischen Unternehmen und Verbrauchern zu treffen. Wenn eine Partei das nicht akzeptiert, darf sie immer noch vor Gericht ziehen.[151]

bb) Citizens' Advice Bureau[152]

Das Citizens´ Advice Bureau hat die vorherigen Befugnisse des *Consumer Directs,* eines staatlich geförderten Call-Centers, das auch eine relevante Webseite für Verbraucherbeschwerden hatte, übernommen. Nach einer staatlichen Überprüfung im Jahr 2010 wurde *Consumer Direct* im März 2012 geschlossen und die Rolle wurde vom „*Citizens Advice Bureau*“ übernommen. Dieses Bureau nutzt die gleiche Telefonnummer und bietet ähnliche Informationen wie das *Consumer Direct* an, ist aber auch für mehr als nur den Verbraucherschutz verantwortlich. Es existiert noch ein „*Citizens Advice consumer service*“.[153] Dort wird ebenfalls ein „Annual Report“ veröffentlicht, welcher wieder online abrufbar ist und das Ziel zu realisieren versucht, die Bürger besser zu informieren.[154] Einfache Informationen für Bürger werden auf einer speziellen Webseite http://www.adviceguide.org.uk/ angeboten. Dabei ist das Citizens´Advice Bureau eine unabhängige, informationelle Behörde, die aber keine stärke Überwachungsverantwortlichkeit für Märkte oder eigene Sanktionsmechanismen innehat.

---

[148] *The Green Deal*, Ombudsman Services Webseite, online verfügbar; http://www.ombudsman-services.org/green-deal.html

[149] *Which? Trusted Traders*, Ombudsman Services Webseite, online verfügbar; http://www.ombudsman-services.org/which-trusted-traders.html

[150] *About the Ombudsman*, Ombudsman Services Webseite, online verfügbar; http://www.ombudsman-services.org/copyright.html

[151] *How we work*, Ombudsman Services Webseite, online verfügbar; http://www.ombudsman-services.org/how-we-work-os.html

[152] http://www.citizensadvice.org.uk/

[153] *Citizens Advice consumer service*, Citizens Advice Bureau Adviceguide Webseite, online verfügbar; http://www.adviceguide.org.uk/england/consumer_e/consumer_protection_for_the_consumer_e/consumer_citizens_advice_consumer_service_e.htm und *If you need more help*, Citizens Advice Bureau Adviceguide Webseite, online verfügbar;
http://www.adviceguide.org.uk//consumer_e/if_you_need_more_help.htm

[154] *Citizens Advice annual report 2012/2013*, Citizens Advice Bureau Webseite, online verfügbar; http://www.citizensadvice.org.uk/index/aboutus/publications/annualreports/annual_report_2013.htm

cc) Intellectual Property Office (IPO)

2012 hat das IPO neue „*draft regulations*“, die einen Mindeststandard („*minimum standard*“) für britische Verwertungsgesellschaften festgelegt haben, veröffentlicht. Danach wird erwartet, dass Verwertungsgesellschaften diesen Mindeststandard bei ihren eigenen Codes benutzen und befolgen. Das könnte für den digitalen Verbraucherschutz wichtig sein, weil das IPO auch umfangsreich für das Urheberrecht verantwortlich ist und die Regelungen auch etwas über Beschwerdeprozesse besagen.

> Last year the IPO published "minimum standards" (6-page / 368KB PDF) that it expects to see adhered to in collecting societies' voluntary codes. The standards stretch across areas including staff conduct, information and transparency, complaints handling and collecting societies' obligations to licensees.
> Now it has set out new draft regulations under which it will have the power to impose "effective, dissuasive and proportionate" sanctions on copyright licensing bodies that fail to adhere to those requirements. Sanctions include a potential £50,000 fine.[155]

Das IPO kann der Regierung auch die Macht geben, in der Industrie einzugreifen, wenn es findet, dass es gravierende Probleme in diesem Bereich gibt und keine ausreichend starke Selbstregulierung der Verwertungsgesellschaften vorliegt.[156]

[155] “Collective licensing bodies face £50,000 fine for non-compliant code”, *Out-Law*, Pinsent Masons, 17 September 2013; online verfügbar; http://www.out-law.com/en/articles/2013/september/collective-licensing-bodies-face-50000-fine-for-non-compliant-code/

[156] “CLA announces new code of conduct to govern its collective licensing activities”, *Out-Law*, Pinsent Masons, 2 November 2012; online verfügbar; http://www.out-law.com/en/articles/2012/november/cla-announces-new-code-of-conduct-to-govern-its-collective-licensing-activities/

IV. Länderbericht zur „Übersicht über die Regulierung des Datenschutzes und des Urheberrechts in der digitalen Welt in den USA“

Im Folgenden werden die Regelungsstrukturen des Datenschutz- und Urheberrechts in den USA sowie etwaige Durchsetzungsbefugnisse von öffentlichen Stellen untersucht. Dieser Länderbericht untergliedert sich in die Darstellung der Regelungsstrukturen des Datenschutz- und Urheberrechts in den USA (1.), der Ausrichtung und Gegenstände der relevanten Verbraucherbehörden (2.), der „verwaltungsrechtlichen“ Durchsetzung des „Datenschutzrechts“ (3.) sowie die Feststellung fehlender behördlicher Befugnisse und Strukturen im Urheberrecht (4.).

1. Regelungsstruktur des Datenschutz- und Urheberrechts

Zum besseren Verständnis der vom deutschen und europäischen System abweichenden Regelungen wird vor der Frage nach der verwaltungsrechtlichen Durchsetzung die materielle Rechtslage zum „Datenschutzrecht“ und Copyright Law in den Vereinigten Staaten dargestellt.

a. Struktur des „Datenschutzrechts“

Weder auf Bundes- noch auf Staatenebene ist in den Vereinigten Staaten ein Äquivalent zu dem breiten Ansatz des Datenschutzrechts in Deutschland durch das BDSG gegeben.[1] Die Nutzung und die Weitergabe von Informationen über einen Verbraucher, welche mittels elektronischer Techniken erhoben, verarbeitet oder weitergegeben werden, sowie anderer persönlicher Informationen von oder über einen Verbraucher, unterliegen in den USA grundsätzlich keinen Beschränkungen. Ein verfassungsrechtliches Recht auf Schutz der eigenen personenbezogenen Daten oder anderen persönlichen Informationen durch Private besteht grundsätzlich nicht.[2]Es gilt der Grundsatz, dass Informationen von und über Verbrauchern durch Unternehmen gesammelt und genutzt werden dürfen, es sei denn Gesetze oder andere Vorschriften schränken ein solches Verhalten ein.[3]

Eine präventive staatliche Regulierung der Verbrauchersachverhalte findet dabei in der Regel nicht statt, sondern es wird auf die Selbstregulierung des Marktes gesetzt. Erst bei einem mas-

[1] Prescilla M. Regan, `*The United States'* in Global Privacy Protection, ed by James B. Rule and Graham Greenleaf (2010), 50, 51 bezeichnet die *privacy protection* in den USA als eher schwach und als einen “patchwork of protection”.

[2] In der *Constitution* ist kein grundlegendes Recht auf Datenschutz oder Schutz der privaten Sphäre gegeben. Der Supreme Court hat zwar für den Bereich des staatlichen Handelns ein solches Recht entwickelt, für den privaten Bereich fehlt eine solche Anerkennung jedoch, siehe Prescilla M. Regan, `*The United States'* in Global Privacy Protection, ed by James B. Ruleand Graham Greenleaf (2010), 50, 51.

[3] Paul M. Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures* 126 Harv. L. Rev. 1966, 1976 (2013).

siven Regelungsbedarf bedingt durch ein Versagen der Selbstregulierung erfolgt ein staatliches Eingreifen[4] und dann auch nur für bestimmte Sachverhaltskonstellationen.[5] Insbesondere für den Bereich der *privacy* wurde lange Zeit das Modell der Selbstregulierung für den digitalen Markt präferiert. Es wurde angenommen, dass die Verbraucher sich für die Unternehmer entscheiden würden, welche die *privacy* des einzelnen Verbrauchers am Besten schützen. Schwarze Schafe würden so durch den Markt selbst abgestraft.[6] Dabei ist kulturell zu beachten, dass zwar dem Staat ein gewisses Misstrauen hinsichtlich der Datenverarbeitung entgegengebracht wird, privaten Stellen hingegen eher vertraut wird.[7] Mit Ende des 20. Jahrhunderts setzte sich jedoch auch die Erkenntnis durch, dass zumindest für einige Bereiche der Ansatz der Selbstregulierung für den Schutz der Verbraucher im Internet nicht die gewünschte Wirkung erzielte,[8] auch weil es der FTC an der Kompetenz fehlte, die Unternehmer zur Erstellung von *online privacy policies* und deren Einhaltung zu verpflichten.[9]Grund für die Abkehr von Selbstregulierungsansatz der FTC im Bereich der *consumer privacy* waren wirtschaftliche Überlegungen: Ein Misstrauen der Verbraucher in die Online Anbieter würde dem Online-Handel Wachstum schaden.[10] In den letzten 15 Jahren ist die FTC im *privacy* Schutz sehr aktiv geworden[11] auch wenn es an einem systematischen Datenschutz bzw. Verbraucherdatenschutz und einem generellen Datenschutzauftrag der FTC fehlt.
Die Regelungen, welche auf Verbraucherdaten Anwendung finden, lassen sich in Regelungen über *consumer privacy* sowie *data security* einteilen. Die Regelungen zur *consumer privacy*

---

[4] Einen solchen sah die FTC 2000 in ihrem Report in Bezug auf *consumer online privacy* als gegeben an, obwohl sie auch weiterhin die Selbstregulierung als Grundidee und zur Implementierung weitergehender Standards vertrat (http://www.ftc.gov/reports/privacy2000/privacy2000.pdf, zuletzt abgerufen am 30.10.2013). Noch 1998 hatte die FTC einen solchen breiten legislativen Schritt abgelehnt und legislative Schritte nur für den Schutz von Kindern befürwortet; Report 1998, 42 (http://www.ftc.gov/reports/privacy3/priv-23a.pdf, zuletzt abgerufen am 30.10.2013).

[5] So Prescilla M. Regan, `*The United States'* in Global Privacy Protection, ed by James B. Rule and Graham Greenleaf (2010), 50, 51 für *privacy* mit Bezug auf bestimmte Arten von Informationen und bestimmte Datensammlungen.

[6] Fred H. Cate, *Privacy in the Information Age* 131 (1997); FTC Report 2000, dissenting Opinion of B. Leary, supra note 2 at 4(s. Fn. 4); so auch die Privacy Protection Study Commission in ihrem Schlussbericht (abrufbar unter http://epic.org/privacy/ppsc1977report/, zuletzt abgerufen am 30.10.2013, welche einen breiten Ansatz für die Privatwirtschaft ablehnte und den Grundstein für den sektoralen Ansatz legte.

[7]Prescilla M. Regan, `*The United States'* in Global Privacy Protection, ed by James B. Rule and Graham Greenleaf (2010), 50, 76.

[8] FTC Report 1998 sowie 2000 (s. Fn. 4).

[9] Michael D Scott, *The FTC, the Unfairness Doctrine, and data security breach litigation*: *Has the Commission gone too far?*60 Admin L. Rev. 128, 130 (2008); im FTC Report 2000 (s. Fn.4) schlug die FTC den Erlass eines Gesetzes vor, welches der FTC eine solche Kompetenz gegeben hätte. Dies wurde nach der Berufung von Timothy Muris als Vorsitzenden der FTC durch Präsident Busch jedoch nicht weiter verfolgt. Muris setzte vielmehr auf die bestehenden Gesetze und die administrative Aufgabe der FTC, siehe Erklärung von Timothy J Muris, Challenges Facing the Federal Trade Commission: Hearing on HR 68 Bevor the Subcomm. On Commerce, Trade and Consumer Protection oft he H. Cimm. On Energey and Commerce, 107th Cong. 12 (2001) (http://www.gpo.gov/fdsys/pkg/CHRG-107hhrg76308/pdf/CHRG-107hhrg76308.pdf, zuletzt abgerufen am 30.10.2013): *A majority of the Commission does not support online privacy legislation at this time but there is no doubt that consumer privacy is an issue that will continue to be studied and debated both at the FTC and in Congress*; für bestimmte Bereiche ist eine solche Verpflichtung nun gegeben, siehe 15 USC § 6803 (a).

[10] FTC Report 1998 (s. Fn. 4); Michael D Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation*: *Has the Commission gone too far?*60 Admin L. Rev. 128 (2008).

[11] Michael D Scott, *The FTC, the Unfairness Doctrine, and data security breach litigation*: *Has the Commission gone too far?*60 Admin L. Rev. 128, 129 (2008).

erfassen hauptsächlich die Erteilung von Informationen an den Verbraucher über die Nutzung seiner Verbraucherinformationen sowie die Einhaltung von *privacy policies.* Die Regelungen zur *data security* hingegen zielen auf den Schutz von *consumer data* oder anderen Daten ab, die von einem Unternehmer gespeichert wurden. Diese Regelungen sehen in der Regel vor, dass die Unternehmen Sicherheitsvorkehrungen gegen Angriffe von Dritten, gerichtet auf den Diebstahl dieser Informationen, einrichten müssen[12]. Die Begriffe „*consumer privacy*" aber auch „*consumer data"* beschränken sich dabei nicht zwangsläufig auf elektronisch verarbeite Informationen von Verbrauchern.
Neben diesen beiden Unterteilungen ist anzumerken, dass der Schutz von Daten in den USA primär einen sektoralen Ansatz verfolgt[13], sodass branchenspezifische Regelungen zum Schutz des Verbrauchers bestehen.[14] Daneben setzen einzelne Regelungen an der Art der Information[15], der Art der Speicherung[16] oder dem Umgang mit Informationen[17], den speichernden Personen oder Organisationen[18], dem Verwendungszweck der Information[19] oder an den betroffene Nutzergruppen[20]an. Dieser sektorale und fragmentierte Ansatz führt dazu, dass insbesondere die Nutzung von Verbraucherdaten durch neue Technologien oder neue Branchen gegebenenfalls nicht reguliert ist.[21] Ein besonderer Schutz im Bereich der digitalen Welt besteht für Verbraucherdaten allgemein nicht. Durch den *Childen Online Privacy Protection Act*[22] gilt ein sektorübergreifender Schutz für sämtliche online-Angebote nur für persönliche Daten von Kindern unter 13 Jahren.[23]
In Kalifornien wurde das branchenabhängige Regelungsmodell für den digitalen Verbraucherschutz durch den *California Online Privacy Protection Act of 2003* (CalOPPA) aufgeweicht, da

---

[12] Siehe zum Beispiel §§ 1798.81 sowie 1798.81.5 (b) California Civil Code; ebenso 15 USC § 6801 (b), welcher den Finanzinstituten vorschreibt gewisse Schutzmaßnahmen einzurichten.

[13] Paul M. Schwartz, *The EU-US Privacy Collission: A Turn to Institutions and Procedures* 126 Harv. L. Rev. 1966, 1974 (2013).

[14] So zum Beispiel der Gramm-Leach-Bliley Act im Hinblick auf Finanzinstute, 15 USC Subchapter I (Disclosure of nonpublic personal information); Title 2 Tex. Business and Commerce Code Chapter 21 im Hinblick auf Consumer Credit Reporting Agencies; California Confidentiality of Medical Information Act; California Financial Information Privacy Act; 47 USC § 222 (Schutz der *consumer privacy* durch Telekommunikationsunternehmen).

[15] Video Privacy Protection Act of 1988; California Confidentiality of Medial Information Act; § 1798.91 Ca. Civil Code (medical information); § 1798.20 Cal. Civil Code (maintaining computerized data); § 1798.85 Cal. Civil Code (confidentiality of social security numbers).

[16] Family Educational Rights and Privacy Act of 1974.

[17] § 1798.80 Cal. Civil Code schreibt besondere Anforderungen bei Zerstörung von Informationen vor.

[18] Health Information Portability and Accountability Act of 1996.

[19] Fair Credit Reporting Act of 1970; im texanischen Business and Commerce Code Title 2 sec. 20.02 wird einer *consumer reporting* agency die Erstellung von consumer reports nur unter besonderen Bedingungen erlaubt.

[20] Familiy Educational Rights and Privacy Act of 1974; California Reader Privacy Act.

[21] Paul M. Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures* 126 Harv. L. Rev. 1966, 1975 (2013); GesetzesvorschlägefüreineninsbesonderestärkerenstrafrechtlichenSchutzwurden in der Vergangenheit unterbreitet, diese sind jedoch entweder nicht weiter verfolgt oder nicht angenommen worden (Cyber-Security Enhancement and Consumer Data Protection Act of 2007, H.R.836; Personal Data Privacy and Security Act of 2009, 111th Congress S 1490 RS; Notification of Risk to Personal Data Act, H.R. 5582). Zuletzt wurde mit dem *Privacy Bill of Rights* durch Präsident Obama Anfang 2012 der Versuch eines weitergehenden Datenschutzes unternommen, jedoch fehlt bis heute ein konkreter Gesetzgebungsvorschlag (http://www.whitehouse.gov/sites/default/files/privacy-final.pdf).

[22] 15 USC §§ 6501-6506.

[23] Nach 15 USC § 6502 ist zwar grundsätzlich nur der Betreiber einer *website* von diesen Regelungen betroffen, in der überarbeiteten COPPA Rule der FTC sind neben *websites* auch *online services* erfasst, 16 CFR 312.

dieses Gesetz auf bestimmte Informationen von sämtlichen Verbrauchern und bei allen „*commercial websites or onlice services*“ Anwendung findet. CalOPPA schreibt den Betreibern solcher online Dienste vor, über ihre *privacy policies* zu informieren. Sofern der staatenübergreifende Handel betroffen ist, steht dem föderalen Gesetzgeber die Möglichkeit zum Erlass von Gesetzen offen, die dann die staatlichen Gesetze außer Kraft setzen.[24] Bislang hat dies für Verbraucherdaten nur in einzelnen Bereichen stattgefunden.[25] Dadurch, dass CalOPPA den räumlichen und sachlichen Anwendungsbereich auf alle online Dienste erstreckt, welche Daten von kalifornischen Verbrauchern sammeln, hat die kalifornische Gesetzgebung Auswirkungen über die Grenzen des Staates Kalifornien hinaus.[26]
Einige föderale Gesetze sehen neben zivilrechtlichen Rechtsbehelfen[27] die Regelung der Aufsicht zur Einhaltung der jeweiligen Regelungen an die Federal Trade Commission oder anderen Bundesbehörden.[28]
Darüber hinaus sehen einige Regelungen vor, dass ein Verstoß gegen die staatliche Regelung zugleich einen Verstoß gegen das staatliche oder föderale Wettbewerbsrechts darstellt.[29] In diesem Fall untersteht dann die Durchsetzung der im Ergebnis datenschützenden Einzelnormen der betreffenden Behörde. Diese werden in der Regel bei Verbraucherbeteiligung die staatlichen Verbraucherschutzbehörden, bzw. die Attorneys General sein.[30] Auch die FTC hat

---

[24] Für den California Online Privacy Protection Act liegt eine solche *preemption* bislang nicht vor, da ein föderales Gesetz mit ähnlich breiten Ansatz fehlt; in besonderen Fällen ist eine solche *preemption* hinsichtlich branchenspezifischen Regelungen möglich.

[25] So zum Beispiel für Finanzinformationen, 15 USC 6801.

[26] Margaret Betzel, *Privacy Law Developments in California* 2 I/S: J. L. &Pol'y for Info. Soc'y 831, 866 (2006); erfasst sind damit nahezu alle Websites im Netz.

[27]Die Durchsetzung durch zivilrechtliche Mittel ist im Bereich des Verbraucherschutzes und Wettbewerbsschutzes sogar eher die Ausnahme, Richard A. Mann & Barry S. Roberts, Business Law 614 (15th 2012).

[28] So überträgt zum Beispiel 15 USC § 6805 (Gramm-Leach-BlileyAct) die Durchsetzung der Regelungen zum Schutz von Informationen von Verbrauchern ‚die Finanzinstituten vorliegen, dem Bureau of Consumer Financial Protection, den föderalen Regulatoren, den staatlichen Aufsichtsbehörden für Versicherungen sowie der Federal Trade Commission; der Fair Credit Reporting Act überträgt nach 15 USC § 1681 die Durchsetzung der Federal Trade Commission; 47 USC § 205 sieht die Aufsichtskompetenz der Federal Communication Commission auch hinsichtlich der *consumer privacy* Bestimmungen vor; Auf Staatenebene ist ebenfalls die ausdrückliche Übertragung von aufsichtsrechtlichen Kompetenzen auf bestimmte *agencies* möglich.

[29] So zum Beispiel Title 2 Tex. Business and Commerce Code § 20.12 für die Bestimmungen hinsichtlich der Consumer Credit Agencies. § 20.12 stellt ein Verstoß gegen die Regelungen zur Nutzung bestimmter Informationen einer *false, misleading, or deceptive trade practice* gleich; hinsichtlich des California Online Privacy Protection Acts wird ausdrücklich keine Durchsetzung oder Haftung im Gesetz angeordnet; allerdings wird auch hier die Möglichkeit zivilrechtlicher Klagen durch die Aufsichtsbehörden gesehen, Margaret Betzel, *Privacy Law Developements in California* 2 I/S: J. L. &Pol'yfor Info. Soc'y 831, 866 (2006); Sarah B. Kemble, *Privacy Policies: Is there really a chance anymore?* 16 S.C.Law 27, 31 (2004) hält eine Durchsetzung durch das California Competition Law für möglich; ebenso Corey A. Ciocchetti, *E-commerce and information privacy: privacy policies as personal information protectors* 44 Am. Bus. L. J. 55, 90 (2007); § 17200 Cal. Business and Professional Code gilt jedoch ausdrücklich nur für bestimmte Abschnitte des Gesetzes. Entscheidungen diesbezüglich sind bislang nicht ersichtlich.

[30]Verbraucherschützende Behörde in Californien ist der Attorney General sowie das Department of Consumer Affairs, wobei das Deaprtment of Consumer Affairs hauptsächlich als Lizensierungsbehörde fungiert; in Texas ebenfalls das Office des Attorney Generals. In New York das Department of State, Division of Consumer Protection sowie ebenfalls der Attorney General als Kläger in Zivilverfahren wegen Verstoß gegen *unfair and deceptive trade practices.* Neben diesen allgemeinen Verbraucherbehörden sind jedoch für bestimmte Wirtschaftssektoren spezielle Behörden als Aufsichtsbehörden zuständig, wie z.B. das Texas Office of Consumer Credit Commissioner für false, misleading or deceptive adverstising bei Verbraucherkrediten.

als Bundesbehörde eine aufsichtsrechtliche Kompetenz bei „*unfair and deceptive acts or practices*.[31]

b. Struktur des Urheberrechts

Obwohl auch einige ***state „copyrights"***[32] vorhanden sind, ist Grundlage des Urheberrechts in den USA der *Copyright Act of 1976*. Der erste föderale Copyright Act wurde bereits 1790 erlassen und wurde zahlreich geändert. 1976 wurde infolge technischer Erneuerungen der Copyright Act zuletzt grundlegend reformiert.[33] Der *Copyrigh Act of 1976* dient nun als maßgeblicher Rahmen für das Urheberrecht in den Vereinigten Staaten.[34] Die Regelungen des Copyright Act finden sich in Title 17 des U.S.Code. Mit Beginn des digitalen Zeitalters wurden Änderungen des Coyright Acts vorgenommen.[35]

Das US-amerikanische Copyright Law verfolgt einen breiten Ansatz: jeder Ausdruck einer Idee durch einen Autor wird geschützt.[36] Es bedarf dafür lediglich eines gewissen Grads an Originalität und muss in einem „*tangible medium ofexpression*" fixiert sein.[37] Mit der Schaffung eines solchen Werks besteht ein Schutz nach dem Copyright Act.[38] Einer Registrierung des Copyrights bedarf es für die Wirksamkeit des Copyrights nicht[39]; eine solche Registrierung ist allerdings Voraussetzung für eine *infringement action* durch den Inhaber des *copyrights.*[40]Das

---

[31] Dazu sogleich unter c.

[32] So ist die Frage nach einer unjust enrichment wegen Nutzung einer Idee nach staatlichem Recht zu behandeln, siehe Roger E. Schechter and John R. Thomas, Intellectual Property, The Law of Copyrights, Patents and Trademarks 250 (2003).

[33] David La Lange, Mary Lafrance& Gary Myers, Intellectual Property. Cases and Materiales 729 (3rded 2007).

[34] Robert P. Merges, Peter S. Menell& Mark A. Lemley, Intellectual Property in the new technological age 385 (4th ed. 2007).

[35] Darunter z.B. Audio Home Recording Act of 1992; Digital Performance Right in Sound Recording Act of 1995; No Electronic Theft (NET) Act of 1996 sowie der Digital Millenium Copyright Act (DMCA) of 1998.

[36] Robert P. Merges, Peter S. Menell& Mark A. Lemley, *Intellectual Property in the new technological age* 388 (4th ed. 2007).

[37] 17 USC § 102:

(a) Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. Works of authorship include the following categories:

(1) literary works;

(2) musical works, including any accompanying words;

(3) dramatic works, including any accompanying music;

(4) pantomimes and choreographic works;

(5) pictorial, graphic, and sculptural works;

(6) motion pictures and other audiovisual works;

(7) sound recordings; and

(8) architectural works.

(b) In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.

[38]Robert P. Merges, Peter S. Menell & Mark A. Lemley, Intellectual Property in the new technological age 388 (4th ed. 2007).

[39] 17 USC § 408 (a) letzter Satz: „Such registration is not a condition of copyright protection".

[40] 17 USC §§ 411, 501 (a):

copyright besteht bis zum Tod des Autors plus 70 Jahre darüber hinaus, 95 nach erster Veröffentlichung im Fall eines anonymen Werks, eines Werkes unter einem Pseudonym oder bei einem solchen Werk, das im Rahmen einer Auftragsarbeit („*worksmadeforhire*) angefertigt wurden. Das Copyright endet jedoch spätestens nach 120 Jahren nach Schaffung des Werks.[41]

c. Unfair and deceptive acts and practices statutes als verbraucherschützende Vorschriften für Verbraucherdatenschutz und Schutz vor urheberrechtlichen Einschränkungen

Ein großer Teil des us-amerikanischen Verbraucherschutzes erfolgt über die Marktverhaltensregelungen und die aufsichtsrechtlichen Kompetenzen der zuständigen Behörden. Dies gilt auch für den „Datenschutz" in den USA. Eine verwaltungsrechtliche Durchsetzung des Urheberrechts ist für die Verfasserin nicht ersichtlich.

aa) Verbraucherdatenschutz und Datensicherheit

Ein Schutz der *privacy* erfolgt nicht nur mittels *privacy statututes* und der darin enthaltenen *private right of actions,* sondern auch über verbraucherschützende Eingriffskompetenzen der Behörden, allem voran der FTC und der auf Staatenebene vorhandenen Attorneys General und/oder - falls vorhanden – anderen zum Schutz der Verbraucher agierenden Behörden. Diese Behörden handeln zum einen gestützt auf die ihr durch Gesetz übertragenen spezifischen Durchsetzungskompetenzen der sektoralen Gesetze[42], zum anderen stützen sie sich im Bereich des Schutzes privater Informationen aber auch auf ihre jeweiligen Kompetenzen zum Schutz des Marktes und der Verbraucher vor *unfair or deceptive acts or practices.*[43]

(1) Unfair and deceptive acts and practices (UDAP)

Die FTC stützt ihre Kompetenz für das Vorgehen gegen Unternehmer zum Schutz der *consumer privacy* auf ihre *unfair and deceptive trade practice* Kompetenz aus section 5 FTC Act.[44]Der Standard der *unfairness* hat dabei von der FTC vor allem für den Bereich der Werbung und dem Verkauf von Produkten und Dienstleistungen Anwendung gefunden.[45] Section 5 (n) FTC Act präzisiert das Vorliegen von *Unfairness*.[46] Eine Handlung oder Geschäftspraktik ist dann unfair, wenn sie eine substantielle Verletzung darstellt, die nicht durch etwaige Vorteile ausgeglichen und vom Verbraucher nicht verhindert werden kann. Grundsätzlich bedarf es für

---

[41] 17 USC § 305.

[42] So zum Beispiel 15 USC § 6505 für den COPPA und 15 USC 6805 für Gramm-Leach-Bliley Act hinsichtlich der FTC.

[43] Für die FTC findet sich diese Kompetenz in section 5 FTC Act; für den Attorney General als zuständige Behörde zur Durchsetzung des Wettbewerbs- und Verbraucherrechts ergibt sich diese Kompetenz aus §§ 17200, 17204 Cal. Business and Professions Code.

[44] 15 USC § 45.

[45] Michael D Scott, *The FTC, the Unfairness Doctrine, and data security breach litigation*: *Has the Commission gone too far?*60 Admin L. Rev. 128, 135 (2008).

[46] 15 USC § 45 (n) The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

eine *substantial injury* eines *monetary harms*.[47]Für eine *deception* bedarf es einer *misrepresentation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment.*[48]Auf Staatenebene sind dem FTC Act nachempfundene Gesetze vorhanden, die in ähnlicher Weise unfaire oder täuschende Handlungen gegen einen Verbraucher verbieten.[49]

(2) Datenschutz und Datensicherheit als UDAP Fälle

Die Einbettung von Datenschutzfragen in das UDAP System kommt auf verschiedene Weise in Betracht:

Der erste Fall betrifft die Sachverhalte, in denen bereits eine Verpflichtung zur Geheimhaltung besteht, aber keine explizite Durchsetzung durch die Sondergesetze vorgesehen ist. Beispiel für einen solchen Fall betrifft das Unternehmen *Accusearch Inc*., welches als Betreiber einer Webseite persönliche Daten, darunter Telefonnummern, verkauft hatte. Die Verletzung des Verbots zur Nichtweitergabe der Daten nach § 702 Telecommunications Act of 1996, 47 U.S.C. § 222 wurde von der FTC als eine *unfair trade practice* angesehen.[50]

Sofern eine solche ausdrückliche Verpflichtung hinsichtlich des Umgangs von Daten nicht besteht, wird in einem anderen Fall das UDAP System genutzt: Zwar gilt in den Vereinigten Staaten nur für einen Teil der Branchen oder Verbraucherinformationen eine Pflicht zur Erstellung einer *privacy policy* und der Information über eine solche[51], ein Verstoß gegen eine solche allein freiwillige Datenschutzerklärung wird von der FTC als *deceptive trade practice*, als Täuschung über die Einhaltung der Datenschutzerklärung oder der Datensicherheit, geahndet. Ein Beispiel ist das Verfahren der FTC in der Sache *Life isGood*.[52] Ein Online-Händler hatte in seiner *privacy policy* die Sicherheit der Daten versprochen, obwohl dies in Wahrheit nicht gewährleistet war.

Neuerdings[53] geht die FTC jedoch auch gegen Unternehmen vor, bei denen eine solche vorherige Erklärung fehlt. In diesem Fall stützt sich die FTC dann nicht mehr nur auf eine Täuschungshandlung, sondern auf das Vorliegen einer unfairen Handlung (*unfair trade practice*) bei eingetretenen *data security breaches.*[54] Beispielhaft für ein solches Vorgehen ist auch das Verfahren *FTC v HTC*[55], in der die FTC aufgrund der bestehenden Sicherheitslücken im Android Betriebssystem eine *unfaire trade practice* annahm. Zudem sah die FTC in der Aussage

---

[47] FTC Policy Statement on Unfairness, 17.12.1980; in dem Verfahren ReverseAuction, File No. 0023046 hingegen verzichtete die Mehrheit der Kommissionmitglieder auf ein solches Kriterium (http://www.ftc.gov/os/2000/01/reverseconsent.htm) siehe dazu jedoch die dissenting opinion der Kommissionsmitglieder *Swindle*and*Leary* (http://www.ftc.gov/os/2000/01/reversesl.htm)

[48] FTC Policy Statement on Deception, 14.10.1983.

[49] So zumBeispiel Cal. Business and Professions Code 17200.

[50] FTc v Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009).

[51] So nach 15 USC § 6801 für Finanzinstitute

[52] FTC complaint, In re Life Is Good, Inc., No.C-4218 (F.T.C. Jan. 17, 2008), abrufbar unter http://www.ftc.gov/os/caselist/0723046/080117complaint.pdf; siehe auch United States v Choice Point, Inc. No. 106-CV-0198 (N.D. Ga. Jan. 26. 2005).

[53]Zu dieser Praktik ausführlich Michael D Scott, *The FTC, the Unfairness Doctrine, and data security breach litigation*: *Has the Commission gone too far?* 60 Admin L. Rev. 128, 134 (2008).

[54] Ein datasecuritybreach ist dabei jede von einem Unternehmen unberechtigte oder unabsichtliche Preisgabe, Weitergabe oder Verlust von sensitiven persönlichen Informationen, welche personenbezogene Informationen wie die Social Security number (SSN) oder finanzielle informationen wie die Kreditkartennummern umfassen können, so jedenfalls Michael D Scott, *The FTC, the Unfairness Doctrine, and data security breach litigation*: *Has the Commission gone too far?* 60 Admin L. Rev. 128, 144 (2008).

[55] HTC America Inc, FTC File No. 122 3049.

im Handbuch darüber, dass vor Installierungen von Drittprogrammen ein Hinweis auf Berechtigungen hinsichtlich persönlicher Informationen und Einstellungen erfolge, eine *deceptive trade practice*.[56] Erst nach Installation des entsprechenden Programms würde der Nutzer über den Zugriff des Programms informiert. Die FTC sah darin eine „*false or misleading representation*".

Bei Beginn der Nutzung dieser *unfair doctrine* als Grundlage für ihr Einschreiten für die Datensicherheit, lagen keine *Rules* der FTC, keine *policy statements* oder *guidelines* dahingehend vor, wann ein *data security breach* ein unfaires Verhalten darstellen könnte.[57] Einige *rules* und *guidances* sind jedoch von der FTC bereits herausgegeben worden.[58]

Gerichtsentscheidungen zu der Frage der Möglichkeit der Berufung der FTC auf die Kompetenz zu Aufdeckung und Eingreifen bei *unfair trade practices* sind für die Verfasserin bislang nicht ersichtlich, obwohl eine solche Erweiterung der Kompetenzen in der Literatur kritisiert wird.[59] Diese Kritik stützt sich gerade darauf, dass bei Fehlen eines Versprechens einer gewissen Datensicherheit keine unfaire Geschäftspraktik vorliegen könne.[60] Zudem entstehe oftmals kein *substantial monetar yharm*[61]*,* wenn nach einem *security breach* z.B. durch Neuausstellung von Kreditkarten Schäden bei den Verbrauchern vermieden werden können. Dieser sei jedoch grundsätzlich für eine unfaire Geschäftspraktik erforderlich.[62] Inwieweit *privacy* Verstöße allein ausreichen, um einen *substantial harm* zu begründen, ist nicht entschieden.[63] Die

---

[56] Complaint, HTC America Inc, FTC File No. 122 3049 (http://www.ftc.gov/os/caselist/1223049/130702htccmpt.pdf).

[57] Michael D Scott, *The FTC, the Unfairness Doctrine, and data security breach litigation*: *Has the Commission gone too far?*60 Admin L. Rev. 128, 143 (2008).

[58]So zum Beispiel 16 CFR 682 (Disposal of Consumer Information and records); 16 CFR 314 (Standards for safeguarding customer information).

[59]Zum Beispiel Michael D Scott, *The FTC, the Unfairness Doctrine, and data security breach litigation*: *Has the Commission gone too far?* 60 Admin L. Rev. 128, 158 (2008).

[60] Michael D Scott, *The FTC, the Unfairness Doctrine, and data security breach litigation*: *Has the Commission gone too far?*60 Admin L. Rev. 128, 144 (2008).

[61] In den beiden Verfahren CardSolution Systems, CardSystems Solutions, Inc., No. C-4168 (F.T.C. Sept. 8, 2006), verfügbar unter http://
www.ftc.gov/os/caselist/0523148/0523148CardSystemscomplaint.pdf (zuletzt abgerufen am 30.10.2013), und BJ Wholesale Club, BJ's Wholesale Club, Inc. No. C-4148 (F.T.C. Sept. 20, 2005), abrufbar unter at http://
www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf (zuletzt abgerufen am 30.10.2013), verzichtete die FTC auf das Kriterium eines substantial harm. Hinsichtlich des Verfahrens der FTC gegen DSW Inc. ist bemerkenswert, dass eine class action gegen DSW wegen der Sicherheitslücken mangels *actual injury* durch das Gericht abgewiesen wurde; eine drohende Verletzung durch etwaige Nutzung der durch den Diebstahl erlangten Informationen bei DSW Inc. durch Dritte reiche nicht für den Nachweis eines „actualor imminent injury aus", Key v DSW, Inc., 454 F Supp. 2d 684 (S.D. Ohio 2006); in ähnlicher Weise wurde in Piscotta v Old National Bancorp., 499 F 3d 629, 639 (7th Cir. 2007) das Risiko eines Identitätsdiebstahls in Folge eines Security Breaches nicht als Schaden gewertet.

[62] So Michael D Scott, *The FTC, the Unfairness Doctrine, and data security breach litigation*: *Has the Commission gone too far?*60 Admin L. Rev. 128, 154 (2008).

[63] In der Sache *Reverse Auction* äußerten sich die beiden Kommissionsmitglieder Swindle und Leary bei der Frage des Vorliegens eines *substantial harm* in ihrer *dissenting opinion* dahingehend, dass *privacy concerns* nicht grundsätzlich allein ein Vorgehen gestützt auf Unfairness Erwägungen entgegenstehen; in konkreten Fall lehnten sie eine solche mangels ausreichenden Ausmaßes eine *substantial injury* jedoch ab, http://www.ftc.gov/os/2000/01/reversesl.htm (zuletzt abgerufen am 30.10.2013).

von der FTC bislang angegangenen Unternehmen haben nach einer *consent order* das Verfahren mit der FTC beendet.[64]Auch in den Bundesstaaten gehen die staatlichen Marktaufsichtsbehörden gegen *unfair or deceptive trade practices* hinsichtlich Verbraucherdaten vor.[65]

bb) Schutz vor urheberrechtlichen Einschränkungen

Eine Durchsetzung eines gewissen Schutzes von Verbrauchern bei Urheberrechtsklagen käme über die Kompetenz zur Verhinderung von *unfair and decepetive trade practices* dann in Betracht, wenn übermäßig einschneidende Vertragslösungen zur Ausübung des Urheberrechts vorlägen. Bislang scheint dies in der Literatur und Rechtsprechung jedoch kaum diskutiert zu werden.[66]

2. Ausrichtung und Gegenstände der relevanten Verbraucherbehörden

Da dem us-amerikanischen Zivilrecht die Regel des *caveat emptor* und dem Markt die Idee der Selbstregulierung zu Grunde liegt, bedarf es sowohl für zivilrechtliche als auch verwaltungsrechtliche Befugnisse eines Handelns des jeweiligen Gesetzgebers. Für den Verbraucherschutz sind durch den Federal Trade Commission Act, den *little FTC Acts* auf Staatenebene sowie zahlreichen branchenspezifischen und vertragstypabhängigen Gesetzen verwaltungsrechtliche Durchsetzungsbefugnisse geschaffen worden.[67] Diese Durchsetzung obliegt zahlreichen unterschiedlichen Verbraucherschutzbehörden oder anderen staatlichen Stellen.[68] Die verwaltungsrechtlichen Kompetenzen beschränken sich dabei meist auf den Erlass von *orders* oder *complaints* sowie einer *rulemaking authority*. Ein ausgeprägtes und einheitliches Verwaltungsrecht ist in den USA nicht gegeben.[69] Eine Unterscheidung zwischen öffentlichem Recht und Zivilrecht gibt es in den USA nicht.[70] Im *Adminstrative Procedure Act* von 1946 sind rechtsstaatliche Mindestanforderungen für Verwaltungsverfahren in den USA festlegt, 5 USC §§551ff. Kompetenzen und Verfahrensabläufe sind zumeist in den Regelungen für ein Rechtsgebiet oder für eine bestimmte Behörde enthalten.[71] Ein besonderer Verwaltungsgerichtszug fehlt.[72] Sofern die einzelnen *statutes* den staatlichen Behörden ein Klagerecht einräumen, sind diese Klagen bei den Zivilgerichten einzureichen.[73] Dies gilt insbesondere für den verwaltungsrechtlichen Schutz von *consumer privacy* und *data security*. Da vor allem die FTC für die föderale Ebene sowie die Attorney Generals auf Staatenebene die wichtigsten staatlichen Durchsetzungsstellen des Verbraucherschutzes sowie der *consumer privacy* sind, soll im Folgenden auf diese beiden Behörden eingegangen werden. Neben der FTC sind auch andere föderale Bundesbehörden zur Durchsetzung von „datenschutzrechtlichen“

---

[64] Beispiele dafür sind die Verfahren DSW Inc, CardSolution Systems und BJ’s Wholesale Club (Fußnote 61).

[65] So zum Beispiel das gemeinesame Vorgehen von 37 Staaten gegen Google wegen Speicherung von Verbraucherdaten, welches durch einen Vergleich beendet wurde. Die Vorwürfe von unfairen Geschäftspraktiken ergeben sich indirekt aus dem Vergleich, da im Anhang die jeweiligen UDAP Regelungen der betreffenden Staaten aufgeführt sind (http://www.ct.gov/ag/lib/ag/press_releases/2013/20130312_google_avc.pdf, zuletzt abgerufen am 30.10.2013).

[66]So jedoch Nicola Lucchi, Digital Media & Intellectual Property.Management of Rights and Consumer Protection in a Comparative Analysis 99 (2006).

[67]So z.B. § 47 USC für die *consumer privacy* im Telekommunikationsbereich; ausführende Behörde ist die FCC.

[68] Neben der Federal Trade Commission sind vor allem das Bureauof Consumer Financial Protection, die Consumer ProductSafteyCommission und Food and Drug Administration zu nennen.

[69] Peter Hay, US-Amerikanisches Recht, 5. Auflage, 36.

[70] Ibidem.

[71] Ibidem.

[72] Ibidem.

[73]Siehe dazu unten (2).

Bestimmungen zuständig, wie zum Beispiel der Federal Communication Commissioner hinsichtlich der Regelungen des Federal Communications Act, der auch Bestimmungen zur *consumer privacy* enthält.[74]
Ein behördlicher Schutz des Urheberrechts ist im Rahmen der strafrechtlichen Sanktionen gegeben[75], ein verwaltungsrechtlicher Schutz darüber hinaus besteht nicht. Für den Schutz des Verbrauchers vor übermäßiger Durchsetzung des Urheberrechtsschutzes kommen unterschiedliche Instrumente in Betracht. Diese sind jedoch nicht rein administrativer Art. Sofern zwischen Verbraucher und Rechteinhaber eine vertragliche Regelung hinsichtlich der Nutzung eines urheberrechtlich geschützten Werks vorliegt, könnte ein Eingreifen von Behörden aufgrund des Vorliegens von *unfair practices* erfolgen.[76] Sofern gerichtliche Verfahren gegen den Verbraucher wegen einer Urheberrechtsverletzung bei Vorliegen eines Vertrages zur Gewährung von Nutzungsrechten geführt werden, könnte die common law Regel der „*doctrine of unconscionability*" Anwendung finden[77]. Diese Regelung findet sich in UCC § 2-302 (2002).[78]
Im Copyright Act of 1976 ist neben den zivilrechtlichen Durchsetzungsmöglichkeiten das Verfahren der *criminal sanctions* vorgesehen. Sonstige verwaltungsrechtliche Befugnisse sind im Copyright Act of 1976 nicht niedergelegt. Eine administrative Kontrolle der zivilrechtlichen Verfahren wegen Urheberrechtsverletzungen gegen Verbraucher ist nicht ersichtlich. Unter 4. wird daher allein auf die *criminal sanction* unter dem Copyright Act eingegangen.
Datenschutz und Datensicherheit sind im Ergebnis in den Vereinigten Staaten, sofern die UDAP Regelungen herangezogen werden, marktschützende Normen. Nicht der individuelle Verbraucher und seine individuellen Bedürfnisse oder der Schutz seiner immateriellen Rechtsgüter von *privacy*, Würde oder Selbstbestimmung über eigene Personen sind im Fokus der FTC, sondern die Wiederherstellung des Marktes zu Gunsten der Verbraucher als auch der Verbraucher als Nachfrager.

3. „Verwaltungsrechtliche" Durchsetzung des „Datenschutzrechts"

Im Folgenden werden die Durchsetzungsmöglichkeiten von datenschutzrechtlichen Regelungen durch die FTC sowie kurz die der staatlichen Verbraucherschutzbehörden dargestellt.

a. FTC

Die *Federal Trade Commission* (FTC) hat zwei Hauptaufgaben: Zum einen die Verhinderung von *unfair methods of competition in commerce* und zum anderen die Verhinderung von *unfair*

---

[74] 47 USC § 222; die FCC kann neben den *orders* auch *charges* erlassen, 47 USC § 205.

[75] Siehe dazu unten 4.

[76] Nicola Lucchi, *Digital Media and Intellectual Property. Management of Rights and Consumer Protection in a Comparative Analysis* 110 (2006) verweist darauf, dass durch die verschiedenen admintrativen Möglichkeiten effektive Instrumente zum Schutz des digitalen Verbrauchers vor *unfair or deceptive practices* zur Verfügung stehen.

[77] Nicola Lucchi, Digital *Media and Intellectual Property.Management of Rights and Consumer Protection in a Comparative Analysis* 110 (2006).

[78] § 2-302. Unconscionable contract or Clause.
(1) If the court as a matter of law finds the contractor any clause of the contract to have been unconscionable at the time it was made the court may refuse to enforce the contract, or it may enforce the remainder of the contract without the unconscionable clause, or it may so limit the application of any unconscionable clause as to avoid any unconscionable result.
(2) When it is claimed or appears to the court that the contractor any clause thereof may be unconscionable the parties shall be afforded a reasonable opportunity to present evidence as to its commercial setting, purpose and effect to aid the court in making the determination.

and deceptive trade practices.[79] Darüber hinaus ist die FTC nach zahlreichen Bundesgesetzen –darunter auch solche zum Schutz der *online privacy* und Verbraucherdaten - zuständige Aufsichtsbehörde.[80]

aa) Selbstverständnis der betreffenden Behörden

Die FTC sieht sich in der Aufgabe, den *Verbraucherdatenschutz* hinsichtlich *sensibler* Verbraucherinformation zu gewährleisten und durchzusetzen.[81] Sie baut dabei auf die Durchsetzung der betreffenden *privacy* Regelungen[82], auf ihre *policy advocacy function* sowie auf Verbrauchererziehung und Bildung. [83] Sofern ihre Funktion auf Section 5 des FTC Acts begründet ist, versteht sich die FTC als eine Behörde, welche vor dem Verständnis einer Selbstregulierung des Marktes nur korrigierend eingreift, wenn Missstände am Markt vorhanden sind. Im Blick der FTC ist dabei der Markt als Ganzes, nicht der individuelle Nachfrager oder Verkäufer. Verbraucher werden damit von der FTC ebenfalls nur als besondere Gruppe mit besonderen Bedürfnissen am Markt gesehen. Verbraucherschutz und Verbraucher*datenschutz* durch Handeln und Einschreiten der FTC dient zum Wohle des Marktes und der Gesamtwirtschaft. Hinsichtlich dieser Regelungen ist die FTC Aufsichtsbehörde für sämtliche Nichteinhaltungen, auch wenn hier ebenfalls nur gegen vereinzelte Unternehmen vorgegangen wird, da ein einzelnes Einschreiten auch Auswirkungen für andere Unternehmen hat.[84] In der Vergangenheit ist die FTC dabei auch gegen große Online Unternehmen wie Twitter[85], Google[86] oder Facebook[87] vorgegangen.

bb) Behördenstruktur

Die FTC wurde 1914 durch den Federal Trade Commission Act gegründet. Dem Congress kommt aufgrund Article1 section 8 clause 3 der Verfassung mit der Regelung des Handels die Kompetenz zum Erlass von Regelungen bezüglich der FTC zu.[88]Die Vorschriften zur FTC befinden sich nun im United States Code, Title 15 Chapter 2. Dazu kommen Regelungen im Code of Federal Regulations, 16 CFR 01. -901.1.

---

[79] Richard A. Mann & Barry S. Roberts, *Business Law* 614 (15thedn, 2012). Zu der Erstreckung der *unfair and deceptive acts und practices* Klausel aus 15 USC § 45 auf den Verstoß gegen die eigene *privacy policy* als auch gegen das Prinzip des Datensicherheit siehe oben (2).

[80] So zum Beispiel 15 USC § 6505 für den COPPA und 15 USC 6805 für Gramm-Leach-Bliley Act hinsichtlich der FTC.

[81]FTC Chairmans Report 2011, p. 32 (abrufbar unter http://www.ftc.gov/os/2011/04/2011ChairmansReport.pdf, zuletzt abegrufen 30.10.2013); zustimmend Nancy J.King and V.T. Raja, *What do they really know about me in the cloud? A comparativelawperspective on protectingprivacyandsecurityof sensitive consumerdata* 50 Am. Bus. L.J. 413, 425 (2013) im Hinblick auf den Schutz sensitiver Daten, wobei die Autoren darauf verweisen, dass das Kriterium der Sensibilität von der FTC weit ausgelegt wird.

[82] Darunter fällt auch eine *privacy protection* nach section 5 des FTC Acts welcher der FTC die Aufgabe übertrag „persons, partnerships, or corporations" vor „unfair and deceptive acts or practices" zu schützen

[83] FTC Report 2012, Protecting Consumer in an Era of Rapid Change, (abrufbar unter http://ftc.gov/os/2012/03/120326privacyreport.pdf), ii.

[84]Siehe dazu unten (d).

[85]In the Matter of Twitter, Inc., a corporation, FTC File No. 092 3093.

[8686] In the Matter of Motorola Mobility LLC, a limited liability company, and Google Inc., a corporation,

FTC File No. 121 0120; auch einige Bundesstaaten sind gemeinsam gegen Google vorgegangen, siehe oben Fn.55.

[87]*In the Matter of* Facebook, Inc., a corporation, FTC File No. 092 3184.

[88] De Gorter v. Federal Trade Commission, 244 F.2d 270 (9th Cir. 1957). .

Die FTC ist eine unabhängige Bundesbehörde mit fünf *commissioners*, welche vom Präsidenten ernannt und vom Senat für 7 Jahre bestätigt werden. Nicht mehr als 3 *commissioner* dürfen derselben politischen Partei wie der des Präsidenten angehören. Anderweitige Tätigkeiten sind während der Amtszeit untersagt.[89] Das Recht zur Benennung des Chairman wurde durch den Reorganization Plan No. 8 von 1950, Section 3 auf den Präsidenten übertragen. Derzeit ist John Leibowitz, Jurist mit Karriere im öffentlichen Dienst, Vorsitzender der FTC. Nach dem Reorganization Plan No. 8 von 1950 Section 1[90] wurden auch die administrativen und exekutiven Aufgaben von der Kommission als Ganze auf den Chairman übertragen, wobei jedoch wichtige Entscheidungen die Zustimmung der Kommission als Ganze erfordern.
Die Unabhängigkeit der Federal Trade Commission besteht darin, dass sie außerhalb der *federal executive departments* steht. Ein Kommissionsmitglied kann nur wegen Ineffektivität, *neglect of duty* oder *malfeasance in office* durch den Präsidenten entlassen werden.[91] Bei Ausübung ihrer Kompetenzen ist die FTC frei von anderer exekutiver Kontrolle.[92] Die FTC wird durch staatliche Gelder finanziert, wobei ein kleiner Teil der Kosten durch eigene Erträge gedeckt wird.[93]
Die FTC hat grundsätzlich rein verwaltungsrechtliche Funktionen[94] und ist nicht Teil des Gerichtssystems,[95] obwohl sie in einigen Bereichen selbst als Kontrollinstanz fungiert.[96] Sie ist vom Kongress eingesetzt, daher beschränken sich ihre Kompetenzen auf diejenigen, die der FTC durch einzelne Gesetze aufgetragen wurden.[97]

---

[89] 15 USC § 41.

[90] (Eff. May 24, 1950, 15 F.R. 3175, 64 Stat. 1264).

[91] 15 USC § 41; einschränkende Auslegung bestätigt durch Humphrey'sEx'r v. United States, 295 U.S. 602, 628 (1935).

[92] Commission acts in part as legislative agency and in part as judicial agency, and exercises quasi legislative and quasi judicial functions, and must be free from executive control, Humphrey's Ex'r v. United States, 295 U.S. 602, 628 (1935).

[93] Siehe zu den Finanzen http://www.ftc.gov/opp/gpra/2012parreport.pdf.

[94] The Commission is not a court; it exercises administrative and not judicial power. Eastman Kodak Co. v. Federal Trade Commission, 7 F.2d 994 (C.A.2 1925), affirmed 274 U.S. 619 (1927); see also, American Tobacco Co. v. Federal Trade Commission, 9 F.2d 570 (C.C.A.1925), affirmed 274 U.S. 543 (1927); Chamber of Commerce v. Federal Trade Commission, 280 F. 45 (C.C.A.1922).

[95] The Commission exercises only administrative functions. J.W. Kobi Co. v. Federal Trade Commission, 23 F.2d 41 (C.C.A.1927); N. Fluegelman & Co., Inc. v. Federal Trade Commission 37 F.2d 59(C.C.A.1930); FederalTrade-Commission v. Balme, 23 F.2d 615 (C.C.A.1928), certiorari denied 277 U.S. 598 (1928); Chamber of Commerce of Minneapolis v. Federal Trade Commission, 13 F.2d 673 (C.C.A.1926).

[96] So prüft die FTC nach Erlass eines *complaints* in einem *hearing*, ob eine *order* gegen das betroffene Unternehmen oder die betroffene Person ergehen soll, 15 USC § 45 (b).

[97] Commission is creation of Congress and extent of its powers can be decided only by considering powers Congress specifically granted it in light of statutory language and background. National Petroleum Refiners Ass'n v. F.T.C., 482 F.2d 672 (C.A.D.C.1973) certiorari denied 415 U.S. 951 (1974); Commission is to administer statutes whose meaning and content are primarily entrusted to judiciary for rational extrapolation; there was no intention on part of Congress that Commission should become a plenary body reshaping American industry into a model which the Commission in its wisdom decided best served the nation; on the contrary, Commission was to prevent “unfair competition” in widely diversioned industries, preserving existent price system; Florida East Coast Ry. Co. v. U.S., 259 F.Supp. 993 (M.D.Fla.1966), affirmed 386 U.S. 544(1967).

Die FTC ist in mehrere Offices untergliedert. Neben anderen Offices und Bureaus gibt es das *Bureau of Consumer Protection*.[98] Das *Bureau of Consumer Protection* unterteilt sich in 7 *divisions*(Abteilungen). Diese sind *Adverstising Practices, Financial Practices, Marketing Practices; Privacy and Identity Protection, Planning and Information, Consumer und Business Education,* sowie *Enforcement.* 1999 wurde zudem ein *Advisory Committee on Online Access and Security* ins Leben gerufen, welchem der FTC beratend bei der Frage der Implementierung von *fair information practices* für nationale kommerzielle Webseiten zur Seite stand.[99]
Direktor des Bureau of Consumer Protection ist derzeit David Vladeck, welcher vom Vorsitzenden der FTC ernannt wurde.[100] Vladeck kam seinem Ruf einer verbraucherfreundlichen Neubesetzung nach, indem er kurz nach seiner Benennung ankündigte, verstärkt gegen *privacy* Verstöße im Internet – auch durch ein aufgestocktes Budget- vorgehen zu wollen.[101]

cc) Befugnisse und informationelle Verfahrensweisen

Der Federal Trade Commission stehen unterschiedliche administrative Instrumente sowie auch Möglichkeiten der Erhebung von Zivilklagen zu. Gestützt auf die Kompetenz zur Verhinderung von *unfair and deceptive acts and practices* können neben einem Vorgehen im Einzelfall (*adjudication*) auch Regelungen im Allgemeinen durch Nutzung informeller (z.B. *joint statements*) oder formeller Mittel (*rules*) getroffen werden, um verbraucherdatenschützende Ziele zu erreichen. Sofern die jeweiligen *statutes* es vorsehen, können diese *statutes* ebenfalls eine *rulemaking authority* geben.[102]

(1) Präventive und regulatorische Mechanismen aller Marktteilnehmer

Eine präventive Regulierung hinsichtlich antizipierter Gefahren wird von den us-amerikanischen Behörden, vor allem von der FTC, vorwiegend nicht vorgenommen. Sofern durch Beobachtungen des Marktes Missstände erkennbar werden, werden regulatorische oder anderweitige Maßnahmen ergriffen.

(a) Policy Advocacy

Die FTC veranstaltet Workshops zu ausgewählten Themen, steht dem Congress als beratende Agency zur Verfügung, gibt Untersuchungen in Auftrag und macht Gesetzgebungsvorschläge.[103] Der 2012 veröffentlichte Report zur *privacy* soll zum Beispiel den Unternehmen als *best practice* Beispiel dienen und dem Gesetzgeber bei künftigen Gesetzgebungsvorhaben beraten.[104]

---

[98] Waller, Spencer Weber, Brady, Jillian G. and Acosta, R.J., Consumer Protection in the United States: An Overview (January 12, 2011). European Journal of Consumer Law, May 2011(abrufbar unter http://ssrn.com/abstract=1000226).

[99] Das Advisory Committee on Online Access und Security wurde nach dem Final Report 2012 wieder aufgelöst.

[100] *Vladeck* war vor seiner Benennung sieben Jahre Professor am Georgetown University Law Center, wobei er zudemDirektor des Center on Health Regulation and Governance of the O'Neill Institute for National and Global Health Law war. Davor war Vladeck fast 30 Jahre als Anwalt für die Public CitizenLitigation Group, den prozessrechtlichen Zweig von Public Citizen tätig, welcher von Nader gegründet wurde und sich für die Durchsetzung von Rechten der Verbraucher einsetzt.

[101] http://www.nytimes.com/2009/08/05/business/media/05ftc.html (zuletzt abgerufen am 30.10.2013).

[102] So zum Beispiel der Childrens Online Privacy ProtectionAct in 15 USC § 6502 (b) (1).

[103] FTC Report 2012, ii (Fn. 83)

[104] FTC Report 2012, iii, (Fn. 83); der Report soll nicht bei der Durchsetzung des bestehenden Rechts als Auslegungsmaterial dienen.

Als eine reine Empfehlung für Online Händler hat die FTC *Fair Information Principles* (*FIPs*) formuliert.[105]Diese bestehen aus *Notice, Choice, Access and Security* sowie *Enforcement*. Bislang sind diese nicht verpflichtend und weder durch die FTC noch durch andere Behörden durchsetzbar. Sie sind ein Beispiel für den Selbstregulierungsansatz. Die FTC untersucht jedoch regelmäßig die Selbstregulierung durch die einzelnen Branchen und Industrien und versucht, die betreffenden Unternehmen von der Nutzung der *best practice* Standards zu überzeugen, welche die FTC in ihren veröffentlichten Berichten empfiehlt.[106] Die FTC verfolgt auch in dem bislang nicht regulierten Bereich den Ansatz der Selbstregulierung durch *privacy disclosures*.[107]

(b) Model Clauses für Unternehmen

Zum anderen kann die FTC z.B. *Model Clauses* herausgeben. Der Gramm-Leach-Bliley Act schreibt Finanzinstituten beispielsweise den Entwurf und die Information über eine *privacy policy* vor.[108] Durch den Financial Services Regulatory Relief Act of 2006 sind die betreffenden Aufsichtsbehörden verpflichtet, eine solche *model privacy clause* für die Erfüllung der Voraussetzungen des Gramm-Leach-BlileyActs[109] herauszugeben, welche dann bei Benutzung als „*safe harbor*" Bestimmung für die Unternehmen Wirkung entfaltet: Die Nutzung der *model clause* wird als Einhaltung der *privacy policy* Verpflichtung gewertet.[110] Die Nutzung der *model clause* ist jedoch nicht verpflichtend. Eine solche *model clause* wurde 2009 von der FTC mit sieben anderen föderalen Behörden herausgegeben.[111] Andere *model clauses* wurden aufgrund ähnlicher Verpflichtung anderer Verbraucherschutzbehörden herausgegeben.[112]

(c) Rulemaking Authority und Informal Rules

Die FTC hat nach 15 USC §§ 46 (g), 57a eine Kompetenz zum Erlass von *trade regulations*, welche unfaire und irreführende Handelspraktiken nach 15 USC § 45 (a) (1) genauer definieren können. Eine solche *rulemaking authority* kann der FTC auch durch Gesetz übertragen werden. Für den COPPA ist dies mit Title 15 USC § 6502 (b) geschehen, welcher der FTC die Aufgabe überträgt, *regulations* zu erlassen. Diese betreffen das Erheben von Daten von Kindern, die Einholung von elterlichen Einwilligungen sowie Auskunftsrechte bezogen auf die Daten des Kindes. Die *regulations* finden sich nun in Title 16 CFR § 312.1-13. Der Verstoß gegen eine *regulation* gilt dabei als Verstoß gegen die Vorgaben aus der jeweiligen Statute[113], bzw. der *unfair and deceptive* Klausel[114].

Insbesondere bis in die 70er Jahre wurde durch die FTC der *adjudication* Ansatz verfolgt, welcher sich dadurch kennzeichnet, dass die Politik durch Einzelfallentscheidungen betrieben

---

[105]http://www.ftc.gov/reports/privacy3/fairinfo.shtm (zuletzt abegerufen am 30.10.2013.)

[106] Für Mobile Apps ist hier der FTC Staff Report 2013, „Mobile Privacy Dicslosures. Building Trust TroughTransparency" herzunehmen, abrufbar unter http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf (zuletzt abgerufen am 30.10.2013); ebenso der FTC Kidd App Report 2012 http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf (zuletzt abegerufen am 30.10.2013).

[107] FTC Report 2012, ii, http://ftc.gov/os/2012/03/120326privacyreport.pdf (zuletzt abgerufen am 30.10.2013).

[108] 15 USC § 6801 (a).

[109] 15 USC § 6801 (b).

[110] 15 USC § 6802 (e) (4).

[111] Siehe dazu http://www.sec.gov/rules/final/2009/34-61003.pdf (zuletzt abegerufen am 30.10.2013).

[112] So zum Beispiel für 15 U.S.C. § 1681g (Fair Credit Reporting Act) durch das Bureauof Consumer Financial Protection als *model summary* für die Rechte des Verbrauchers nach dem Fair Credit Reporting Act.

[113] Für den COPPA ist dies in 16 CFR § 312.9 festgelegt.

[114] 15 USC § 57a (d) (3).

wird.[115] Ob *regulations* erlassen werden oder der Ansatz der *adjudication*[116] gewählt wird, steht der FTC frei.[117] Auch wird der FTC ein nicht zu unterschätzender Spielraum für den Erlass von informellen Regelungen eingeräumt, für die es nicht des offiziellen Verfahrens bedarf. [118]

(aa) Informelle und Formelle Rules

Grundsätzlich kann zwischen zwei verschiedenen Regelungstypen unterschieden werden: Zum einen die informellen Regelungen, *interpretative rules* und *general statements of policy,* und zum anderen die formellen *rules*. Nur für letztere bedarf es eines besonderen *rulemaking process*.

Informelle Regelungen hingegen können von der FTC zu einer Vielzahl von Themen herausgegeben werden und geben oftmals die aktuellen Bestrebungen der FTC oder ihr Verständnis der jeweiligen Regelungen wieder. Für informelle Regeln haben die Gerichte eine strikte Pflicht zur Beachtungs der Ansichten der FTC nicht befürwortet, sondern ihnen nur eine „*power to-persuade*" zugesprochen, da den informellen Empfehlungen gerade eine formelle Gesetzeskraft fehle. [119]

Interpretative rules und *policy guidance* sind aufgrund der Beschränkungen im *rulemakingprocess* in der Praxis eher favorisiert.[120] Grundsätzlich sind die Konkretisierungen von Gesetzen durch die Aufsichtsbehörden zulässig und notwendig, wenn ausdrücklich oder implizit aufgrund des nicht eindeutigen Wortlauts den Behörden die Konkretisierungskompetenz zukommt. Bei einer solchen Konkretisierungskompetenz darf das Gericht in einem Verfahren dann nur in sehr engen Grenzen die Ansicht der Behörde außer Kraft setzen.[121]Für den Bereich des „Datenschutzes" sind jedoch solche informellen *guidelines* nicht besonders ersichtlich. Die FTC gibt ihre Empfehlungen vielmehr bereits in allgemeiner Form und in ihrem Report wieder.[122]

(bb) Rulemaking authority nach Title 5 USC §§ 553 ff

Das Verfahren zum Erlass von *rules*, bzw. *regulations* im Allgemeinen ist in 5 USC §§ 553ff geregelt.[123] Sofern die betreffende Behörde *regulations* erlässt, zu denen sie verpflichtet oder befugt ist, ist zuerst die Einleitung eines solchen Verfahrens unter Angabe der Zeit, des Ortes und der Art der regulation sowie der rechtlichen Grundlage und einer Beschreibung des Inhalts und der rechtlichen Fragen im Federal Register bekanntzugeben. Dieses formelle *rulemaking* Verfahren ist grundsätzlich erforderlich, es sei denn, ein anderes Verfahren wird angeordnet,

---

[115] Sam Kalen, Guidance Documents and the Courts 57 RMMLF-INST 5-1 (2011)

[116] *Adjudication* meint die Konfliktlösung im Einzelfall, entweder durch die Beilegung des Streitfalls durch eine consentorder oder durch die gerichtliche Überprüfung einer FTC Maßnahme durch die Gerichte, siehe Jessica Horne, Pink-Profiters: Cause-related Marketing and the Exploitation of consumers' consciences 81 Geo. Wash. L. Rev. 223, 240.

[117] Securities and Exchange Commission v. Chenery Corp. (Chenery II) 332 US. 194 (1947); North American Van Lines, Inc. v. U. S., 412 F.Supp. 782 (N.D.Ind.1976).

[118] Wagner Elec. Corp. v. Volpe, C.A.3 1972, 466 F.2d 1013.

[119] Zu diesem Punkt ausführlich Sam Kalen, Guidance Documents and the Courts 57 RMMLF-INST 5-1 (2011); siehe die Gerichtsentscheidungen Christensen v. Harris County 529 U.S. 576 (2000); ebenfalls etwas unklar, aber gegen eine strikte Beachtungspflicht United States v. Mead Corp.533 U.S. 218 (2001).

[120] Am. Radio Relay League, Inc. v. FCC, 524 F.3d 227, 248 (D.C. Cir. 2008); Sam Kalen, Guidance Documents and the Courts 57 RMMLF-INST 5-1 (2011); ein formelles *rulemaking* bedarf es für die informellen Absprachen gerade nicht Action For Children's Television v. F. C. C., 564 F.2d 458 (C.A.D.C.1977).

[121] Chevron U.S.A., Inc. v. NRDC, 467 US.837, 844, 865-66 (1984).

[122] So zum Beispiel in FTC Staff Report „ „Mobile Privacy Disclosures" (http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm, zuletzt abgerufen am 30.10.2013).

[123] Im FTC Act wird auf diesen Mechanismus durch 15 USC § 57a (b) (1) verwiesen.

die betreffenden Regelungen sind reine Empfehlungen oder *interpretive rules* oder die Durchführung eines solchen formellen Verfahrens widerspräche nach den gegeben Umständen nach begründeter Ansicht der Behörde den Grundsätzen der Praktikabilität, Notwendigkeit und öffentlichem Interesse.[124] Dies gilt auch für die Änderung von *regulations*.[125] Nach Erlass der *notice* ist den betreffenden interessierten Kreisen durch Einreichung von Stellungnahmen und Argumenten mit oder ohne persönlichen Vorträgen die Möglichkeit der Teilnahme an dem *rulemaking* Prozess zu gewähren.[126] Die betreffende Behörde hat neben der *regulation* selbst eine Begründung zu geben.[127] Grundsätzlich ist die *regulation* 30 Tage vor Inkrafttreten zu veröffentlichen.[128] Jeder Person steht das Recht zu, sich gegen die betreffende Behörde zu wenden, um den Erlass, die Änderung oder Rücknahme einer solchen *regulation* zu erreichen.[129] Bestimmte *rulemaking* Verfahren erfordern ein *agency hearing*, über das –sofern gesetzlich vorgesehen - gewisse Personen und Institutionen zu informieren sind.[130] Sofern ein *agency hearing* durch ein Gesetz im Rahmen des *rulemaking procedures* durchzuführen ist, gilt nicht § 553 (c) sondern die Bestimmungen der §§ 556, 557.[131] Den betreffenden Kreisen ist auch in dieser Verfahrensart die Möglichkeit zur Beteiligung zu geben, wobei die Beteiligungsmöglichkeiten auch den Beratungsprozess wie z.B. Änderungsanträge betreffen. [132] Die Beteiligungsrechte der betroffenen Kreise dienen grundsätzlich dem Erfahrungsgewinn für die Behörde sowie auch dem Austausch zwischen der Behörde und den betroffenen Kreisen, um die Flexibilität, Offenheit und Fairness der FTC zu gewährleisten.[133] Bei dem Verfahren durch *general notice* (*notice and comment procedure*) bedarf es nicht der Information über jede mögliche Einzelregelung,[134] sofern jedoch mehr als 50 % der Sachfragen nicht in der *general notice* bekannt gemacht wurden, reicht dies nicht aus.[135] Es reicht in der Regel aus, wenn sich die finale Regelung aus der Zusammenschau von *notice* und den daraus folgenden Kommentaren ergibt; einer zweiten Runde der *notice* bedarf es dann nicht.[136] Fehlt eine Beteiligung der betreffenden Kreise grundlegend oder liegt ein anderer erheblicher Fehler bei Verletzung der

---

[124] 5 USC § 553 (b); für die einschränkende Auslegung der Ausnahmen siehe Environmental Defense Fund, Inc. v. Gorsuch, 713 F.2d 802 (C.A.D.C.,1983); Center for Auto Safety v. Tiemann 414 F.Supp. 215 (D.C.D.C. 1976); je größer die Auswirkungen der betreffenden Rule, desto enger müssen die Ausnahmeregelungen gelesen werden, Natural Resources Defense Council, Inc. v. Securities and Exchange Commission 389 F.Supp. 689 (D.C.D.C. 1974).

[125] Owner-Operator Independent Drivers Ass'n, Inc. v. Federal Motor Carrier Safety Owner-Operator Independent Drivers Ass'n, Inc. v. Federal Motor Carrier Safety Admin. 494 F.3d 188 (C.A.D.C.,2007).

[126] 5 USC § 553 (c) sentence 1.

[127] 5 USC § 553 (c) sentence 2.

[128] 5 USC § 553 (d); eine Ausnahme gilt z.B. bei rein interpretativen Vorschriften oder solcher, die eine Ausnahme oder eine Beschränkung lockert.

[129] 5 USC § 553 (e).

[130] 5 USC § 554 (b).

[131] Diese gelten nach 15 USC § 57a (b) (1) jedoch nicht für das FTC *rulemaking* Verfahren.

[132] Siehe 5 USC § 554 (c).

[133] Natural Resources Defense Council, Inc. v. Securities and Exchange Commission 389 F.Supp.689 (D.C.D.C. 1974); Brown Exp., Inc. v. U.S. 607 F.2d 695 (C.A.5, 1979); Texaco, Inc. v. Federal Power Commission, 412 F.2d 740 (C.A.3 1969).

[134] State of S.C. ex rel. Tindal v. Block, 717 F.2d 874 (C.A.4 S.C. 1983), certiorari denied, 465 U.S. 1080 (1984).

[135] Council Tree Communications, Inc. v. F.C.C., 619 F.3d 235 (C.A.3 2010), certiorari denied 131 S.Ct. 1784 (2011).

[136]Omnipoint Corp. v. F.C.C, 78 F.3d 620 (C.A.D.C.1996); Health Ins. Ass'n of America, Inc. v. Shalala, 23 F.3d 412 (C.A.D.C.1994), certiorari denied 115 S.Ct. 1095 (1995).

Beteiligungsrechte vor, entfaltet die *regulation* keine Wirkung.[137] Die fehlende Beteiligung im *notice and comment* Verfahren schließt die nachträgliche Überprüfung der Geltung der *rule* durch ein betroffendes Unternehmen nicht aus.[138] Fehlende Beteiligung am *notice and comment* Verfahren ist nicht erst vor Gericht, sondern schon gegenüber der betreffenden Behörde zu erheben.[139]

Der Erlass von *regulations* unterliegt neben den Anforderungen des 5 USC 553 auch anderen Beschränkungen, sodass neuerdings ein Rückgang solcher *regulations* zu sehen ist, was sicherlich auch dem „*hardlook*"[140] approach der Gerichte zuzuschreiben ist.[141] Erlässt die betreffende Behörde *regulations,* so werden die Unterlagen, Berichte und Protokolle des *rulemaking* Verfahrens sehr genau dahingehend überprüft, ob die Behörde willkürlich gehandelt, gegen gesetzliche Bestimmungen verstoßen oder ihr Ermessen missbraucht hat. Auch die Kenntnisnahme und Einholung sämtlicher Daten wird von den Gerichten nach dem „*hardlook*" geprüft.[142] Fehlt eine ausreichende Begründung der *rule,* kann der Fehler im Einzelfall entweder durch dementsprechendes Verhalten der Behörde geheilt oder vom Gericht ausgesetzt werden.[143] Die Hürden für formelle *regulations* sind damit größer als für informelle Regelungen. Sofern sie der Überprüfung standhalten, sind sie jedoch rechtliche verbindliche Standards, welche in einem gerichtlichen Verfahren nicht durch die Ansicht des Gerichts ersetzt werden können.

(cc) Rulemaking authority im FTC Act

Die FTC hat im Rahmen ihrer Aufgabe des Schutzes vor unfairen und irreführenden Handelspraktiken eine eigenständige *rulemaking authority* in 15 USC § 57a. Für die FTC *rules* gelten zusätzliche, teils von den 5 USC §§ 553 abweichende Regelungen.[144] Die FTC hat bei dem Erlass von Regelungen nach 15 USC § 57a in der betreffenden *notice* bereits den Text der Regelung, eienn Alternativtext und eine Begründung anzugeben, § 57a (b) (1). Vor Erlass dieser *notice* ist bereits eine *advance notice* abzugeben, welche den Bereich, Ziele und Alternativen für eine *rule* aufzeigt sowie die betreffenden Personen zu diesem Verfahren einlädt, 15 USC § 57a (b) (2) (A). Den interessierten Personen müssen die Möglichkeiten gegeben sein, schriftliche Stellungnahmen abzugeben, welche die FTC dann zu veröffentlichen hat, sowie weiterhin auch informelle Anhörungen durchzuführen. Der fertigen *rule* müssen ein Statement und eine Begründung angefügt sein, 15 USC § 57(b). Eine *rulemaking authority* nach 15 USC § 57a – also außerhalb anderer gesetzlicher Regelungen- steht unter dem Vorbehalt, dass die von der *rule* erfassten verbotenen Handlungen weit verbreitet sind; dies erfordert das Vorliegen von *cease-and-desist orders* oder andere Arten von Informationen, welche ein *widespread pattern of unfair and deceptive acts or practices* nachweisen. Zudem kann die

---

[137] So z.B. U.S. v. Utesch 596 F.3d 302 (C.A.6 (Tenn.),2010.).

[138] Fleming Companies, Inc. v. U.S. Dept. of Agriculture, 322 F.Supp.2d 744 (E.D.Tex.2004), affirmed 164 Fed.Appx. 528, 2006 WL 237854; anders jedoch noch Tex Tin Corp. v. U.S. E.P.A., 935 F.2d 1321 (C.A.D.C.1991) opinion after remand 992 F.2d 353 (C.A.D.C.,1993)

[139]Pacific Gas and Elec. Co. v. F.E.R.C., 533 F.3d 820 (C.A.D.C.2008).

[140]Harold Leventhal, "Environmental Decisionmaking and the Role of the Courts," 122 U. Pa. L.Rev.509 (1974).

[141]Sam Kalen, Guidance Documents and the Courts 57 RMMLF-INST 5-1 (2011); Am. Radio Relay League, Inc. v. FCC, 524 F.3d 227, 248 (D.C. Cir. 2008).

[142] Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29 (1983); Sam Kalen, Guidance Documents and the Courts 57 RMMLF-INST 5-1 (2011); siehe zudem die Anforderungen in 5 U.S.C. § 706.

[143] Independent U.S. Tanker Owners Committee v. Dole, 809 F.2d 847 (C.A.D.C.1987).

[144] Siehe 15 USC § 57a und § 57b-3. 15 USC § 57b-3 (b) sieht zum Beispiel die Veröffentlichung einer *preliminary regulatory analysis* vor. Nur das gänzliche Fehlen einer solchen Analyse kann zur Aufhebung der *rule* wegen Verstoß gegen diese Voraussetzung führen.

FTC nicht aus rein eigenem Interesse ein solches *rulemaking* Verfahren anstreben, sondern der Erlass solcher Regelungen muss im *public interest* sein.[145] Die Änderung oder Rücknahme einer Regelung nach 15 USC § 57a (a) (1) (B) unterliegt der gleichen richterlichen Kontrolle wie der Erlass einer Regelung, Title 15 USC § 57a (d) (2) (B)[146], es sei denn, die Auswirkungen einer solchen Änderung sind gering.[147] Innerhalb von 60 Tagen nach Erlass der *rule* kann jede interessierte Person, auch Verbrauchergruppen, vor Gericht eine *petition for judicial review* der betreffenden *rule* einreichen, Title 15 USC § 57a (e) (1) (A). Grundsätzlich gelten die oben genannten Gründe für das Aussetzen der *rule.*[148] Das Gericht kann die betreffende *rule* außer Kraft setzen, wenn eine der in Title 5 USC § 706 (2) A bis C genannten Gründe vorliegen[149], kein ausreichender Nachweis im *rulemaking record* vorliegt oder die Rechte auf *cross examination* im informellen Beteiligungsverfahren missachtet oder nicht ausreichend gewährt wurden und dadurch der FTC nicht sämtliches für eine faires *rulemaking* Verfahren erforderliche Material vorlag.[150] Der Inhalt und die Adäquatheit der Stellungnahme zu den Gründen und den Fakten für den Erlass der Regelung unterliegen nicht der gerichtlichen Kontrolle, 15 USC § 57a (e) (5) (C). [151]
Die gerichtliche Kontrolle der Änderungen ist auf substantielle Änderungen beschränkt.[152] Es bedarf gerade eines „*substantial evidence*“ für ein Verhalten, welches *arbitrary, capricious, abuse of discretion, or otherwise not in accordance with law* ist.[153]

(2) Investigative Powers

Hauptdurchsetzungsfunktion des Verbraucherdatenschutzes ist neben der *rulemaking authority* die repressive Funktion der FTC, wobei ein solches Vorgehen gegen einzelne Unternehmen auch für andere Marktteilnehmer Konsequenzen hat.

(a) FTC als Ansprechpartner bei Beschwerden

Die FTC dient als Ansprechpartner für Beschwerden von einzelnen Verbrauchern, wobei eine solche Beschwerde auch per Internet gemacht werden kann.[154] Die Beschwerden, die bei der FTC eingehen, werden in eine Datenbank eingegeben, welche auch anderen Verbraucherschutzbehörden zugänglich ist und von diesen genutzt wird.[155]

---

[145] 54A Am. Jur.2d Monopolies and Restraints of Trade § 1170.

[146] Eine Ausnahme ist der Erlass einer Ausnahme, 15 USC § 57a (d) (2) (B).

[147] 15 USC § 57b-3 (a) (1); eine der genannten Gegenausnahmen ist dabei ein jährlicher Effekt auf die nationale Wirtschaft von 100.000.000 $ und mehr.

[148] So auch Pennsylvania Funeral Directors Ass'n, Inc. v. F.T.C., 41 F.3d 81 (C.A.3 1994): Court reviewing Federal Trade Commission (FTC) regulation rule may set aside FTC conclusion if it is not supported by substantial evidence in rule-making record taken as whole, or if it is arbitrary, capricious, abuse of discretion, or otherwise not in accordance with law; substantial evidence standard applies only to FTC's factual determinations, while arbitrary and capricious standard applies to all other determinations and conclusions”.

[149] 15 USC § 57a (e) (A).

[150] 15 USC § 57a (e) (B).

[151] Allerdings Konsultation der Stellungnahme für das Gericht als zulässig erachtet in American OptometricAss'n v. F. T. C., 626 F.2d 896 (D.C. Cir. 1980).

[152] Funeral Consumer Alliance, Inc. v. F.T.C., 481 F.3d 860 (C.A.D.C.2007).

[153] Pennsylvania Funeral Directors Ass'n, Inc. v. F.T.C., 41 F.3d 81 (C.A.3 1994); Consumers Union of U.S., Inc. v. F.T.C., 801 F.2d 417 (C.A.D.C.1986).

[154]https://www.ftccomplaintassistant.gov/#&panel1-1 (zuletzt abgerufen am 30.10.2013).

[155] Der Bericht des Sentinel Networks für 2012 findet sich online unter http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf (zuletzt abgerufen am 30.10.2013).

(b) Civil Investigative Demands& Reports

Die FTC hat eine *investigative authority* um *deception, unfair activities* oder Verletzungen der anderen Vorschriften, zu deren Durchsetzung sie ebenfalls befugt ist, zu erkennen.
Die FTC hat grundsätzlich für ihren Aufgabenzweck ein umfangsreiches Recht auf Kopie sämtlicher Unterlagen von einer von der Untersuchung betroffenen Person oder eines solchen Unternehmens, 15 USC § 49. Jedes Mitglied der Kommission kann *subpoenas* unterschreiben, Zeugenaussagen, auch unter Eid, sowie andere Beweise entgegennehmen. Die Durchsetzung dieser investigativen Befugnisse ist durch die Gerichte möglich; der Verstoß gegen dem Nachkommen einer solchen beantragten *order* zur Durchsetzung der *subpoenas* stellt einen *contempt of court* dar.[156] Das Nichtbefolgen der Ladung zu einer Anhörung oder einer Ladung als Zeuge kann als *offense* geahndet werden, 15 USC § 50.[157]
Der erste Schritt –auch im Rahmen eines *complaint*-Verfahrens- ist dabei der Erlass von *civil investigative demands* (CID), um mögliche Verletzungen aufzudecken. Die Regelungen diesbezüglich finden sich in 15 USC § 57b-1. Nach 15 USC § 57b-1 (c) (1) kann die FTC eine CID erlassen, wenn es *reason to believe* (Grund zur Annahme) hat, dass eine Person in Besitz oder Kontrolle von Material ist, welche mit *unfair or deceptive practices* in Verbindung steht. Der *reason to believe* steht im Ermessen der Behörde und unterliegt nicht der *judicial review.*[158]Wie eine *subpoena* dient ein CID dazu die Zusammenstellung von bestehenden Dokumenten oder die Abgabe einer Zeugenaussage sowie schriftlicher Stellungnahmen und Antworten auf Fragen zu erreichen. Der Vorteil ist, dass damit Informationen direkt an der Quelle gesammelt werden und auch die Bereitschaft zur Verhandlung und außergerichtlichen Einigung groß ist. Ein Nachteil besteht darin, dass durch den zivilgerichtlichen Weg Zeit verstreicht, in der z.B. die Unternehmen Beweismittel vernichten können. Untersuchungen können dabei durch Aufforderungen des Präsidenten oder Kongresses, der Gerichte, der Verbraucherbeschwerden oder durch interne Vorgänge ausgelöst werden. Neben diesen CIDs kann die FTC auch Antworten auf Fragen sowie Reports von Personen und Unternehmen anfordern, 15 USC § 46 (b).

(c) Complaint

Wenn die FTC Grund zur Annahme (*reason to believe*) hat, dass eine Person oder ein Unternehmen unfaire Geschäftspraktiken oder unlautere Wettbewerbsmethoden verfolgt oder verfolgt hat und wenn zudem das Einschreiten der FTC im öffentlichen Interesse ist, kann die FTC ein *complaint* gegen die betreffende Person oder das Unternehmen mit dem jeweiligen Vorwurf erlassen. Zudem wird gleichzeitig eine Anhörung angesetzt, die innerhalb der nächsten 30 Tage stattfinden muss, 15 USC § 45 (b) S.1. Dieser *complaint* ist keine bindende Feststellung eines Verstoßes.
Die FTC muss sich nicht gegen jedes Unternehmen mit der betreffenden Praktik wenden, auch wenn alle die gleiche Praktik anwenden.[159] Das Handeln der FTC muss dabei dem öffentlichen Interesse dienen (*public interest*). 15 USC § 45 (b) (1). Die Anforderungen an den *public interest* sind relativ gering, da nicht zwangsläufig Rechtsgüter wie die Gesundheit oder das wirtschaftliche Gemeinwohl betroffen sein müssen. Der Supreme Court erkennt in jeder Verletzung des Rechtsgutes einer Privatperson beispielweise ein solches *public interest* an.[160] Im

---

[156]15 USC § 49.

[157] Dies gilt auch bei anderen Handlungenb, wie z.B., bei Falschaussage.

[158] Boise Cascade Corp. v. F.T.C., 498 F.Supp. 772 (D.C.Del.1980), stay denied 498 F.Supp. 782 (D.C.Del., 1980).

[159] Without simultaneously proceeding against all firms in an industry, the Commission has the discretionary power to enter an order against one firm that is practicing an industrywide illegal trade practice. Johnson Products Co. v. F.T.C. 549 F.2d 35 (C.A.7 1977); ähnlich Ger-Ro-Mar, Inc. v. F.T.C., 518 F.2d 33 (C.A.2 1975),

[160]Radiant Burners, Inc. v. Peoples Gas Light & Coke Co., 364 U.S. 656 (1961).

Ergebnis ist der *private interest test* eine Form der *rule of reason*.[161] Allerdings bedeutet dies nicht eine fehlende Signifikanz dieses Kriteriums. Für das Einschreiten des FTC ist dieses Element von Bedeutung. Es muss eine irgendwie geartete Markt-, bzw. Verbrauchergefährdung[162] und nicht nur ein reiner privatrechtlicher Streit zwischen zwei Mitbewerbern vorliegen.[163] Das Erfordernis eines *public interest* muss spezifisch und substantiert vorliegen,[164] auch wenn dies von den Gerichten nicht in jedem Fall als Voraussetzung geprüft wird. Liegt ein *public interest* nicht vor, kann die *order* der FTC aufgehoben werden.[165] Grundsätzlich steht der FTC jedoch ein großes Ermessen hinsichtlich der Beurteilung eines *public interests* zu.[166] Die FTC nimmt die Verbraucher damit als Ganzes wahr, nicht den einzelnen Verbraucher als solches bzw. bei Verletzung einzelner subjektiver Rechte. Bei den dann zu untersuchenden Unternehmen kann sich die FTC bei mehreren Unternehmen mit ähnlichen Geschäftspraktiken auf solche bzw. nur auf denjenigen, der den consumers den größten Schaden zufügt, beschränken.[167] Die Complaint Database FTC dient dazu, die in Frage kommenden Geschäftspraktiken, Unternehmen und Zeugen für Rechtsverstöße zu identifizieren. Es folgt eine Anhörung vor einem Administrative Law Judge gem. 15 USC § 45 (b). Bei der Anhörung kann dann die betreffende Person/das betreffende Unternehmen erklären, warum eine solche Verletzung nicht stattgefunden hat, so dass keine *cease-and-desist-order* ergeht, 15 USC § 45 (b). Bei dieser Anhörung kann jede Person oder jedes Unternehmen, welche/welches einen *good cause* zeigt, teilnehmen. Die Beteiligung am Verfahren steht jedoch im Ermessen der FTC.[168] Zeugenaussagen finden in dem Verfahren nicht statt, da grundsätzlich nur schriftliche Aussagen zugelassen sind, 15 USC § 45(b).

(d) Cease-and-Desist Orders.

Wenn die FTC nach der Anhörung der Ansicht ist, dass eine Verletzung des FTC Acts oder einer anderen Regelung stattgefunden hat oder stattfindet, wird dies in einem Bericht festgehalten. Zudem wird eine *cease and desist order* gegen die betreffende Person/das Unternehmen erlassen, mit dem Inhalt, das betreffende Verhalten zu beenden. Die Regelungen für den Erlass eines solchen *reports* und der *cease- and-desist order* sind in 15 USC § 45 (c) enthalten. Eine Order beschreibt, was das betroffene Unternehmen zukünftig zu unterlassen hat, aber

---

[161] Louis Altmann and Malla Pollack, Callmann on Unfair Comp., Tr. & Mono. § 4:24 (4th ed. 2012)

[162] F.T.C. v. Klesner, 280 U.S. 19 (1929): "*The public interest must be specific and substantial. Often it is so, because the unfair method employed threatens the existence of present or potential competition. Sometimes because the unfair method is being employed under circumstances which involve flagrant oppression of the weak by the strong. Sometimes, because, although the aggregate of the loss entailed may be so serious and widespread as to make the matter one of public consequence, no private suit would be brought to stop the unfair conduct, since the loss to each of the individuals affected is too small to warrant it*.".

[163]Hershey Chocolate Corporation v. Federal Trade Commission, 121 F.2d 968 (C.C.A. 3d Cir. 1941); American Airlines v. North American Airlines, 351 U.S. 79 (1956); Louis Altman and Malla Pollack, Callmann on Unfair Comp., Tr. & Mono. § 25:6 (4th ed. 2012.)

[164] Federal Trade Commission v. Raladam Co., 283 U.S. 643 (1931),F.T.C. v. Klesner, 280 U.S. 19 (1929).

[165]43 Harv. L. Rev. 285 (1929); Louis Altman and Malla Pollack, Callmann on Unfair Comp., Tr. & Mono. § 25:6 (4th ed. 2012)

[166] Louis Altman and Malla Pollack, Callmann on Unfair Comp., Tr. & Mono. § 25:6 (4th ed- 2012); F.T.C. v. Klesner, 280 U.S. 19 (1929); Thompson Medical Co., Inc. v. F.T.C., 791 F.2d 189 (C.A.D.C.,1986).

[167] In F.T.C. v. Universal-Rundle Corp., 387 U.S. 244 (1967) entschied der Supreme Court dass die FTC auch nur gegen einzelne Unternehmer vorgehen darf, auch wenn mehrere Unternehmen die gleiche Handelspraktiken verwendeten.

[168] Siehe 16 CFR § 3.14; als ein subjektives Recht jedoch gesehen von PepsiCo., Inc. v. F. T. C. 472 F.2d 179 (C.A.2, 1972).

auch, was ihm erlaubt ist. Nach Ende der Einspruchsfrist bzw. wenn keine Einwendung gegen die order innerhalb der Einspruchsfrist stattgefunden hat, kann die FTC den Bericht und die *cease-and-desist-order* jederzeit – ganz oder teilweise- zurücknehmen, ändern und oder das Verfahren wieder aufnehmen.[169] Bei gerichtlicher Überprüfung[170] der Maßnahmen, angeregt durch den Betroffenen oder bei Vorliegen einer Order und einem *request* zur Änderung der *order,* sind die Möglichkeiten der FTC zum Festhalten an bzw. zum Ändern von ihren Entscheidungen eingeschränkt. Nach Erlass einer *cease and desist order* hat der Betroffene eine Frist von 60 Tagen, um bei Gericht (Court of Appeals) innerhalb jedes von der fraglichen Maßnahme betroffenen Bezirks eine Überprüfung der order zu beantragen. Das einmal angerufene Gericht ist jedoch dann auch für weitere Verfahren zuständig, 15 USC § 45 (d). Die *petition* wird der FTC übersandt, die mit Absendung der Unterlagen an das Gericht keine Befugnisse mehr in dem Verfahren hat. Bis zur Absendung der Verfahrensunterlagen hat die FTC allerdings eine konkurrierende Zuständigkeit mit dem Gericht und kann die *order* bestätigten, ändern oder zurücknehmen. Die Änderung der *order* betrifft auch das Nachschieben von Gründen und Fakten. Durch die Gerichte (Court of Appeals, Supreme Court) kann eine Wiedereröffnung des Verfahrens angeordnet werden.[171] Viele der untersuchten Fälle werden jedoch ohne weitergehende Rechtsdurchsetzung beendet.

(e) Consent Orders

Bei einem Verstoß gegen die eigenen Grundsätze in der *privacy policy* nutzt die FTC oftmals auch *consent orders,* um den Missstand zu beheben und die Sache zu erledigen, nachdem ein *complaint* ergangen ist. Die in dem Verfahren in *reGeocities* verwendete *consent order* dient dabei als Vorlage für alle nach diesem Verfahren ergangenen *consent orders*.[172] Inhalt der *consent orders* ist sowohl das Verlangen nach Einhaltung der *privacy policy* als auch die Implementierung von „*reasonable security measures*“ zum Schutz der gespeicherten Information vor dem Zugriff Dritter.[173] Das Verfahren für die c*onsent order* ist nicht im Title 15 USC geregelt. Die Möglichkeiten für eine *consent order* ergeben sich entweder aus den jeweiligen Statutes oder aus 16 CFR 2.31 unter der *unfair and deceptive acts and practices* Kompetenz der FTC. Eine solche Beendigung des Verfahrens durch ein *consent order agreement* ist nur bei entsprechenden Umständen des Einzelfalles möglich.[174] Die *consent order*, auch *consent decree* genannt, wird dabei nicht als echte Durchsetzung der rechtlichen Standards, sondern als Vertrag zwischen Behörde und Unternehmen verstanden. Die in der *consent order* ausgehandelten Inhalte haben entgegen den *cease-and-desist orders* keine Wirkung für Dritte, so dass für Nichtbeteiligte die Einhaltung der Standards in den *consent orders* kein „*safe harbor*“ darstellt.[175]

---

[169] 15 USC § 45 (b).

[170] Die Standards für die gerichtliche Überprüfung gleichen der für die FTC rules. Hierbei gilt der *substantial evidence standard* für die Tatsachenbasis, wohingegen sich der *arbitrary-or-capricious standard* auf alle anderen Feststellungen der Kommission bezieht, American OptometricAss'n v. F.T.C., 626 F.2d 896 (C.A.D.C.1980).

[171]Siehe 15 USC § 45 (i).

[172] Michael D Scott, *The FTC, the Unfairness Doctrine, and data security breach litigation*: *Has the Commission gone too far?*60 Admin L. Rev. 128, 133. (2008).

[173] Michael D Scott, *The FTC, the Unfairness Doctrine, and data security breach litigation*: *Has the Commission gone too far?*60 Admin L. Rev. 128, 133.(2008).

[174] Siehe 16 CFR 2.31; grundsätzlich ist ein solches Verfahren nicht nach Erlass eines *complaints* möglich, 16 CFR 2.31 (b); als Ausnahme gewährt 16 CFR 3.25 (b) eine solche *consent order* nach Erlass eines Complaints möglich. Von dieser Möglichkeit wird in den Verfahren bei Verstößen gegen *privacy policies* regelmäßig Gebrauch gemacht, nachdem ein *complaint* gegen die Unternehmen erlassen wurde.

[175]May Dept. Stores Co. v. First Hartford Corp., 435 F.Supp. 849 (D.C.Conn.1977).

dd) Sanktionsregime

Die repressive Durchsetzung erfolgt aufgrund zivilrechtlicher Klagen wie auch strafrechtlicher Sanktionen.

(1) **Verstoß gegen *order* und *rule***

Sofern einer *cease-and-desist-order* zuwidergehandelt wird, ist eine *civil penalty* von bis zu $10,000 für jede Verletzungshandlung zu zahlen. Diese *civil penalty* steht den Vereinigten Staaten zu und kann vom Attorney General durch Zivilklage eingeklagt werden. Jede Verletzungshandlung wird als separater Verstoß behandelt, wobei bei einer andauernden Handlung jeder Tag als einzelner Verstoß gewertet wird. Neben der *civil penalty* darf das angerufene Gericht zudem *mandatory injunctions* sowie andere e*quitable reliefs* erlassen, sofern dies zur Durchsetzung der *orders* der FTC erforderlich ist.[176]

Bei einem Verstoß gegen eine *FTC rule* oder gegen eine *cease-and-desist order* kann die FTC zudem auch eine *civil action* gegen die betreffenden Personen betreiben. Das Gericht kann dann „*grant such relief as the courts find necessary to redress injury to consumers or other persons, partnerships, and corporations resulting from the rule violation or the unfair and deceptive act or practice*", 15 USC § 57b (b). Diese vom Gericht zu bestimmende *relief* kann die Auflösung von Verträgen, Rückgabe von Geld oder Rückgabe von *property* umfassen. Das Gericht hat die Einreichung einer solchen Zivilklage hinreichend für die geschädigten Personen bekannt zu machen.[177] Es kann zudem anordnen, den geschädigten Verbrauchern eine Entschädigung zu verschaffen und den Verletzern die unrechtmäßig erwirtschafteten Gewinne absprechen.[178]

(2) Civil Penalty Verfahren

Sofern eine Verletzung der *unfair and deceptive acts and practices clause* nach 15 USC § 45 (a) (1), ein Verstoß gegen andere *statutes*[179] oder eine Verletzung der FTC *regulations* vorliegt, stehen der FTC verschiedene Klagemöglichkeiten zu. Wie auch bei einem Verstoß gegen eine *cease and desist order*, kann der Verstoß gegen eine *rule* der FTC mit einer *civil penalty* bis zu $ 10,000 belegt werden. Die Vorschriften hinsichtlich der Zivilklagen zur Durchsetzung der *penalties* bei Verstoß gegen FTC *rules* oder eine *order* finden sich in 15 USC § 45 (m). Die *civil penalty* ist vor dem district court zu erheben. Im *civil penalty* Verfahren ist dabei die order nicht angreifbar.[180]

Zu beachten ist, dass es sowohl für die Verletzung einer FTC rule als auch einer *cease-and-desist order* hinsichtlich des Verstoßes eines „*actual knowledge or knowledge fairly implied on objective circumstances that such act is unfair or deceptive and is prohibited by such rule"* bedarf, 15 USC § 45 (m) (A) und (B).[181] Eine *civil penalty* ist dabei auch von den Personen einklagbar, die zwar nicht Empfänger der ursprünglichen *cease –and-desist-order* waren, sondern auch alle anderen, die wissentlich eine Handelspraktik verfolgen, welche von der FTC als unfair in einer *cease-and-desist-order* beschrieben wurden, 15 USC § 45 (m) (1) (B) (1).

---

[176] 15 USC § 45 (l).

[177] 15 USC § 57b (c) (2).

[178] So in dem Verfahren FTC v Accusearch, 570 F.3d. 1187 (C.A.10 (Wyo.), 2009.).

[179] Sofern die Durchsetzung durch die FTC angeordnet.

[180] *Defendant cannot attack final cease and desist order of Commission in subsequent enforcement proceeding*, U.S. v. H.M. Prince Textiles, Inc., 262 F.Supp. 383 (S.D.N.Y.1966).

[181] In drawing inferences about knowledge of corporate officers of deceptive practices of corporation, Commission properly draws upon its expertise. Standard Educators, Inc. v. F.T.C., 475 F.2d 401 (C.A.D.C.1973), certiorari denied 414 U.S. 828 (1973).

(3) Strafrechtliche Sanktionen

Wird der FTC bekannt, dass eine bestimmte Verhaltensweise eine föderale Strafrechtsnorm erfüllt, leitet sie das betreffende Material an den Attorney General weiter, 15 USC § 46 (k) (1). Strafrechtliche Befugnisse hat die FTC selbst nicht. Solche föderalen Strafverfahren sind in den Federal Courts durch das U.S. Department of Justice einzubringen. Eine strafrechtliche Verurteilung erfolgt nur bei *proof beyond a reasonable doubt* von einem Richter oder einer Jury.

ee) Spielräume der eigenen Politik

Die FTC hat grundsätzlich einen sehr weiten Spielraum für die Ausübung ihrer Kompetenzen.[182] Dieser Ermessensspielraum umfasst sowohl das Betätigungsfeld als auch die Nutzung bestimmter Handlungsformen.[183] Sie ist damit nur frei, gegen bestimmte Praktiken, Branchen oder Unternehmen vorzugehen.[184] Dieser Spielraum unterliegt dabei nur in sehr eingeschränktem Maße der richterlichen Kontrolle.[185] Es bedarf allein eines substantiellen Nachweises bzw. Begründung durch die FTC.[186] Für einen *complaint* und die Einleitung eines Verfahrens steht der FTC dabei ebenfalls ein weites Ermessen zu. Allerdings muss sich die Handlung der FTC am „*public interest*" messen lassen.[187] Die FTC ist aufgrund ihres grundsätzlich sehr großen Handlungsspielraums auch nicht zur Einleitung bestimmter Verfahren verpflichtet. Den betroffenen Verbrauchern, Verbraucherverbänden oder Mitbewerbern steht allerdings die Möglichkeit der Einreichung eines *request for investigation* offen.[188] Grundsätzliche Untätigkeit bei gravierenden, die Verbraucher im Ganzen betreffenden Missständen, ist jedoch nicht tragbar. Dies lässt sich aus den Entlassungsgründen in 15 USC § 44 entnehmen.

Die FTC kann zwar gegen unfaire und täuschende Handlungen von Unternehmen vorgehen, dies bedeutet jedoch nicht, dass sie Verbraucherrecht autonom setzen kann, indem sie die

---

[182] *Commission rather than courts has power, expertise and implements to explore and correct unfair trade regulations,* Eagles v. Harris Sales Corp., 368 F.2d 927 (C.A.4 (N.C.) 1966); *The Commission is clothed with wide discretion in determining type of order necessary to bring an end to unfair practices*, Federal Trade Commission v. National Lead Co., 352 U.S. 419 (1957); *Commission has broad authority to conduct investigations concerning conduct and practices of corporations in order to enforce mandates of this chapter,* Beltone Electronics Corp. v. F.T.C., 402 F.Supp. 590 (N.D.Ill.1975).

[183] *Where an illegal trade practice has been proved and found, the Commission is empowered to determine the appropriate remedy*. Independent Directory Corp. v. Federal Trade Com'n, 188 F.2d 468 (C.A.2 1951); *The Commission has wide discretion in determining the type of order that is necessary to cope with unfair practices found, and Congress has placed the primary responsibility for fashioning orders upon the Commission.* F.T.C. v. Colgate-Palmolive Co., 380 U.S. 374 (1965); Doherty, Clifford, Steers &Shenfield, Inc. v. F.T.C., 392 F.2d 921 (C.A.6, 1968).

[184] F.T.C. v. Universal-Rundle Corp., 387 U.S. 244 (U.S.Ill.1967); Johnson Products Co. v. F.T.C., 549 F.2d 35 (C.A.7 1977).

[185] *Court will not interfere with remedy imposed by the Commission in false advertising case except where the remedy selected has no reasonable relation to the unlawful practices found to exist.* Porter &Dietsch, Inc. v. F.T.C., 605 F.2d 294 (C.A.7 1979), certiorari denied 445 U.S. 950 (1980).

[186] *"Substantial evidence" with which findings of Commission must be supported, is evidence that affords a substantial basis from which fact in issue can be reasonably inferred and is more than a scintilla and must do more than create a suspicion of existence of fact to be established*. J.B. Lippincott Co. v. Federal Trade Commission, 137 F.2d 490 (C.C.A.3, 1943); ebenso Carlay Co. v. Federal Trade Commission, 153 F.2d 493 (C.C.A.7, 1946).

[187] Siehe oben (c).

[188] Reorganization Plan Np. 4 of 1961 s. 1 (b) (Eff. July 9, 1961, 26 F.R. 6191, 75 Stat. 837); so z.B. in Complaint and Injunction, Request for Request for Investigation and for Other Relief, Google, Inc., F.T.C. No. 1023136 (Mar. 17, 2009), abrufbar unter http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf (zuletzt abgerufen am 30.10.2013).

Standards von *unfairness und deception* nach eigenem Gutdünken festlegt.[189] Die Ausübung des Ermessens, was eine *unfair method* ist, unterliegt der *judicial review*.[190]
Die einzelnen Unterstrukturen der Behörde sind nicht im gleichen Maße frei von Bindungen. Sofern mindestens die Mehrheit der Kommissionsmitglieder minus eine Stimme für die Überprüfung einer bestimmten Sachfrage bzw. Verfahren stimmt, sind die betreffenden Unterabteilungen daran gebunden, siehe Reorganization Plan No. 4 of 1961, s 1 (b).
Die FTC kann unter den bereits genannten Voraussetzungen das Verfahren nach Erlass des Reports als auch der *cease and desist order* beenden. Sofern bereits die Verfahren der *civil penalty* erreicht sind, kann die FTC ebenfalls durch Kompromiss oder Vergleich mit Zustimmung des Gerichts die Sache beilegen.[191]

ff) Einbindung von Verbrauchergruppen

Die Einbeziehung von Verbrauchergruppen geschieht im *rulemaking process* als eine der interessierten Gruppen, bzw. Personen. Ein einklagbares Beteiligungsrecht ist nicht ersichtlich. Die Beteiligung der Verbrauchergruppen dient allein dem Erfahrungsgewinn. Die Einbindung ist kein automatisches Recht auf tatsächliche Ausübung in vollem Umfang, wenn auch auf andere Weise die betreffenden Informationen von der Kommission zu Kenntnis genommen werden.[192] Nach Erlass der Regelungen können die Verbrauchergruppen eine richterliche Überprüfung anstreben[193]; die Gründe für die Aufhebung wegen Nichtbeachtung der Einbindung ist jedoch gerade eingeschränkt. Eine *petition* für ein Tätigwerden ist für die Verbrauchergruppen allerdings möglich.

gg) Besonderheiten bei grenzüberschreitender Durchsetzung?

Die Regelungskompetenz der FTC beschränkt sich auf den innerstaatlichen Handel (sowie Import), es sei denn, dass auch grenzüberschreitende Handelspraktiken Auswirkungen auf den innerstaatlichen Handel haben.[194] Die FTC nimmt für die USA Aufgaben im Global Privacy Enforcement Network wahr und auch hinsichtlich der Arbeiten der OECD und APEC[195]. Zwar sieht die FTC die Notwendigkeit grenzüberschreitender Durchsetzung, verweist aber auch auf die unterschiedlichen Schutzstandards.[196] Grenzüberschreitende Aktivitäten im Bereich der *privacy* Belange sind für die Verfasserin jedoch kaum ersichtlich. In einigen Entscheidungen ist die FTC zwar gegen ausländische Unternehmen vorgegangen, diese betrafen jedoch nur

---

[189] National Petroleum Refiners Ass'n v FTC, 482 F 2d 672, 693 (C.A.D.C., 1973):

[190] Missbrauch der *agency discretion* in FTC v Sperry & Hutcheson Co. 405 US 233 (1972); FTC v RF Keppel &Brp. Inc 291 US 304, 314 (1934). Ein maßgeblicher Maßstab findet sich in 15 USC § 45 (n), welcher für eine Unfairness eine erhebliche Verbraucherschädigung ohne Ausgleich durch andere Vorteile vorliegen..

[191] 15 USC § 45 (m).

[192] Harry and Bryant Co. v. F.T.C., 726 F.2d 993 (C.A.4 1984), certiorari denied 469 U.S. 820 (1984).

[193] 15 USC § 57 (e) (1).

[194] 15 USC § 45 (a) (3): (3) This subsection shall not apply to unfair methods of competition involving commerce with foreign nations (other than import commerce) unless—
(A) such methods of competition have a direct, substantial, and reasonably foreseeable effect—
(i) on commerce which is not commerce with foreign nations, or on import commerce with foreign nations; or
(ii) on export commerce with foreign nations, of a person engaged in such commerce in the United States; and
(B) such effect gives rise to a claim under the provisions of this subsection, other than this paragraph.
If this subsection applies to such methods of competition only because of the operation of subparagraph (A)(ii), this subsection shall apply to such conduct only for injury to export business in the United States.

[195] Hier ist das APEC Cooperation Arrangement for Cross-Border Privacy Enforcement zu nennen.

[196] http://www.ftc.gov/os/2011/01/111301dataprotectframework.pdf (zuletzt abgerufen am 30.10.2013).

am Rande *privacy* Belange.[197] Sofern die FTC durch Zivilklage *restitution* für die Geschädigten einklagt, ist diese nicht auf US-Bürger beschränkt.[198]
Sofern Verletzungen von ausländischem *anti trust law* in den USA betroffen ist, hat die FTC nach dem International Antitrust Enforcement Assistance Act of 1994 die Befugnis, Untersuchungen wegen Verletzung dieser ausländischen Regelungen durchzuführen.[199] Bittet eine ausländische Behörde die FTC bei der Aufklärung von möglichen Verstößen gegen Regelungen, welche *fraudulent or deceptive commercial practices* verbieten oder den sonstigen Regelungen, welche die FTC durchsetzt, entsprechen, um Hilfe, kann die FTC ebenfalls Untersuchungen durchführen, 15 USC § 46 (j).

b. Staatenebene

Auf Staatenebene findet die Durchsetzung des Verbraucherdatenschutzes wie auch der Verbraucherschutz als solcher zumeist neben der Gewährung von *private rights of actions* auch durch die Verbraucherschutzbehörden bzw. Attorneys General statt. Sind die State Attorneys General die zuständigen Verbraucherbehörden, ist dies ein gewähltes Amt. Die Durchsetzung und die Interessen des staatlichen Verbraucherschutzes sind damit je nach politischen Strömungen unterschiedlich. Teilweise ist eine „Verbraucherschutzbehörde" dem Attorney General zu- bzw. untergeordnet. In anderen Fällen ist die Verbraucherschutzbehörde eine eigenständige Behörde. Datenschutzbehörden als solche sind nicht ersichtlich. Dem sektoralen Ansatz folgend, kommen auch andere Behörden, welche für den Bankensektor oder Gesundheitsleistungen zuständig sind, als zuständige Behörden für die Durchsetzung der sektoralen Bestimmungen in Betracht.
Sofern die einzelnen Staaten datenschutzrechtliche Regelungen eingeführt haben, kommt eine Durchsetzung durch Zuweisung bestimmter Behörden oder aber durch die staatlichen Verbraucherschutzbehörden als Verstoß gegen eine Marktverhaltensregel als „*unfair and deceptive trade practice*"[200] in Betracht.[201] Einige staatliche Regelungen sehen von einer verwaltungsrechtlichen Durchsetzung jedoch ab.[202]
Die State Attorneys General oder Verbraucherschutzbehörden haben unterschiedliche Aufgaben und Funktionen. Neben der Durchsetzung – bei State Attorneys General auch die strafrechtliche Durchsetzung- kommen beratende Funktionen, Bürgerinformationen, Lizenzierungen usw. in Betracht.[203] Auf der Durchsetzungsebene stehen den zuständigen Behörden für den Schutz der *privacy* die dem föderalen Recht ähnlichen Instrumente zur Verfügung, um an

---

[197] Vielmehr sind dann spezielle Regelungen wie zum Beispiel der CAN SPAM Act betroffen gewesen, siehe FTC v Olsen and Leroy, Civil Action No. C05-1979 (JCC), FTC Nr. 052 3180; ebenso Verbraucherdaten und ander Regelungen betreffend FTC v Interbill United States District Court for the District of Nevada), CV-S-06, FTC File No. 042-3192 sowie FTC v Practical Marketing , United States District Court for the Southern District of Illinois) Civil Action No.: 3:07-cv-00685-JPG-DGW, FTC File No. 062-3053.

[198] 15 USC § 45 (a) (4) (B): All remedies available to the Commission with resprect to unfair and deceptive acts or practices shall be available for acts and practices described in this paragraph, including restitution to domestic or foreign victims.

[199] 15 USC § 45 (i); welche Regelungen betroffen sind regelt 15 USC § 6211.

[200] Die Bezeichnung „*unfair*" oder „*decepive*" findet sich zwar nicht in jedem „little FTC Act", dennoch lassen sich Gemeinsamkeiten erkennen.

[201] So zum Beispiel die Durchsetzung des CalOPPA durch den kalifornischen State Attorney General.

[202] So gibt der CaCivil Code § 1798.84 ein *privat right of action*, sieht aber keine direkte Durchsetzung durch staatliche Behörden vor.

[203]So zum Beispiel das kalifornische Department of Consumer Affairs, welches für die Lizensierung von bestimmten Berufszweigen zuständig ist, Cal. Bus. & Prof. Code s. 145.

Informationen zu gelangen, *regulations* zu erlassen,[204] einzelne Verstöße zu sanktionieren ,zivilrechtlich *civil penalties* einzuklagen oder Klage im Namen der betroffenen Verbraucher zu erheben.

4. Fehlende behördliche Eingriffe im Urheberrecht

Im Bereich des US-amerikanischen Urheberrechts fehlt es an administrativen Durchsetzungsbefugnissen. Die Durchsetzung des Urheberrechts erfolgt durch zivilrechtliche Klagen der Rechteinhaber oder mittels strafrechtlicher Normen. Eine verbraucherschützende Wirkung des Urheberrechts als solches ist, vor allem unter der engen Begrenzung der *fair use defense* und der hohen Schadenssumme nicht gegeben.

a. Zivilrechtliche Durchsetzung des Urheberrechts

Dem Inhaber des Copyrights stehen die in Titel 17 §§ 106f aufgeführten Rechte zu. Das Herunterladen oder Hochladen von Filmen, Musikstücken und anderen Werken, welche dem Schutz des Copyright Acts of 1976 unterliegen, stellt eine unberechtigte *reproduction* des Werks dar.[205]Die Nutzung digitaler Tauschbörsen im Internet führt damit beispielsweise zur Verletzung der Rechte des Copyright Inhabers durch den Verbraucher. Bei Verletzung der Bestimmungen des Urheberrechts kann der Inhaber des Copyrights den Erlass einer *injunction* verlangen wie auch eine Schadenersatzklage wegen tatsächlichen Verlusten (*actualdamages*) oder aber wegen *statutory damages* erheben.[206] Neben der Möglichkeit zivilrechtlicher Verfahren sieht der Copyright Actof 1976 auch *criminal offenses* vor. Eine Durchsetzung des Urheberrechts durch staatliche Behörden sieht der Copyright Act hingegen nicht vor.
Zwar liegt auch eine Haftung der Betreiber von solchen Plattformen[207] oder Hersteller und Verkäufer von Software zu Ermöglichung von Peer-to-Peer Kommunikationen vor[208]; sofern diese jedoch von außerhalb der Landesgrenzen betrieben werden, ist die Ermittlung der Schädiger schwierig. Eine Haftung der Provider liegt oftmals auch nicht vor: Mit dem Digital Millenium Copyright Act (DMCA) wurden 1998 *safe harbor* Bestimmungen für *online content provider* hinsichtlich der urheberrechtlich verletzenden Inhalte eingeführt, welche das System des Providers durchlaufen. Eine solche Haftungseinschränkung[209] wird gewährt, wenn unter anderem keine Auswahl der Nutzer durch den Provider erfolgt und fehlende Kenntnis des Service Providers von den Urheberrechtsverletzungen vorliegt. Zur Ermittlung der Identitäten der Verbraucher können die Rechteinhaber jedoch den Erlass von *subpoenas* gegen die Service Provider zur Ermittlung der Identität der die Urheberrechtsverletzung begangenen Person beantragen.[210] Sofern die Identität des Verbrauchers vorliegt, wird gegen ihn Klage erhoben. Vor Er-

---

[204] So der Calivornia Government Code §§ 1340 et seq, welcher die Vorgaben für das *rulemaking* Verfahren aufstellt. Darunter ist auch die Beteiligung der Verbrauchergruppen.

[205]Capitol Records, Inc. v. Thomas-Rasset 799 F.Supp.2d 999 (D.Minn.,2011).

[206] Titel 17 USC §§ 501 -505; neben den *damages* kann der Geschädigte auch die Kosten des Verfahrens und Anwaltskosten ersetzt bekommen.

[207]A&M Records, Inc. v. Napster Inc., 239 F.3d 1004 (9th Cir. 2001).

[208]Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd, 545 U.S. 913 (2005).

[209] 17 USC § 512.

[210] 17 USC § 512 (j).

hebung der Klage erfolgt oftmals die Versendung eines *cease-and-desist-letters* mit der Unterbreitung eines Vergleichs.[211] Die bei der Verletzung des Copyright Acts of 1976 zu gewährenden *statutory damages* liegen zwischen $ 750 und $150,000 pro verletztem Werk, wobei das obere Ende der Spanne für *wilfull infringement* angewendet werden soll.[212]
Die Haftung ist in bestimmten Fällen, wie dem *fair use* jedoch eingeschränkt.[213] Vor dem Hintergrund hoher *statutory damages* oder strafrechtlicher Sanktionen[214] ist die *defense* des *fair use* bei Verbraucherbeteiligung für Verbraucher entscheidend. Die Anwendbarkeit dieser Haftungseinschränkung ist jedoch gering.[215] Bei Verletzungen des Urheberrechts von Verbrauchern wurde diese defense bislang nicht von den Gerichten als regelmäßig anzuwendende *defense* erwogen.[216] Die Anwendung der *fair use doctrin* erfolgt gerade nur im Einzelfall.[217] Sofern der ursprüngliche Zweck des urheberrechtlich geschützten Werks nicht gehindert und das Werk auf einer Website von einem Verbraucher nur für nicht kommerzielle Zwecke verwendet wird, kommt die *fair use doctrin* jedoch auch ohne Änderung des Werks in Betracht.[218]

b. Strafrechtliche Durchsetzung des Copyright Law

Eine „verwaltungsrechtliche" Durchsetzung des Urheberrechts findet in den USA, soweit ersichtlich, nicht statt. Eine Durchsetzung des Urheberrechts erfolgt neben der Zivilklage der Rechteinhaber durch das strafrechtliche Sanktionssystem.[219] 17 USC § 506 erfasst vier Fälle der Strafbarkeit: *willful infringement for profit, fraudulent use of a copyright notice, fraudulent removal of notice* sowie *false representation in connection with a copyright application*.[220]Hierbei ist der „*fair use*" ebenfalls wie bei der Zivilklage eine *defense*, welche aber nur in den oben genannten Einschränkungen anwendbar ist. Eine anderweitige Einschränkung der *criminal sanctions* findet, soweit ersichtlich, nicht statt.

---

[211] Dirk Lasater, Comment: *"Closing Pandora's Box": Speculative Invoicing and Opportunism in File Sharing*, 12 Wake Forest J. Bus. &Intell. Prop. L. 25, 28 welcher zudem darauf verweist, dass die erheblichen Prozesskosten und hohen Schadenssummen zu einer hohen Vergleichsquote führen würde.

[212] 17 USC § 504(c)

[213] 17 USC § 107 für den *fair use*; andere Einschränkungen ergeben sich z.B. aus §§ 108ff.

[214] Siehe unten b.

[215] Eine Anwendung der *fair use* Doktrin hinsichtlich des Rechts auf Änderung und Benutzung kommt lediglich bei erheblicher Änderung des Ursprungswerks in Betracht, siehe Daniel Gervais, *The Tangled Web of UGC: Makimng-Copyrigt user-generated Content* 11 Vand. J. Ent. & Tech. L. 841m 869 (2009); Kritisch zu Filesharing, hohen Strafen und Informationen im Netz David Fagundes, *Property Rhetoric and the Public Domain* 94 Minn. L. Rev. 652 (2010).

[216] In den bislang ergangenen und vielfach diskutierten Filesharing Fällen wurde die Fair Use doctrin abgelehnt, A & M Records, Inc., 239 F.3d 1004, 1011; im vielfach diskutierten Verfahren Capitol Records, Inc. v. Thomas-Rasset 692 F.3d 899 (C.A.8 (Minn.),2012), in dem eine Privatperson Musikstücke mittels filesharing herunter- und hochgeladen hatte, wurde *fair use* nicht erwogen.

[217]17 USC § 107.

[218]Righthaven, LLC v. Hoehn, 792 F. Supp. 2d 1138 (D. Nev. 2011), vacating in part Righthaven, LLC v Hoehn, 716 F.3d 1166 (C.A.9 (Nev.), 2013). Das Gericht setzte das summary jugdement hinsichtlich des fair use aus, ohne auf die Begründung des unterinstanzlichen Gerichts Bezug zu nehmen.

[219] 17 USC § 506 (a); die Bestimmungen werden ergänzt durch 18 USC § 2319, welcher für die *wilful infringement* und *for purposes of commercial advantage* von Urheberrechten in Bezug auf Ton- und Filmaufzeichnungen Höchstsätze für Geldstrafen (250,000 $ bei erstmaliger Begehung) festsetzt. Im Ergebnis haben die Gerichte damit jedoch ein weites Ermessen, so auch 4 West'sFed. Admin.Prac. § 4009.

[220]4 West's Fed.Admin.Prac. § 4009 (West's Federal Administrative Practice; Database updated July 2013; Part 7. Business Regulations; Chapter 43. Copyrights; Prepared by Michael Landau, Professor of Law and Director, Intellectual Property, Technology, and Media Law Program, Georgia State University College of Law, Atlanta, Georgia.).

c. Fehlender spezifischer Verbraucherschutz im Copyright Law

Eine echte verbraucherschützende Wirkung hat der Copyright Act faktisch und praktisch nicht.[221] Nur ansatzweise finden sich verbrauscherschützende Ausnahmen, wie beispielsweise die Erlaubnis zum Umgehung von *access controls* im Internet zur Ausübung der elterlichen Sorge sowie zum Schutz der *privacy*.[222] Auch der DMCA steht in der Kritik. Der DMCA erweiterte die Rechte von Copyrightinhabern dahingehend, dass unter anderem auch bei Umgehung technischer Zugangskontrollen zum geschützten Werk eine Zivilklage wegen dieses Verhaltens erhoben werden kann.[223] Verbraucherrelevante Probleme werden in der US-amerikanischen Literatur zum Urheberrecht in den Verbraucher zu stark einschränkenden technischen[224] oder vertragsrechtlichen Lösungen[225], der starken Einschränkung des Erlaubnistatbestandes von *fair use*[226]sowie den hohen Schadensersatzsummen gesehen.[227] Die hohen Schadensersatzsummen und hohen Prozesskosten schrecken viele Verbraucher vor einem Prozess ab, so dass oftmals einem Vergleich nach oder bereits vor Klageerhebung zugestimmt wird.[228] Der Schutz vor zu großer Inanspruchnahme sowie (anderen) Problemstellungen resultierend aus dem DMCA sollten mit dem *Digital Media Consumers Rights Act* gelöst werden. Der Gesetzesvorschlag wurde erfolglos 2003 in das Repräsentantenhaus[229] sowie 2005 in den Senat eingebracht.[230] Einige Bestimmungen wurden im FAIR USE Act 2007[231] übernommen, ebenfalls mit dem Ziel der Wiederherstellung eines gerechten Ausgleichs zwischen Urheberschutz und Nutzungsrechten der Verbraucher, welche digitale Medien erworben haben und diese ohne Verletzungen des Copyrights nutzen möchten. Der FAIR USE Act 2007 wurde jedoch ebenfalls nicht verabschiedet.

---

[221]Anders Robert P. Merges, Peter S. Menell& Mark A. Lemley, Intellectual Property in the new technological age 385 (4thed. 2007) welche im Copyright Act zum Beispiel mit den Regelungen zur Auflagenstärke eine „pro consumer“ Idee verankert sehen.

[222]Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be revised*, 14 Berkely Tech. L. J. 519, 542 (1999); Nicola Lucchi, Digital Media and Intellectual Property. Management of Rights and Consumer Protection in a Comparative Analysis 108 (2006).

[223] 17 USC § 1203; die Bestimmungen zur Circumvention of Technological Measures finden sich in 12 USC § 1201; der DMCA hat hinsichtlich dieses Verhaltens auch Strafvorschriften eingeführt, siehe 17 USC § 1204.

[224]Zu den Beschränkungendurch den DMCA siehe Thomas A. Mitchell, *Copyright, Congress, and Constititionality: How the Digital Millenium Act goes to far* 79 Notre Dame L. Rev. 2115, 2172 (2004).

[225]Nicola Lucchi, Digital Media and Intellectual Property. Management of Rights and Consumer Protection in a Comparative Analysis 108 (2006)

[226]Zu der starken Einschränkung des Erlaubnistatbestan des *fair use* durch den DMCA Jeff Sharp, *Coming soon to pay-for-view: How the Digital Millenium Copyright Act enables digital content owners to circumvent educational fair use,* 40 Am.Bus.L.J. 1, 3 (2002); Steve P. Calandrillo and Ewa M. Davison ,*The dangers of the Digital Millennium Copyright Act: Much ado about nothing?,* 50 Wm. & Mary L. Rev. 349, 414 (2008).

[227] So zum Beispiel Kate Cross, *David v Goliath: How the record industry is winning substantial judgements against individuals for illegally downloading music* 42 Tex. Tech L. Rev. 1031, 1067 (2010); Jeffrey Stavroff, *Damages in Dissonance: The “Shocking” Penalty for Illegal Music File-Sharing* 39 Cap. U.L. Rev. 659, 721 (2011).

[228] Dirk Lasater, Comment: “Closing Pandora’s Box”: Speculative Invoicing and Opportunism in File Sharing 12 Wake Forest J. Bus. &Intell. Prop. L. 25, 28.

[229]108th Congress H. R. 107.

[230]109th Congress H.R, 1201.

[231] 110th Congress H.R. 1201.