EU study on the

Legal analysis of a
Single Market for the Information Society

New rules for a new age?

12. Dispute resolution
13. Self regulation

November 2009
# Table of contents

## Chapter 12 Dispute resolution in the online context

1. Introduction .................................................................................................................. 3
2. Dispute resolution challenges in the online environment ............................................ 4
3. Application of traditional legal instruments of international private law .................... 4
   3.1. Do the traditional instruments still apply? ............................................................... 4
   3.2. The problem of localisation .................................................................................. 5
4. Alternatives to the traditional approach ...................................................................... 7
   4.1. Alternative Dispute Resolution ............................................................................. 7
   4.2. Online Dispute Resolution .................................................................................. 11
   4.3. Small claims procedure ....................................................................................... 17
   4.4. Credit card charge backs .................................................................................... 18
5. Conclusions .................................................................................................................. 19
6. Recommendations ....................................................................................................... 20
   6.1. Short term ............................................................................................................. 20
   6.2. Mid-term .............................................................................................................. 21

## Chapter 13 Self regulation

1. Introduction .................................................................................................................. 26
2. Self-regulation in the information society ................................................................... 26
3. Approaches to self-regulation .................................................................................... 27
4. Types of self-regulation ............................................................................................. 28
   4.1. Codes of conduct .................................................................................................. 28
   4.2. Trustmarks .......................................................................................................... 28
   4.3. Technical standards ............................................................................................ 30
   4.4. Labelling systems, user rating systems and reputation techniques ....................... 30
5. Importance of self-regulation ...................................................................................... 31
6. Advantages and limitations of self-regulation ............................................................ 33
   6.1. Advantages of self-regulation .............................................................................. 33
   6.2. Primary disadvantages and limitations of self-regulation .................................... 34
   6.3. Secondary disadvantages and limitations of self-regulation ................................ 35
7. Some examples of self-regulation ............................................................................... 36
   7.1. Internet content ................................................................................................... 36
   7.2. Technical standards ............................................................................................ 37
8. Second-level self-regulation on online platforms ........................................................ 38
   8.1. Social communities ............................................................................................ 38
   8.2. Wikipedia ............................................................................................................ 39
   8.3. Virtual worlds ..................................................................................................... 40
   8.4. Conclusion .......................................................................................................... 42
9. General evaluation of self-regulatory initiatives ......................................................... 43
   9.1. Success criteria ................................................................................................... 43
   9.2. Requirements for all self-regulation initiatives .................................................... 43
10. Conclusions ............................................................................................................... 44
11. Recommendations ..................................................................................................... 44
   11.1. Supporting self-regulatory initiatives ................................................................. 45
   11.2. Incorporation in technology ............................................................................. 45
   11.3. Increased use of standards ................................................................................. 45
12. Recommended uses for self-regulation .................................................................... 47
This study was commissioned by the European Commission's Information Society and Media Directorate-General, in response to the invitation to tender OJ 2007/S 202 244659 of 19/10/2007. The study does not, however, express the Commission's official views. The views expressed and all recommendations made are those of the authors.
Chapter 12
Dispute resolution in the online context

1. Introduction

On 22 May 2000, the Tribunal de Grande Instance of Paris issued an injunction against American internet service provider Yahoo!, which required Yahoo! Inc. (US entity) to take all possible measures to prevent the access in France of web pages that auction Nazi objects. Furthermore, Yahoo France was ordered to warn all French surfers about the risks involved in viewing the web pages concerned.

The Court found that the auctioning of Nazi objects constituted a "manifestly illegal disturbance" and a contravention of the French Penal Code. Yahoo, on the other hand, argued that the French court was not competent, as the web pages were targeted at an American audience, Yahoo offered its services from the United States, and the measures imposed by the Court undermined its freedom of opinion and expression, guaranteed by the First Amendment of the United States. Yahoo furthermore argued that it was technically challenging to properly distinguish French surfers and other surfers.

Despite the technical objections — confirmed by a panel of experts appointed by the Court — and the various objections against the Court's competence, the injunction was confirmed in November 2000. If Yahoo would not comply with the order, it would be fined 100,000 francs (about 9,150 EUR) for each day of delay.

The decision of the French Court triggered significant reactions: thousands of websites criticized the judgement, and hundreds of newspapers followed suit. According to these reactions, France was destroying "free speech" on the Internet by forcing its rule on anyone who used the Internet anywhere. The case has therefore become the landmark case on the difficulty to apply national laws to a global medium such as the Internet.

Although the decision caused a stir in 2000 (at a time when many legal commentators argued that national states were not competent to regulate the transnational internet), these extra-territorial judicial decisions have become increasingly accepted. Only recently, in a judgement of 2 March 2009, a Belgian penal court sentenced search engine Yahoo! to pay a fine of 55,000 Euro because the company refused to hand over information that would enable the Belgian authorities to identify several fraudsters using Yahoo e-mail accounts. Yahoo's argument that the Court was not competent due to its US establishment was once again rejected, despite its reasonable objection that Belgium and the United States had agreed an international treaty that specified how a prosecutor should seek information from a U.S. company. The Belgian decision quickly sank in oblivion, as these types of decisions seem to have become commonplace.

* * *

The cases above illustrate that dispute resolution procedures on the Internet are intrinsically complex, due to a combination of factors, such as the difficulty to apply traditional rules of jurisdiction to an

---


international medium. Even in more straightforward cases, such as consumer disputes over goods or services bought on the Internet, the dispute resolution procedures lack in effectiveness, despite the emergence of new dispute resolution models and a variety of initiatives that have been undertaken over the years. Not much substantive progress has been made in resolving the fundamental problems, which demonstrates that the problem of online dispute resolution does not lend itself to traditional solutions\(^3\). This chapter therefore aspires to provide guidance in this debate and looks for alternatives.

2. **Dispute resolution challenges in the online environment**

**Greater number of potential conflicts** – The growth of the Internet has intensified international contacts and transactions. Web shops are mushrooming, as starting an online business is relatively easy. Online shopping has now become mainstream. Furthermore, citizens spend a significant amount of time online, often multitasking between participation in international communities or seeking involvement in collaborative creative projects with other citizens from various countries. Many activities on the Internet are also widely distributed among actors. Consequently, a greater number of cross-border disputes can arise, involving small businesses, consumers and other non-professional parties\(^4\).

**Involvement of multiple jurisdictions** – Transactions on the Internet often involve persons from foreign jurisdictions, and typically have immediate cross-border effects or even a global reach (such as publishing a web page). This mix of jurisdictions involved creates legal difficulties, not only with respect to the substantive legal rules that apply to the parties’ relationships, but also with respect to the court that is competent to handle disputes and the possibility to enforce judicial decisions in other jurisdictions.

**Low value of disputes** – Many online transactions have a low value. In case of a dispute, the monetary value of the dispute will often be less than the cost of convening the disputants in the same room, or perhaps even less than the cost of a teleconference\(^5\).

**Anonymity and lack of face-to-face contacts** – Transactions take place all over the world, typically between parties that have never met face-to-face. Furthermore, a party can never be presumed to be who he or she claims to be.

**Automated decision making** – Contrary to face-to-face relations, where humans are involved to take conscious decisions, many decisions and transactions on the Internet are taken and generated, without direct human involvement\(^6\).

3. **Application of traditional legal instruments of international private law**

3.1. **Do the traditional instruments still apply?**

Determining the jurisdiction and applicable law in traditional (offline) court proceedings is handled by private international law, which is a complex field of law. This complexity is exponentially augmented in

---


\(^5\) C. RULE, *Online dispute resolution for business*, 2002, p. 4

the online environment, because the traditional laws regarding the applicable law are focused on elements of the physical world.

The traditional laws of private international law were created by "digital immigrants", and are organised on the assumption that activities can be geographically delimited (whereby each state can regulate what occurs within its territory)\(^7\). The online context, however, has few real connections with the physical world: beyond the telecom infrastructure, the Internet is often said to have no connections with the real world\(^8\). Hence, online activity is not by default located in a single territory — for example, a website can be accessed everywhere. The technical characteristics of the Internet and its ubiquitous nature therefore result in occasional inconclusiveness of the traditional legal instruments\(^9\), which leads to confusing discussions and situations where an activity is subject to multiple and contradictory regulation, or to no regulation at all\(^10\).

Particularly in the early days of the public adoption of the Internet (mid-1990s), many scholars were eager to discard traditional state-based laws\(^11\). They asserted that the traditional, geographical-based rules of law would not be transferable to the transnational internet, that states could not possibly apply their laws to all the online activities, and that this new "cyberspace" was completely beyond their legitimate and actual supervision\(^12\). They therefore concluded that cyberspace should be treated as a distinct and independent place for regulatory purposes\(^13\).

The problem is, however, that the fundamental building blocks and actors of cyberspace have a real-world existence, and are necessarily located in some physical country\(^14\). Consequently, the predictions of these early authors have not proved to be true. On the contrary, states have regulated the Internet, although with varying success. The debate has thus moved from the question of whether States can regulate the Internet, to the question of how it can be done. This has particularly resulted in a tendency towards applying "country-of-origin" and "country-of-destination" rules\(^15\).

3.2. The problem of localisation

The most important legal instrument to determine which court is competent to handle a dispute, is the Brussels I Regulation\(^16\). Related to this is the question which country's laws apply to a certain transaction, for which the most important legal instruments are the Rome I Regulation\(^17\) (for contractual obligations) and the Rome II Regulation\(^18\) (for non-contractual obligations).

---

7 U. KOHL, Jurisdiction and the Internet - regulatory competence of online activity, Cambridge University Press, 2007, p. 4
9 A. PATRIKIOS, o.c., p. 67
10 C. REED, o.c., p. 308
11 For example, in their epic article "Law and Borders - The Rise of Law in Cyberspace", Johnson and Post argued that "[g]lobal computer-based communications cut across territorial borders . . . undermining the feasibility – and legitimacy – of laws based on geographic boundaries".
12 U. KOHL, o.c., p. ix
13 U. KOHL, o.c., p. 11
14 REED, p. 218
15 U. KOHL, o.c., p. 25
17 Regulation No 593/2008 of 17 June 2008 on the law applicable to contractual obligations
18 Regulation No 864/2007 of 11 July 2007 on the law applicable to non-contractual obligations (Rome II)
All three legal instruments strongly and mainly rely on the localisation of objective elements (such as the residence of a party, the place of business, the place where the contract is performed, where advertisements were received, where a tortuous act took place, etc.) in order to determine the applicable law or the competence of a national state.

**Evaluation** – To a certain extent, the Regulations simplify the issue of determining the jurisdiction and applicable law in the EU. However, the localisation element can be particularly troublesome in an online context, because resources are available from everywhere and the communications infrastructure is deliberately flexible, so that communication can pass an undefined number of servers. The result in many cases is that parties are faced with overlapping and contradictory claims as regards the localisation. The application of the localisation element to the online world can then either produce a reasonable result (when the transaction presents a clear link with the physical world), or a virtually useless result (when the product or service is delivered electronically). Hence, as is often stated, the Regulations do not sufficiently take into account the online context, and are insufficiently clear in their application to Internet disputes.

The following examples illustrate these concerns:

- **Place of delivery** – The place of delivery is one of the factors to determine the jurisdiction for a transaction. Although predictable for typical products in an offline context, the outcome of the "place of delivery" criterion for the electronic delivery of products or services depends on the technology used to deliver the product or service. When the service is provided through e-mail, the place of delivery can either be the location of the server of the mail provider, or the location of the user's personal computer. Conversely, when the service is delivered on an online platform or virtual world, the place of delivery is the location of the server of the service provider. However, using the location of a server (e.g., the web server of the service provider, or the e-mail server of the customer) is problematic, as it may even not be possible to determine the location in cloud computing infrastructures, where data may be distributed across different data centres.

- **Consumers** – With respect to consumers, the Brussels I and Rome I Regulation provide that a consumer can bring litigation against a business either in the consumer's domicile or in the defendant's domicile. Conversely, a business can sue a consumer in the consumer's domicile if the business "pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities." It is unclear, however, what "pursue in" and "direct to" mean in ecommerce transactions. Neither concept is further explained in the Regulation itself, and each can encompass a wide range of activities (Is it, for example, sufficient that a website allows to be accessed from everywhere?).

The European Council and the Commission later clarified that "it is not sufficient for an undertaking to target its activities at the Member State of the consumer's residence, or at a number of Member

---

19 C. REED, o.c., p. 230  
20 C. REED, o.c., p. 217  
21 e.g., an online order for the physical delivery of goods  
22 C. REED, o.c., p. 223  
23 HÖRNLE, o.c., p. 72  
25 Z. TANG, o.c., p. 44
States including that Member State; a contract must also be concluded within the framework of its activities" and that "the mere fact that an Internet site is accessible is not sufficient for Article 15 to be applicable, although a factor will be that this Internet site solicits the conclusion of distance contracts and that a contract has actually been concluded at a distance, by whatever means." However, the required level of advertising or active selling will be clarified by the ECJ.

Pending cases – Taking into account these ambiguities, it should not surprise that the ECJ has been asked to issue a ruling on the interpretation of these instruments. The following cases are currently pending:

- **Case C-278/09**
  does a court have jurisdiction for infringement of personal rights allegedly committed by placing on-line of information and/or photographs on a website published in another Member State by a company domiciled in that second State, (i) on the sole condition that that Internet site can be accessed from the first Member State; or (ii) on the sole condition that there is between the harmful act and the territory of the first Member State a link which is sufficient, substantial or significant? Which criteria should be applied when the second condition would be used (number of hits, nationality of plaintiff, language used on the website, …)?

- **C-144/09**
  Is the fact that a website of the party with whom a consumer has concluded a contract can be consulted on the Internet sufficient to justify a finding that an activity is being "directed", within the terms of Article 15(1)(c) of the Brussels I Regulation?

- **C-585/08**
  Is it sufficient for the Brussels I regulation to assume that activities are "directed" to a certain Member State if a website can be consulted via the Internet?

### 4. Alternatives to the traditional approach

This section 4 describes various procedures and legal instruments that have emerged in recent years to resolve the dispute resolution conundrum on the Internet.

#### 4.1. Alternative Dispute Resolution

Although traditional court proceedings have since long proved their merits, they also have inherent shortcomings. These shortcomings include the cost of the procedure, the often lengthy trial and the complex question of which law applies and which court is competent to handle a case.

These shortcomings become even more pronounced in an online environment, where the issues of the applicable law, the competent court and the low value of the disputed transactions can become prohibitive for parties to effectively pursue their rights. As a result, customers may become discouraged to initiate legal proceedings, even when the service provider would be located in the same country as the consumer. However, the threat of lengthy and costly litigation may also discourage online service.

---

26 Z. TANG, o.c., p. 44
27 Reference for a preliminary ruling from the Tribunal de grande instance, Paris (France) lodged on 16 July 2009 - Olivier Martinez, Robert Martinez v Société MGN Limited
28 Hotel Alpenhof GesmbH v. Oliver Heller
29 Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG
30 Green Paper on alternative dispute resolution in civil and commercial law, COM(2002) 196 final, 19 April 2002, nr. 49
providers, particularly medium and small sized businesses — which take up the bulk of the online service providers\textsuperscript{31}.

Alternative dispute resolution (ADR) is widely regarded as holding great promise for the low-cost and efficient resolution of consumer disputes, especially cross-border disputes.

*Note: unless mentioned otherwise, the following paragraphs deal with ADR as a mechanism to deal with disputes ensuing from business-to-business, business-to-consumer and consumer-to-consumer transactions.*

4.1.1. Introduction to alternative dispute resolution

Alternative dispute resolution is a collective expression for all out-of-court dispute resolution mechanisms that interpose a neutral third party\textsuperscript{32}. The word "alternative" points to the fact that it was originally conceived as an alternative to the traditional, state-court system.

Systems for the out-of-court settlement of disputes differ greatly as regards their structure, operation and implementation\textsuperscript{33}. However, two basic forms of ADR can be recognised: *mediation* (where the neutral third party tries to broker a settlement between the parties) and *arbitration* (where the neutral third party makes a binding and enforceable decision as to how the dispute should be resolved). Both types require the parties to agree on the arbitration procedure, although such agreement is often reached before the actual dispute arises\textsuperscript{34}.

- **Mediation** – During mediation, a third neutral party (the mediator) helps the parties in reaching an amicable settlement, by applying information management skills that encourage the parties to more effectively communicate through rephrasing and better articulation of arguments. The distinctive feature of mediation is that the parties voluntarily agree the terms of their settlement. Although mediation, as compared to arbitration or court decisions, can sometimes result in a significantly better outcome for both parties because the mediator will try to dig into the interests of both parties in the dispute, only some disputes really lend themselves neatly to mediation. When the underlying interests of the parties cannot be aligned and the case does not lend itself to a compromise, mediation will be of little help\textsuperscript{35}.

  Mediation is sometimes also said to be contrary to the notion of justice and fairness, because it tries to make each party's interests meet in order to remove the dispute, instead of relying on each party's rights (as a court would do)\textsuperscript{36}. For this reason, it is often said that mediation is not an alternative to arbitration or court decision, but instead a complement to it that should be tried first\textsuperscript{37}. In fact, when no settlement is reached, mediation is often followed by (expedited) arbitration or expert determination. Mediation is therefore an important method to filter out certain disputes.

\textsuperscript{31} Z. TANG, o.c., p. 45
\textsuperscript{32} G. KAUFMANN-KOHLER and T. SCHULTZ, Online Dispute Resolution: Challenges for Contemporary Justice, Kluwer Law International, 2004, p. 6
\textsuperscript{34} For example, in cases of domain name disputes
\textsuperscript{35} HÖRNLE, o.c., p. 55
Arbitration – Unlike mediation, arbitration is mandatory: once the parties have submitted to arbitration, they cannot withdraw from the process. Furthermore, mediation is coercive: the arbitration decision ("award") can be directly enforced, similar to a judgment, even cross-border due to the widespread ratification of the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards. An arbitration decision is also final: once it has been rendered, a court or other arbitrator can no longer handle the same issue (unless the decision would be successfully challenged). For these reasons, only arbitration is a real "alternative" to litigation.

As will be seen below (section 4.2), even more interesting new ways to deal with online disputes can be created when ADR is combined with typical online technologies, in what is typically referred to as "online dispute resolution" (ODR).

4.1.2. Importance of ADR

Growth – There has been an important growth of ADR in all economic areas. Even before the widespread public adoption of the Internet, it was predicted that the use of ADR would grow considerably in the years to come.

Recommended by the European Commission – ADR was recognised by the European Commission as one of three approaches to help individual consumers gain access to justice. The Commission published several documents to improve ADR in consumer contracts, such as the Green Paper on alternative dispute resolution in civil and commercial matters, the Recommendation on the principles for out-of-court bodies involved in the consensual resolution of consumer disputes, and the proposal for a Directive on certain aspects of mediation in civil and commercial matters.

The European Commission has also supported ADR-related projects, such as the ECC-NET network. The aim of this network is to create consumer confidence by providing information to consumers on their rights, and by assisting them with cross-border disputes. Each Member State that participates in this network, is required to set up a central contact point, to provide consumers with information and support for making a claim towards a business located in another Member State. The network is co-financed by the European Commission and each of the participating countries.

Recommended by the eCommerce Directive – Article 17 of the eCommerce Directive provides in a general manner that Member States should ensure that their legislation does not hamper the use of out-of-court schemes available under national law, for dispute settlement.

Recommended or required by national courts – Some Member States require parties to try a mediation procedure before they are allowed to engage in the traditional litigation procedures. In Portugal and several German Länder, claimants must first resort to ADR before the actual judicial

38 K. BENYEKHLEF and F. GÉLINAS, p. 11
39 Communication from the Commission on "Enhancing Trust and Confidence in Business-to-Business Electronic Markets", COM(2004) 479 final, 14 July 2004, p. X. The other two approaches are the simplification and improvement of court procedures, and the improvement of communication between consumers and professionals
40 COM(2002) 196 final
41 Commission Recommendation of 4 April 2001
42 Commission Recommendation of 30 March 1998
43 COM(2004) 718 final
44 formerly EEJ-NET
45 OECD, Consumer dispute resolution and redress in the global marketplace, 2006, p. 28
proceedings may begin. In the United Kingdom, the court must encourage the disputants to use ADR to resolve the dispute, although it is not mandatory for the parties themselves to initiate ADR. In Ireland, Germany and Sweden, the court will attempt to achieve a settlement among the parties, even if such is not legally required.

**Used by governments** – A number of member countries have established ADR boards for B2C complaints. For example, in Austria, an arbitration panel was established to resolve disputes relating to energy services; in Denmark, Finland, Norway and Sweden, state-run ADR panels are competent to deal with most commercial consumer disputes; in Greece, there are public ADR panels operating in every prefecture. The Scottish Parliament has also held a historic debate on ADR, and disclosed plans for an ADR Centre in Scotland

### 4.1.3. Advantages of ADR

**Faster resolution** – When properly channelled, ADR mechanisms enable parties to resolve their disagreements in weeks, instead of years through traditional state court proceedings

**Greater expertise** – Although state courts have profound knowledge of their national laws, they often lack expertise in specialised or highly technical fields. In ADR procedures, the parties can often select the person they want to serve as their mediator or arbitrator, which can save the parties the time to “educate” the judge. This is particularly important in complex business transactions or technical areas.

**Confidentiality** – Discussions held in ADR proceedings are confidential, and parties can decide how much control over the process they want to retain. Conversely, state proceedings are often held publicly.

**Costs** – ADR proceedings are often said to be cheaper than traditional state court proceedings, and are heralded as a way to significantly reduce litigation costs. This is especially true for mediation, but also – to a lesser extent – for arbitration. For example, in cross-border disputes, documents often need to be translated into the national law of the state court – in most cases even when the language used is English – which can quickly become costly when large amounts of data are involved. Such translations are not typically needed in ADR proceedings.

### 4.1.4. Limitations of ADR

**Limited use for consumers** – The use of arbitration in consumer contracts is widely restricted in Europe, so that parties would still have to litigate and invoke traditional courts, despite an arbitration clause. For example, the Directive on unfair terms in consumer contracts requires Member States to invalidate any unfair term, “which has not been individually negotiated” and “causes a significant imbalance in the parties' rights and obligations to the detriment of consumer”. Mandatory arbitration agreements are not only explicitly listed as a prohibited unfair term in consumer contracts, they are also

---

46 See [www.casecheck.co.uk/tabid/1421/default.aspx?article=History+is+Made++Mediation](http://www.casecheck.co.uk/tabid/1421/default.aspx?article=History+is+Made++Mediation)
47 C. RULE, o.c., p. 2
48 M.S. MARTIN, “Keep it online: the Hague Convention and the need for online alternative dispute resolution in international business-to-consumer e-commerce”, *Boston University International Law Journal*, 2002:20, 125, p. 155; HÖRNLE, o.c., p. 70
49 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, Article 3(1), and provision (q) of the Annex
contrary to the principles set forth in the Recommendation on Certain Aspects of Mediation. This restriction is retained in the new Proposal for a Directive on Consumer Rights. Although mandatory arbitration agreements are generally prohibited for consumers in the EU, other "soft" forms of arbitration may be permitted, provided they are individually negotiated, and do not affect consumers' right to resort to court. It may also be a solution to make arbitration agreements asymmetrically binding, i.e. binding businesses only, while consumers remain free to initiate judicial proceedings.

**Getting the service provider to agree** – ADR schemes rely on the voluntary participation of parties. Although in specific cases (such as domain name disputes or trustmarks) a party may have committed in advance to ADR, this is most often not the case in general disputes.

**No standards** – There are no binding international principles that define procedural safeguards for the accessibility, independence, transparency, and cost of ADR procedures. Only some principles have been developed by both national states and the private sector. On the EU-level, the European Commission has issued the Directive on mediation as well as two recommendations to guide the implementation of ADR services for consumer disputes.

**Not yet up to its full potential** – A number of surveys suggest that ADR has not yet fulfilled its full potential as a low cost and efficient mechanism for the resolution of business to consumer disputes, either because the cost is still too high for consumers, or because the existence of the procedure is simply not known to disputing parties.

### 4.2. Online Dispute Resolution

Although there is some disagreement about its precise scope (particularly in relation to traditional ADR), online dispute resolution (ODR) can be defined as a type of dispute resolution which is performed online.

50 Commission Recommendation of 30 March 1998, section IV, in which it is stated that "The consumer's recourse to the out-of-court procedure may not be the result of a commitment prior to the materialisation of the dispute, where such commitment has the effect of depriving the consumer of his right to bring an action before the courts for the settlement of the dispute."


52 Z. TANG, o.c., p. 49

53 Ibid.

54 T. SCHULTZ, *Online dispute resolution: an overview and selected issues*, United Nations Economic Commission for Europe Forum on Online Dispute Resolution Geneva, 6-7 June 2002, section 3.2

55 See, in general, OECD, o.c., p. 18

56 For example, The International Chamber of Commerce has issued best practices for online dispute resolution (ODR) in business to consumer and consumer to consumer transactions.


58 Commission Recommendation of 30 March 1998

59 Commission Recommendation of 4 April 2001

60 See S. REILLY, The Need to Develop ADR in Ireland, European Consumer Centre Dublin, 2004, available at www.ecic.ie/resources/publications/ADR_development_in_Ireland.pdf. For example, in a 2004 survey of the UK National Consumer Council, it was found that the provision of ADR services to consumers is "ad hoc and presents a lottery for the consumer...[depending] either on the type of problem faced or where the problem arises, and sometimes depending on the ability of the consumer to afford the fees." A 2004 Eurobarometer survey found that 38% of respondents had never heard of bodies, such as arbitrators, ombudsmen, arbitration or conciliation bodies, that could offer an alternative to court action.

substantially online, and uses the information processing powers of computers with the networked communication facilities of the Internet to facilitate the resolution of disputes between parties. Although ODR is relatively new, it has deep roots, being based on decades of work in the ADR field.

In ODR proceedings, the different stages of the dispute resolution process are performed through electronic communication means (such as online document management systems, multi-functional ODR platforms, settlement and negotiation software, online documents and forms, chatrooms and instant messaging, e-mail, videoconferencing, voice-over-IP software, etc.). These new techniques can augment the traditional means of resolving disputes.

ODR is said to have great potential to resolve disputes in e-consumer contracts, particularly in small disputes where the costs of the resolution must be kept proportionally low. For this reason, ODR is also often recommended by the European Commission. ODR is less appropriate to be used in fields where legal constraints are higher, such as family law and taxation law, because states are more sensitive to interventions in their sovereignty in these fields.

The majority of European countries have not yet developed ODR systems, and tend to maintain the traditional methods of Alternative Dispute Resolution (ADR) only. However, ODR procedures exist in a variety of contexts, from general disputes to specific disputes (e.g., in online auction sites), as part of a trustmark or seal programme, or on an independent basis. Currently, there are more than 100 ODR providers operating.

4.2.1. Types of ODR

"ODR" encompasses a variety of different methods. The most important are set forth below.

Automated negotiation – This type of ODR is carried out on an automated software platform, without the involvement of human operators. It usually involves a "blind bidding" negotiation process designed to
facilitate the settlement of the dispute. During this process, each party submits successive secret offers to the platform, which are not revealed to the other party until both parties’ submissions match certain standards (e.g., are within a certain monetary range of each other). This process encourages each party to define the preferred and bottom-line outcome of the dispute. It has proved to be particularly successful with insurance compensations and commercial activities. Automated negotiation is relatively successful, and is offered by many providers. Examples include Cybersettle and InterSettle.

**Assisted negotiation** – In assisted negotiation, a software platform assists the parties in their internal negotiations (no human arbitrator or mediator intervenes). The ODR service provider offers a variety of instruments to facilitate the negotiation, such as an overview of standard solutions, templates of written agreements, the storage of documents relevant to the dispute and secure sites.

**Online mediation** – Online mediation is the online form of traditional mediation, in which a third neutral person tries to bring the parties to settle by using one of the styles developed for traditional mediation, for instance facilitative or evaluative mediation. The only significant difference with traditional mediation is that the parties communicate online, often using advanced communication platforms that are tailored to specific types of disputes. For example, online forms can be offered that are focused on the particular type.

**Online arbitration** – Similar to traditional arbitration, online arbitration involves a third party who is chosen by the parties, and renders a decision on the case after having heard the relevant arguments and seen the appropriate evidence. The most well-known examples include the UDRP procedure and the .EU domain name dispute resolution process.

### 4.2.2. ODR success stories

Although ODR has not yet seen widespread adoption, there have been specific areas and ODR initiatives that are recognised as success stories.

**Austrian Internet Ombudsman** – The Austrian Internet Ombudsman was founded in 1999, and handles consumer disputes arising from e-commerce through mediation and arbitration. Austrian residents can initiate a complaint procedure against any business established in an EU Member State. The involvement of the Austrian Internet Ombudsman is free of charge for both parties. Although participation is not mandatory for web shops, some companies have agreed in advance to cooperate, as part of the Euro-label Trustmark Code of Conduct. In addition, the Ombudsman publishes the names of companies that are unwilling to participate on its website.

The Austrian Internet Ombudsman can be considered as a nice illustration of the capabilities of ODR. In 2006, it worked on 4,750 complaints, with a total of claims amounting to 609,000 EUR.

**UDRP** – Another successful example of ODR is the WIPO Arbitration and Mediation Centre, which is the dominant ODR provider registered with ICANN under its Uniform Domain Name Dispute Resolution...
Policy (UDRP). Since 1999, it has resolved over 25,000 domain name disputes online, involving parties from 144 countries. The UDRP applies primarily to international domains (such as .com, .net, .org and .info), but is also used for a large number of country code top-level domains.

The ICANN UDRP administrative procedure is mandatory to domain name holders, although results are not binding. Panel decisions are enforced by domain name registrars, unless the respondent has filed an appeal to competent court of jurisdiction within a time period of ten days.

.EU – The alternative dispute resolution (ADR) for .EU domain name disputes is provided by an Arbitration Court established in Prague. The Czech Arbitration Court administers ADR Proceedings according to ADR rules, in line with the .EU public policy rules. The Czech Arbitration Court is the only arbitration board that is authorized to resolve domain name disputes regarding .EU domains, and handles complaints in all official EU languages.

Similar to UDRP, the .EU ADR procedure seems to be a very effective and fast way of resolving disputes. Hundreds of disputes have already been solved using ADR. Since the initiation of the first .EU ADR proceeding in 2006, close to 1,000 proceedings have been brought before the Court, and more than 900 decisions have been issued and published.

SquareTrade – SquareTrade was the official online negotiation and mediation service provider for auction platform eBay. Since 2000, it has handled over two million disputes, across 120 countries in five languages. It discontinued its dispute resolution services in early 2008.

During its operational period, SquareTrade was – from a practical point of view – the only formal dispute resolution option that was available to resolve disputes. For eBay seller-buyer disputes, litigation is generally very unattractive (even where no cross-border situation is involved), because the amount at stake is very low. However, the ODR-service of SquareTrade turned out to be very attractive, since it is integrated into the eBay platform on the basis of a cooperation agreement. The dispute resolution procedure was, literally, only one click away from a party's eBay account. Moreover, it was the only option for the resolution of negative feedback disputes.

SquareTrade provided automated negotiation and human-assisted disputed resolution. In the free of charge negotiation phase, the process was fully automated, with parties being guided by multiple choice suggestions on how their dispute might be solved. As a result, most disputes were resolved in the negotiation phase. Only if parties could not agree, a mediator could be invoked, although this resulted in a small charge. In total, 80% of the cases were resolved either through negotiation or mediation.

ECODIR – ECODIR (www.ecodir.org) consists of a consortium of European and North American Universities, as well as some private partners. It was launched in 2001 and ran as a pilot project until June 2003. During this time, ECODIR handled 62 cross-border cases, from over 14 countries.

ECODIR's dispute resolution process is entirely voluntary, as there are no binding rules that force a party to respond to a claim submitted to ODR. All information relating to the claim, as well as the communication between the disputants and the mediator, take place on a secured private web space.

---

78 See www.wipo.int/amc/en/center/caseload.html
79 EC Regulation 874/2004
80 See J. GRIFFITH, p. 277-279
82 M. BONNICI, G. PIA, Self-regulation in cyberspace, 2007, p. 186
83 G.P. CALLIESS, o.c., p. 653
ECODIR’s popularity has been very limited\textsuperscript{84}, primarily because – unlike SquareTrade – there is no direct link between the platform where the disputes arises (e.g., the web shop) and the dispute resolution platform. Furthermore, the remedies offered by ECODIR do not bind the parties. A party relies completely on the goodwill of the other party to actually stick to the agreement reached.

4.2.3. Advantages

All of the advantages of ADR, as set forth in section 4.1.3 above, also apply to ODR. In addition, the following advantages can also be identified.

Integration with the online platform – As ODR procedures rely heavily on IT tools, they can be more easily integrated with the online platform (as was the case, for example, with SquareTrade). It should be pointed out, however, that examples of direct integration have been fairly limited up to now.

Time savings – The use of the Internet creates greater flexibility for the parties to resolve their dispute. Similar to the permanent opening hours of a web shop, parties can submit their claims and reactions around the clock, not just during court hours or arbitration procedures\textsuperscript{85}. Traditional court proceedings, on the other hand, often invoke long delays, strict requirements for the submission of documents and various other procedural rules that are liable to create delays for the parties.

Convenience of the procedure – The use of asynchronous communications allows the parties to be prepared to carefully produce their response, without being intimidated by the physical appearance of the other parties.

Costs savings – ODR is less costly than traditional ADR or court proceedings, because there are no travel costs. Such savings are particularly important in low-value disputes, where the cost of a plane ticket is often higher than the value of the disputed transaction.

No geographical limitations – As ODR is not bound to a specific geographical location, parties can rely on expertise from neutral experts around the world. Furthermore, parties can find a solution for their problem even if they are far apart from each other.

4.2.4. Issues surrounding ODR

Need of party consent – Few parties participate voluntarily in a dispute resolution procedure. In most cases, they only participate because they are directly or indirectly forced to do so. This causes no issues for the UDRP procedure (where ownership of a domain name is at stake) or for online auctions such as eBay (where a seller or buyer’s reputation is at stake), but can be particularly problematic for other voluntary schemes of dispute resolution, as is – for example – the case with the ECODIR project.

Recognition of decisions – It may be difficult to get ODR awards to be recognised and enforced by courts. For example, the New York Convention requires an \textit{authentic original} (or duly certified copy) of an award, which must be \textit{in writing} and \textit{signed} by the majority of the arbitrators. Although these conditions can be met if electronic documents qualify as writing and electronic signatures are used, such solutions do not correspond to the current wording of the New York Convention, nor to its common interpretation\textsuperscript{86}.

---

\textsuperscript{84} M. BONNICI, o.c., p. 191
\textsuperscript{85} C. RULE, o.c., p. 6
\textsuperscript{86} T. SCHULTZ, o.c., section 3.1
Due process – One of the most important advantages of ODR is its speed, which can be reached by using simplified procedures and less formalism than is the case with traditional state court proceedings. However, these formalities in traditional judicial procedures have been introduced for valid reasons, the most important of which is ascertaining due process. Care must be taken to avoid that ODR procedures do not jeopardise due process in their flexibility\(^87\).

Viable business model? – The viability of the ODR business model seems to be the major problem, as an ODR service only becomes economically sustainable when it handles large quantities of disputes of a similar nature. The problem is that a for-profit ODR provider must find an equilibrium between fees that are high enough to ensure a viable business model, and fees that are low enough to be proportionate to the amounts in dispute\(^88\). This may impact an ODR service provider’s independence and impartiality\(^89\).

Lack of face-to-face contact – Although the asymmetric nature of most ODR procedures constitutes a distinct advantage, the lack of face-to-face contact may also prove an important disadvantage, because body language and facial expressions are important components of communications. While videoconferencing and other online technologies may help to compensate this lack of face-to-face contact, they are no substitute for face-to-face meetings in the current state of the technology.

Loss of public oversight – Online disputes may reveal important information about emerging issues (such as defective products, consumer restrictions on digital services, ...) or societal trends (discriminatory practices, unethical business conduct). While authorities should police these issues, they become difficult to monitor in ODR, as ODR procedures are usually confidential.

Digital divide – The so-called “digital divide” between citizens who are proficient in online techniques and citizens who are not, may also constitute an important hurdle to the widespread use of ODR. The ODR procedure requires all parties in a dispute to be rather comfortable with sophisticated web technology\(^90\), which may favour those who are more acquainted with the use of computers. It would be advisable neither to impose the use of technology nor to discourage it, taking into consideration all types of individuals and their needs\(^91\).

4.2.5. Evaluation

An evaluation of the current state of ODR shows ambivalent characteristics.

On the one hand, ODR has proved to be very successful in specific areas, such as domain name disputes and auction websites. In these areas, ODR-service providers do not only make a very attractive offer for easy accessible, quick, effective, and low-cost dispute resolution, but have also succeeded in integrating their services in the online platform on which the dispute arises\(^92\). They have therefore demonstrated to have reached a stage of maturity in these areas\(^93\).

On the other hand, ODR shows little success outside its preferred specific areas. The general market of ODR services seems quite volatile, with limited success and recognition among potential customers.

\(^87\) Ibid.
\(^88\) M. BONNICI, o.c., p. 207
\(^89\) T. SCHULTZ, o.c., section 3.3
\(^90\) T. SCHULTZ, o.c., section 3.4
\(^91\) P. CORTES, o.c., p. 31
\(^92\) As was, for example, the case with the integration of the SquareTrade procedure in the eBay platform. See G.P. CALLIES, o.c., p. 653
\(^93\) A. PATRIKIOS, o.c., p. 73
This limited success is linked to a variety of factors, the most important being the requirement that parties must consent to the ODR procedure. This is particularly problematic in B2C relationships, where the consumer is the weaker party and the web shop or online service provider does not generally have sufficient incentives to consent to the ODR procedure.

Another important hurdle for the success of general ODR services is the lack of direct integration with the online platform on which the dispute arises. This direct integration increases parties' awareness of the possibility of ODR, and has been key in the successful SquareTrade procedure.

Nevertheless, we are of the opinion that the existing ODR services are representative of the potential of self-regulation in the resolution of online disputes.

4.3. Small claims procedure

Introduction – Small claims procedures have been described as a "middle ground" between formal civil litigation and alternative dispute resolution. Such a procedure already exists in several Member States, and has now also been adopted at the Community level, following a Green Paper launched by the European Commission in December 2002.

The same Green Paper also led to the adoption of a European Order for Payment Procedure for uncontested pecuniary cross-border claims. The procedure sets forth minimum standards, compliance with which renders unnecessary any intermediate proceedings in the Member State of enforcement prior to recognition and enforcement. The procedure is primarily administrative, and less substantial than the full, adversarial small claims procedure, which will be dealt with in detail below. However, it is interesting to note that Germany and Austria have developed an IT application for the electronic processing of the European order for payment procedure. Such efforts could be extended to make the procedure available online everywhere in Europe.

The Regulation establishing a European small claims procedure aims to provide a Community wide uniform procedure for greatly reducing cross-border litigation costs, as an alternative to the domestic claims procedures. The new procedure is optional, as it is offered as an alternative to the possibilities existing under the national laws of the Member States. It will be applicable from 1 January 2009 in all EU Member States except Denmark, but is limited to cross-border cases.

Procedure – The procedure is (in principle) in writing, so that parties do not need to travel. To file a claim, the claimant must fill in a standard claim form giving proper details of the claim, the sum demanded, etc. This form then needs to be submitted to the competent court by any means of communication acceptable to the Member State in which the action is taken. Once the court has received the form, it prepares a standard answer form which, together with the supporting documents, is served on the defendant. The defendant must then reply within thirty days. Any counterclaim submitted

94 OECD, o.c., p. 28
95 E.g., the Online Small Claims in Ireland and the Online Money Claim in England and Wales
96 Regulation 861/2007 of 11 July 2007 establishing a European small claims procedure
97 COM/2002/0746 final
100 See www.epractice.eu/en/cases/europa
101 The Court can, however, ask the parties to physically appear, if the court deems this necessary for the merits of the case.
by the defendant is served on the claimant in the same way as the original claim was served on the defendant. Judgment is given in thirty days, and the procedure provides for the direct enforcement of the court decision, without the need for going through mutual recognition of judgements.

Scope – The Regulation deals with claims under 2,000 EUR in value (excluding interest, but including legal costs), arising in cross-border disputes within the EU. The Regulation covers civil and commercial matters, including not only consumer disputes, but a range of civil claims, such as personal injury compensation, disability discrimination and unequal access to services\textsuperscript{102}.

Use of new technologies – The Regulation allows the use of new technologies for transferring information (e.g., evidence) to the court. However, it will be up to the Member States to decide which means of communication are actually acceptable to them. It can be expected that in due time electronic communications will be possible for every aspect of the judicial procedure to assist in the resolution of online, as well as off-line disputes\textsuperscript{103}.

Evaluation – The objective of the Regulation is to create a cost-efficient procedure. This objective can only be achieved by using electronic tools\textsuperscript{104} and other ODR-like facilities. It is therefore regrettable that the Regulation has missed the opportunity to exhort the extensive use of information technology. Although it is still too early to evaluate the effectiveness of the Regulation, the Regulation nevertheless has the potential to increase the effectiveness of redress mechanisms when appropriately assisted with ICT tools.

4.4. Credit card charge backs

Credit card charge backs are remedies offered by payment card issuers to consumers. The actual protection scheme varies considerably among Member States, and can include anything from the ability to correct billing errors, to liability limits for unauthorised charges, or redress for non-conforming or non-delivered goods and services\textsuperscript{105}. These protections can enhance consumer confidence in the use of payment cards, and can also constitute consumer-friendly dispute resolution mechanisms.

Credit card charge backs can be a very efficient and practical means to deal with disputes small-value transactions: they provide the consumer with significant leverage, and tend to equalise the unequal bargaining power. The threshold towards application is very low, as a consumer does not need to search for a lawyer, mediator or arbitrator, as he only needs to contact the payment card issuer\textsuperscript{106}.

The scope of credit card charge backs is, however, very limited. First, it obviously only applies to purchases made by credit card. Secondly, it only applies to very simple disputes, e.g. when the cardholder denies to have made the recorded purchase.

Even so, this mechanism of easy redress deserves approval. We therefore recommend integration of similar features in other online payment instruments\textsuperscript{107}.

\textsuperscript{102} There are some exceptions, e.g. regarding customs, administrative matters, wills and succession, violation of privacy and rights relating to personality, employment law and social security.
\textsuperscript{103} P. CORTES, o.c., p. 31
\textsuperscript{104} Ibid.
\textsuperscript{105} J. HÖRNLE, o.c., p. 38
\textsuperscript{106} Z. TANG, o.c., p. 49
\textsuperscript{107} See section 6.1.1 below
5. Conclusions

The relative anonymity, lack of face-to-face contacts, as well as digital and cross-border nature of the Internet have increased the number of potential conflicts on the Internet.

While traditional state court proceedings have long established their role in the resolution of offline conflicts, there is substantial evidence that they are not able to meet the requirements of the online environment. Parties that want to resolve their dispute through traditional state court proceedings, will encounter difficulties in determining the applicable law and the competent court, and may also face important issues during the actual cross-border enforcement of the judicial decision. Moreover, state court proceedings are often slow, costly and formal, which does not align with the fast-moving nature of (often low-value) transactions on the Internet.

Alternative dispute resolution (ADR) is widely regarded as an alternative to state court proceedings, which can resolve online and offline disputes in an efficient, confidential and cost-effective manner. However, as is the case with state court proceedings, claimants can still be confronted with difficulties to enforce decisions resulting from ADR in case the other party does not comply voluntarily. Nevertheless, there has been an important growth of ADR in all economic areas, even before the widespread public adoption of the Internet. ADR has also been recommended and accelerated by the European Commission, national authorities as well as international institutions (such as the OECD). It is also recommended by the eCommerce Directive, which provides that Member States should ensure that their legislation does not hamper the use of out-of-court schemes.

While ADR proceedings were available before the public adoption of the Internet, the growth of the Internet has brought important new possibilities to ADR. The synergy between ADR and (online) information technology – online dispute resolution (ODR) – holds great promise as a method of resolving disputes that arise online, and for which traditional means of dispute resolution are unavailable or inefficient. Compared to "traditional" ADR, the inherent online characteristics of ODR provide further advantages, such as time savings, cost savings and a convenient procedure. In addition, ODR procedures integrated in online platforms can use reputation mechanisms (such as user rating systems), which can increase voluntary compliance with decisions. Numerous ODR service providers are available today, offering a variety of different methods to resolve disputes online, from automated negotiation to assisted negotiation, "blind bidding" and online arbitration.

Although ODR has proved to be very successful in specific areas (such as the UDRP and .EU domain name procedures and the SquareTrade settlement for auction provider eBay), it has seen fairly limited popularity outside these specific areas. Nevertheless, the existing ODR services are representative of the potential of self-regulation in the resolution of online disputes. The most important drawback of ODR is that it requires the parties to consent to the ODR procedure, which is particularly problematic in B2C relationship, where the consumer is the weaker party and the web shop or online service provider does not generally have sufficient incentives to consent to the ODR procedure. The most important other issues surrounding ODR include the recognition of ODR decision and concerns about due process.

The European Commission has recognised these concerns, and has recently adopted the European small claims procedure to resolve cross-border disputes. While some aspects of this new procedure (limitation to cross-border cases, low value of 2,000 EUR; data protection disputes are not covered; lack of adequate provisions supporting ADR and ODR) may hamper the adoption of this procedure, it holds great promise to resolve typical cross-border disputes of limited value, for which traditional court

---

108 See Chapter II, Section 4.4 for more information on user rating systems.
proceedings or ADR may be too costly or troublesome for parties to undertake. However, as the European small claims procedure has only taken effect in 2009, it is too early to tell whether this procedure will be adequate.

6. **Recommendations**

In this section 6, we provide a list of recommendations to resolve the various issues identified in this chapter. A distinction is made between recommendations that can be implemented on the short term (2010-2015) and recommendations that can be implemented on the mid-term (2015-2020). These time frames align with the relative political and legal difficulty to implement these recommendations, as well as the urgency involved. Hence, the threshold for implementing recommendations for the short term is relatively low, or the urgency involved is rather high. Conversely, recommendations for the mid-term require important legal modifications, or may receive more political resistance.

6.1. **Short term**

6.1.1. **Building in consumer protection in payment facilities**

Getting a service provider to participate has been pointed out as the Achilles heel of online dispute resolution procedures. We therefore recommend the European Commission to facilitate the creation of new payment methods that integrate dispute resolution and/or consumer protection in the core of their payment flow.

In addition to the credit card charge backs discussed in section 4.4, we refer to the PayPal Buyer Protection Programme for tangible goods as an example of such (limited) integration of dispute resolution procedures. The PayPal Buyer Protection Programme service was created to counter the media and buyer dissatisfaction for faulty items that are sold through eBay. At the informal level, PayPal users are obliged to file a dispute and use a dedicated online platform to obtain a solution together with the seller (in some cases, PayPal mediates between the parties). PayPal also allows formal complaints and provides limited insurance.

6.1.2. **Encouraging the use of financial escrow services**

Financial escrow services are a type of self-enforcement, and can prove an effective means of redress, for both consumers and businesses. With an escrow account, the customer first submits payment to a third party (the escrow company), who verifies the payment and authorises the service provider to provide the service or ship the products ordered. The escrow company then tracks the shipment or delivery of the service, sets a number of days after reception, and pays the service provider unless the customer would file a complaint. The escrow company therefore acts as a secure third party.

As there have been several cases of fraudulent escrow companies, it could be envisaged to submit financial escrow services to a specific regulatory regime and/or encourage the use of trustmarks. In this regard, we refer to our recommendation in the electronic payments chapter of this study.

6.1.3. **Self-regulation of online service providers**

The most optimal type of dispute resolution for a certain online service (wiki, online game, virtual world, discussion forum, auction site, creative platform, etc.), depends on the type of service and the target

---

110 T. SCHULTZ, *o.c.*, section 3.2
audience. Consequently, we think self-regulation constitutes the most interesting option to create flexible online dispute resolution procedures.

For reasons of efficiency and better enforcement, these self-regulated dispute resolution procedures should be directly integrated in the platform itself. As pointed out in section 4.2.5 above, such direct integration has been one of the most important success factors of popular ODR procedures, such as the UDRP, .EU and SquareTrade procedures.

As argued in Chapter II.10 (self-regulation), we recommend to create formal technical standards for these self-regulated dispute resolution procedures. Such technical standards can, for example, specify how technical links can be established between a complaint, the user account of the disputing parties and (where relevant) the mediator or arbitrator.

6.1.4. Self-regulation of ODR service providers

In order to counter the various concerns with respect to ODR service providers (see section 4.2.4 above), it can be envisaged to create voluntary accreditation schemes of ODR service providers, similar to the accreditation scheme introduced by the eSignatures Directive.

These schemes should encourage ODR to respect certain minimum values, such as:

- **Impartiality** – which is the basic guarantee to ensure that all parties have confidence in the fairness of the ODR procedure. The problem, however, is that ODR service providers are often unilaterally selected and paid by one party. This may cause ODR service providers to lean towards favouring businesses.

- **Transparency** – transparency means that relevant and clear information about the procedure should be available to both parties, preferably on a durable medium. This information must allow each party to understand how the procedure is developing, in order to decide how to react. Furthermore, any agreed solution should be recorded.

- **Fairness** – Fairness primarily aims to protect the consumer as the weaker party. It permits the parties to resort to judicial procedures or other dispute resolution systems before, during, or after the ODR procedure.

6.2. Mid-term

6.2.1. Resolving outstanding ADR/ODR legal questions

As noted in section 4.1.4, it is prohibited to impose mandatory arbitration procedures on consumers. In our opinion, the consumer protection Directives should state that imposing ADR / ODR is allowed towards consumers, under the conditions that the ADR/ODR service provider meets certain minimum quality criteria and that consumers retain the right to resort to court following the ADR/ODR. Such a possibility would be especially useful for dealing with small claims, provided that the ADR/ODR services are made cost-effective to consumers, e.g. through collective funding by online service providers.

---

111 See M. BONNICI, o.c., p. 206; J. HÖRNLE, "Online Dispute Resolution - More than the Emperor's new clothes.", Proceedings of the UNECE forum on ODR 2003, 25
112 See also the Commission communication on out-of-court settlements
113 Z. TANG, o.c., p. 48
114 Ibid.
115 Ibid.
recommendation can also be linked to our previous recommendation that self-regulation for ODR service providers should be encouraged.

Another issue that should be resolved to foster the uptake of ADR/ODR, is the compatibility of the New York Convention with ODR awards (as noted in section 4.2.4).

6.2.2. Optimising the rules of private international law

As pointed out in section 3, the application of current legal instruments for private international law raises questions when applied to the online world. In the short to medium term, we think that there is a need either to clarify (e.g. through guidelines by the ECJ) how the rules apply in the online world or to insert specific provisions for the internet.

6.2.3. Introduction of e-courts

This chapter has made clear that it is difficult to find solid solutions to the transnational Internet within the parameters of national law. Even though the European small claims procedure holds great promise for resolving disputes in an efficient manner, it is limited in scope and essentially still relies on national courts. It is therefore frequently said that real solutions to the online dispute resolution conundrum lie outside the national-law framework.\(^{116}\)

In the medium term, we think it is useful to envisage creating EU-level online courts, dedicated to resolving (specific) disputes of civil law that arise in the online world. This court would be specialised in online matters – and its competence would at the same time be limited to online cases – but would in other aspects function like a traditional court, although everything would be handled online, without the necessary physical presence of the parties or their legal representatives. The whole process should be completely digital, and the hearing can be carried out in a more flexible way, e.g. through telephone, audio, video, or e-mail conference.

The idea may seem far-fetched and rather radical at this moment, but is not unrealistic: it has already been proposed in legal literature.\(^{117}\) Also, there are examples that are already operational and resemble an e-court, such as the .EU arbitration panel in Prague (Czech Republic) and the WIPO panels for UDRP procedures, which have proven to be able to efficiently handle cases from very different jurisdictions. In fact, similar to the .EU arbitration panel, we propose that the EU court would also publish its cases (respecting privacy rights of natural persons).

**Difference with state courts** – The proposed e-courts should not be confused with the ongoing efforts in various Member States to modernise traditional courts. Although information technology is not used extensively in the majority of the judicial procedures in the EU,\(^{118}\) several Member States are undertaking efforts to introduce electronic evidence, filings, hearings and testimonies, as well as other electronic documents, or other technologies in courtrooms. In the proposed e-courts, the use of online technologies would be mandatory (instead of optional).

**Advantages** – The e-court would have all the advantages associated with ODR proceedings, such as time savings (it requires no travelling), cost savings and convenience of the procedure (as the entire procedure would be performed online). Provided that a sufficient number of cases is submitted to the e-court, it will also be possible for the judges to specialise in matters, which avoids the current state of

\(^{116}\) U. KOHL, o.c., p. 24
\(^{117}\) See Z. TANG, o.c., p. 50
\(^{118}\) P. CORTES, o.c., p. 30
affairs, where traditional courts must often be "educated" by the parties on the technology or online facility that underlies their dispute.

Compared to other ODR procedures, the most important advantage of the e-court would be that parties cannot refuse cooperation (at the risk of being sanctioned by the e-court). However, a possible modulation of the e-court could be that it would only apply when other means of dispute resolution (such as normal ODR) do not apply, for example because a party (most probably the service provider) refuses to participate\(^\text{119}\). Another important advantage is that e-courts would be more powerful, as their decisions do not need to be recognised by a court in order to be enforced.

**Competence** – In order to make the introduction of the e-court acceptable and realistic, we think it can be envisaged to apply several limitations to the competence of the e-court, at least during the initial phase.

A first restriction would be in the matters handled by the court. We would restrict the competence of the e-court to traditional e-commerce disputes, copyright and trademark infringements, data protection disputes and defamation cases:

- E-commerce disputes would include both services ordered and delivered online (download of software, music, videos or books, as well as access to other content online) and products ordered online.
- Disputes relating to intellectual property rights infringements would be limited to copyright, designs & models and trademark infringements, excluding any patent litigation. In our opinion, patent litigation issues are too complex to handle in a court for which an important goal is the speed and flexibility of its procedure.
- Cross-border data protection / defamation cases are becoming increasingly common, but are particularly difficult to deal with under the current legal instruments. For example, the "Rome II" Regulation on the law applicable to non-contractual obligations, explicitly excludes data protection issues. The same scope exemption applies to the new European small claims procedure.

In the initial phase, we would propose to limit the competence of the e-courts to disputes with a relatively low value (for example uphold a threshold of 4,000 EUR during the pilot phase). In light of the inexperience with the new court medium, cases with a value greater than this amount are probably best left to traditional courts during the start-up phase of the project.

It could also be considered to give e-courts the competence to deal with group proceedings (collective redress). It was already noted by the Commission that there is a need to develop specifically designed instruments for mass claims\(^\text{120}\). The organisation of such proceedings could be greatly enhanced by the use of Web 2.0 tools, which are tailored to cooperation between users.

**Enforceability** – As pointed out above, one of the major obstacles towards each ADR/ODR system is the enforceability of decisions. In this regard, it could be considered to link the decisions of the e-court to the domain names. When online service providers would refuse to comply with the e-court's decision, their domain name could be temporarily suspended (or even permanently blocked), provided that all rights of defence have been respected and all appeal possibilities have been exhausted.

---

\(^\text{119}\) Should, by the time the e-court is introduced, sufficient self-regulation regimes be developed for ODR service providers, then it could be envisaged to not take into account refusals to cooperate with ODR service providers that are not subject to a decent self-regulatory regime.

While the blocking of a domain name may seem like a harsh decision in reaction to an individual transaction, it should be borne in mind that such blocking is a very efficient tool, which would only be used in case a service provider persistently refuse to comply with the court's decision, which would be similar to "contempt of court" in the offline environment. Also, the blocking of a domain name is practically feasible across the EU, as the number of DNS-operators and large internet access providers is manageable across the EU (preferably, standards should be developed to facilitate how the e-court's decision to block a domain is ultimately rippled down to the access provider's systems).

In a first stage, the blocking of domain names could be limited to .EU domain names, which would then be promoted towards customers as a guaranteed safe shopping haven. National domain names and generic domain names could then join the e-court enforceability mechanism when the system would prove successful.\footnote{It should be acknowledged, however, that the blocking of their domain name blocking may not be a sufficient threat to all online service providers (in particular those service providers that do not operate a web site). Nevertheless, it would also affect these service providers to a certain agree (e.g., because the functioning of their e-mail addresses would be affected).}

**Difficulties** – Some practical difficulties can be expected in the technical aspects, for example how the real identity of parties can be checked, and how effective security can be ensured. However, as technology is rapidly maturing and the introduction of the e-courts is likely not for the immediate future, we think these practical hurdles can be overcome in time.

**Open issues** – There are no reasons why the e-court could not be used between two private individuals. However, the enforceability of decisions between private individuals could be lower than conflicts with service providers, as the leverage obtained from the domain-name blocking mechanism would not apply.

**Applicable law** – The question arises which laws should be applied by the new e-court. As pointed out in section 3 of this chapter, it is often very difficult to determine which law applies to a certain dispute, particularly when it concerns electronic services or tort law cases. These issues could be solved by clarifying the current rules of private international law (as set forth in section 6.2.2 above).
Chapter 13
Self regulation

1. Introduction

A lack of trust in the safety of internet transactions is the third most important reason for consumers not to engage in online transactions: a recent survey indicates that 42% of respondents do not have confidence in these transactions. In order to counter this trust issue, trustmarks and "web-seals" were introduced as from the late nineties. These trustmarks offer a kind of quality certification system, and are particularly used to foster a consumer's trust in the merchant's behaviour — particularly with respect to security, privacy, and general commercial practices. Web shops and online service providers that want to place the trustmark on their website, subscribe to the code of conduct of the trustmark organisation, and typically undergo an audit by the trustmark organisation to guarantee compliance. Trustmarks have therefore become the hallmark of typical self regulation schemes.

However, although they have been around for quite some time, trustmarks have never really taken off. According to recent studies, some EU Member States do not have any trustmark at all. Also, relatively very few web traders belong to trustmark organisations — for example, in the UK and Germany less than 10% of web shops have applied for a trustmark. There is also evidence which suggests that trustmarks have difficulties in achieving brand recognition by consumers and in becoming commercially viable and sustainable operations. As a result, there is a very low awareness of trustmarks, with only 10% of EU consumers claiming to have heard of them. Moreover, some trustmark organisations have proven to be not as trustworthy as they seem to be, as they did not react at all to obvious breaches of their code of conduct. Instead, the trustmark remained on the breaching merchant's website at the time the violations occurred and remained there after the wrongful act was discovered.

It may therefore not surprise that trustmarks have not yet lived up their expectations. Still, there is evidence that trustmarks can positively contribute to customer confidence in online shopping.

2. Self-regulation in the information society

Self-regulation is not a new concept in the information society, as it has been part of the Internet since its very conception. For example, the inner working of the most fundamental building blocks of the Internet

---

123 See, for example, TRZASKOWSKI, E-commerce Trustmarks in Europe — an overview and comparison of Trustmarks in the European Union, Iceland and Norway, January 2006
126 P. BALBONI, Third-party liability of trustmark organisations in Europe, p. 11, available at http://arno.uvt.nl/show.cgi?fid=90317
127 European Parliament, Consumer Confidence in the Digital Environment Briefing Note, o.c., p. 10
are based on so-called "Request For Comments", i.e. *de facto* standards developed by the Internet Engineering Task Force, an open standards organisation. Self-regulation is also a well-known concept in the regulation of professions, sports, not-for-profit associations, financial services, insurance, advertising, medical care, environment protection and press\(^\text{128}\).

### 3. Approaches to self-regulation

Legal literature typically distinguishes between *self-regulation* and *co-regulation*\(^\text{129}\).

- **Self-regulation (sensu stricto)** refers to the "substitution approach", according to which self-regulation can be used as replacement regulation, until state regulation would be adopted. Once the state intervenes, the self-regulated efforts step aside in favour of the state regulation. Contrary to the "co-regulation" approach described below, self-regulation *sensu stricto* is developed independently of state regulation, and is not situated in a predefined legal framework developed by the state. It implies a minimal legal environment model, which is independent from a state public law framework\(^\text{130}\).

- A second approach is "co-regulation", where the authority to self-regulate comes from the state, following traditional concepts of delegation of power. The state then entrusts the achievement of its objectives to recognised parties in the field (such as economic operators, social partners, non-governmental organisations or associations), drawing on their practical expertise in order to achieve optimum regulatory results\(^\text{131}\). All self-regulation should then be developed within the legal framework constructed by the state. Hence, there is a clear hierarchy between state regulation and self-regulation, as state regulation is more authoritative than self-regulation.

The co-regulatory framework is aspired to be dynamic and adaptable to markets, while at the same time being backed by government protection in areas of fundamental importance, such as privacy and consumer protection. The result is claimed to achieve wider "ownership" of the policies and better compliance\(^\text{132}\), as stakeholders are involved during the preparation and enforcement of the rules. Co-regulation then offers a customised regulatory solution that can fit the policies of a state, while meeting the demands imposed by the technical reality of the Internet. This approach is mainly followed in the European Union.

For the sake of brevity, the term "self-regulation", as used in the remainder of this chapter, refers to both subtypes (unless noted otherwise)\(^\text{133} \text{134}\).

---


\(^{129}\) See, for example, the definitions from the 2003 Inter-institutional Agreement Co-regulation between the Community institutions, the European Parliament, the Council and the Commission

\(^{130}\) M. BONNICI, G. PIA, *Self-regulation in cyberspace*, 2007, p. 25


\(^{133}\) M. BONNICI, o.c., p. 15

\(^{134}\) Some authors (see, for example, J. BONNICI, o.c., p. 15) also recognise a third approach to self-regulation: "hybrid self-regulation". This means that self-regulation is used together with state regulation to create a hybrid regulatory arrangement on the Internet, which contains elements of both state regulation and self-regulation, but can in effect be called neither. In this approach, the state regulation does not give authority to, or exercise control over, self-regulation. Instead, hybrid arrangements are developed for activities that would be problematic for either state regulators or self-regulation to be dealt with. An example is the safe harbour arrangement for data transfers from Europe to the United States.
It should be noted that self-regulation is not necessarily more effective in achieving its regulatory objectives than state regulation, as there is no decisive argument why state involvement means better regulation. In fact, the opposite is often stated\textsuperscript{135}. It should also be noted that self-regulation is not a dichotomous situation of "only state regulation" or "only private regulation". Instead, multiple sources of regulation (which also include social norms and technical standards) can be active in parallel in the information society\textsuperscript{136}.

4. Types of self-regulation

There exists a wide variety of self-regulatory arrangements, which behave differently in ways that reflect history, government and stakeholder support and engagement, policy domain and area, resources, competition, etc.\textsuperscript{137}. This section 4 provides an overview of the most common types of self-regulation, including some types for which the self-regulatory nature may not be immediately obvious.

4.1. Codes of conduct

Codes of conduct are the most well-known types of self regulation. A code of conduct is a set of rules that outlines the responsibilities of or proper practices for an individual or organisation\textsuperscript{138}. Member organisations subscribe to the code of conduct, and undertake to comply with the rules contained in it.

Codes of conduct are also at the core of a trustmark scheme, as it specifies all the obligations of participating shops, e.g. information requirements, mandatory participation in dispute resolution procedures and/or money-back guarantees\textsuperscript{139}.

The drafting of codes of conduct is recommended by several Directives, including the eCommerce Directive\textsuperscript{140} and the Data Protection Directive\textsuperscript{141}.

4.2. Trustmarks

4.2.1. Overview

Trustmarks or "web seals" arose out of the desire for data security and merchant credibility. They are generally considered as useful instruments for policymakers to foster the creation of consumer trust in e-commerce.

Typical trustmark systems are implemented via a vertical, top-down approach to accreditation, whereby an independent, high-level, third party is positioned as the final authority on trust.

\textsuperscript{135} HANS BREDOW INSTITUTE, Final Report Study on Co-Regulation Measures in the Media Sector, Study for the European Commission, Directorate Information Society and Media Unit A1 Audiovisual and Media Policies, June 2006, p. 17

\textsuperscript{136} See L. LESSIG, Code and other laws of cyberspace, 1999, p. 87

\textsuperscript{137} J. CAVE, C. MARSDEN, S. SIMMONS, \textit{Options for and Effectiveness of Internet Self and Co-Regulation}, Report prepared for the European Commission, 2008, p. 8

\textsuperscript{138} \url{http://en.wikipedia.org/wiki/Code_of_conduct}

\textsuperscript{139} R. DE BRUIN et al, o.c., p. 22

\textsuperscript{140} articles 10.2 and 16

\textsuperscript{141} article 27
If an online service provider fails to meet the trustmark’s requirements, a complaint can be filed. The trustmark provider will then investigate the alleged breach. Depending on the severity of the breach, the investigation can lead to recommendations to remedy the breach, or revocation of the trustmark.

In Europe, the online trustmark phenomenon is still in its infancy\(^\text{142}\), despite the fact that they have existed since the late nineties. Important trustmarks in Europe include Confianza Online (Spain), "Luxembourg e-commerce certified" (Luxembourg), Thuiswinkel (the Netherlands) and Trusted shops (United Kingdom). In the United States, Verisign, TRUSTe and BBB (Better Business Bureau) are the most important examples.

### 4.2.2. Shortcomings of trustmarks

**Recognition by consumers** – A number of studies have been undertaken on the effectiveness of such trust-mark initiatives. These studies derived varying conclusions as to their effectiveness. Some research indicates that, although consumers are aware of trustmarks, the awareness of legitimate trustmarks is dubious, and the actual understanding of what the trustmark effectively represents is relatively poor\(^\text{143}\).

**Low popularity with online service providers** – The percentage of companies who use trust seals is very low\(^\text{144}\). For example, less than 10% of German and UK web shops have subscribed to a trustmark scheme.

**Enforcement of compliance** – Trustmarks have been criticized for not being responsive enough to sanction members that – even repeatedly – violate the trustmark’s code of conduct or policy. Most trustmark organisations do not seem to put in place all possible mechanisms for establishing and monitoring compliance with their specifications\(^\text{145}\).

**Stability of trustmarks** – Due to the difficult business model, trustmarks do not yet offer sufficient stability. Since their boom in 2000 and 2001, many trustmarks have gone out of business, although new trustmark initiatives are still regularly announced. Although there was an initial boom in the establishment of trustmarks immediately after the adoption of the eCommerce Directive, activity in this area slowed down\(^\text{146}\). Already, many trustmarks have gone out of business.

**Poor "EU sensitivity"** – Trustmarks predominantly work only on the domestic level\(^\text{147}\). Most of the trustmark schemes expose a lack of "European sensitivity", i.e. a lack of multilingual information and lack of co-ordination between the existing EU initiatives regarding consumer confidence\(^\text{148}\).

**Independence and integrity of trustmark-provider** – Trustmark providers are paid by the website operator, which may undermine the independence and integrity of the trustmark provider. Trustmark

---

\(^{142}\) M. BONNICI, o.c.

\(^{143}\) T. MOORES, "Do Consumers Understand the Role of Privacy Seals in eCommerce?", *Communications of the ACM*, March 2005, Vol. 48 No 3


\(^{145}\) R. DE BRUIN et al, o.c., p. 78.

\(^{146}\) Report on E-commerce Directive, p. 16

\(^{147}\) G.P. CALLIESS, "Online Dispute Resolution: Consumer Redress in a Global Market Place", *German Law Journal*, Vol. 7, nr. 8, p. 656

\(^{148}\) R. DE BRUIN et al, o.c., p. 9
organisations can only be considered independent if their funding structure and the composition of their board of directors are neutral. However, this is often not the case\textsuperscript{149}.

**Liability of trustmark-provider** – It is currently not clear to which extent trustmark providers can be held liable by consumers\textsuperscript{150}.

**Continued compliance** – Another issue is that trustmarks reflect that the service provider complied with the trustmark’s requirements at the moment of audit. It is debated whether the display of trustmarks illustrates continued compliance, or just compliance at the time the user organisation was audited\textsuperscript{151}.

**Legitimising sub-optimal behaviour** – The very concept of trustmarks is sometimes criticised for legitimising sub-optimal behaviour, as they give consumers the impression that certain behaviour is better-than-average, while it may in fact be less-than-average (for example, with respect to privacy and data protection)\textsuperscript{152}.

### 4.3. Technical standards

Technical standards are an essential feature of the Internet. While not their primary intention, technical standards also have (self-)regulatory effects on internet activities, as compliance with technical standards is conforming to acceptable behaviour\textsuperscript{153}. Technical standards not only constitute a source of technical and legal rules, but also provide a way to implement rules of states and other entities, as they apply cross-border. Technical standards therefore complement the implementation of rules coming from state legislation.

Although this has been criticised in literature, in fact most technical standards meet all the criteria that are commonly required for a rule to be considered “law”\textsuperscript{154}. Most standards are *generally applicable to all situations*, and are not decided upon on an ad hoc basis. Also, most technical standards are *publicly known* and available to citizens\textsuperscript{155}. Technical standards also have a *prospective character*, by applying to future situations, and not only to past behaviour. Finally, technical standards are generally *consistent with existing higher ranked laws* and legal doctrine. Technical standards are therefore a kind of self-regulation in their own way.

### 4.4. Labelling systems, user rating systems and reputation techniques

Labelling systems, user rating systems and similar reputation-based techniques involve a platform where either content is rated, or the quality of service providers is rated (quality of products, richness of information provided, responsiveness after customer care services, …). Often, comments can also be attached and warnings can be issued about the content or the service provider, which can then be used as guidance for other customers.

**Traditional labelling systems** involve a self-regulatory group that examines content and attaches a certain label, in accordance with predefined rules. They are recommended by the European

\textsuperscript{149} P. BALBONI, o.c., p. 63
\textsuperscript{150} P. BALBONI, o.c., p. 14
\textsuperscript{151} C. MARSDEN, o.c., p. 225
\textsuperscript{152} C. MARSDEN, o.c., p. 234
\textsuperscript{153} M. BONNICI, o.c., p. 135
\textsuperscript{154} M. BONNICI, o.c., p. 163
\textsuperscript{155} The actual use of the standard may, however, require licensing.
Commission\textsuperscript{156} in the context of the Audiovisual Media Services Directive. Examples include the Internet Content Rating Association (ICRA) and the Netherlands Institute for the Classification of Audio-visual Media (NICAM), which are further discussed below.

User rating systems\textsuperscript{157}, on the other hand, constitute a typical example of the consumer use of Web 2.0 technologies to counter the information asymmetry in the environment for trust. They rely on the collective goodwill of participating users. Practice shows, however, that a significant amount of users is willing to make such small contributions to foster the improvement of the community\textsuperscript{158}. Some websites have also adopted these user ratings for rating their own products, services and content\textsuperscript{159}. Other than rating service providers, products and services, they can also used to filter harmful content, select useful comments\textsuperscript{160}, or report inappropriate behaviour\textsuperscript{161}.

5. Importance of self-regulation

Self-regulation is seen as an important regulation strategy for the EU. It has been advocated by the European Commission, Member States and various experts, and has been invoked by the Commission. Moreover, it is already used in different EU legal instruments.

5.1.1. European Commission

The European Commission is a strong supporter of self-regulation, and has repeatedly recommended self-regulation as a way to improve consumer confidence and gradually resolve issues in the online world\textsuperscript{162}.

In the “Interinstitutional Agreement on Better Lawmaking”\textsuperscript{163}, the European Parliament, Council and Commission agreed that co-regulation constitutes an alternative method of regulation, which fits well with the obligation to legislate only where it is necessary and to the principles of subsidiary and proportionality\textsuperscript{164}.

Various documents emanating from the Commission reflect this position, such as the Council Resolution and Commission Communication on illegal and harmful content on the Internet\textsuperscript{165} and the Commission Green Paper on the protection of minors and human dignity in audiovisual and information services\textsuperscript{166}.

\begin{itemize}
  \item[157] Examples include epinions.com, ciao.co.uk, www.bizrate.com, www.consumerreview.com, etc.
  \item[158] ENISA Position Paper No.1, Security Issues and Recommendations for Online Social Networks, October 2007, p. 20
  \item[159] C. MARSDEN, o.c., p. 232. Well-known examples include the product ratings on Amazon.com and iTunes
  \item[160] e.g., on a discussion forum with many reactions
  \item[161] ENISA, o.c., p. 20
  \item[162] V. REDING, speech at the ISFE Expert Conference, 26 June 2007
  \item[163] 2003/C 321/01
  \item[164] HANS BREDOW INSTITUTE, o.c., p. 19
  \item[165] See, respectively, OJ C70 6, March 1997 and COM (1996) 487, 16 October 1996
  \item[166] COM (1996) 483, 16 October 1996
\end{itemize}
5.1.2. Previous studies

Self-regulation has also been recommended by numerous studies undertaken on behalf of the Commission. For example,

- the Bangemann Group Report\textsuperscript{167} referred to self-regulation as an interesting legal instrument that supports the argument that the EU should only directly regulate itself to ensure the competitiveness and regulatory position of the internal market;

- the use of self-regulation has also been recommended by a recent study on the effectiveness of self-regulation on the Internet, undertaken on behalf of the Commission. In their final report, the contractors argue that "wherever possible, policy should incorporate analysis of [co-regulation and self-regulation organisations], and should be designed with positive incentives for compliance and innovation by [these organisations]"\textsuperscript{168};

- at the presentation of the study on co-regulation in the media sector and Internet industry, commissioner REDING stated that "self-and co-regulation offer very real alternatives to traditional legislative approaches in the media sector today. Where such self and co-regulatory models are credible and efficient, the European Commission will encourage their use, in particular for the online environment."\textsuperscript{169}.

5.1.3. Existing legal instruments that refer to self-regulation

Self-regulation is already advocated by several Directives in the information society.

- Article 16 of the \textbf{eCommerce Directive} requires Member States to encourage trade, professional and consumer associations / organisations to draw up codes of conduct to facilitate the implementation of the Directive. Member States should also encourage the involvement of other stakeholders (such as consumer organisations, associations representing the visually impaired and disabled) in the drafting process. Article 16 also requires that these codes of conduct are made accessible by electronic means.

  Furthermore, article 10.2 of the eCommerce Directive requires an online service provider to indicate all relevant codes of conduct to which it subscribes and information on how those codes can be consulted electronically.

- Article 27 of the \textbf{Data Protection Directive} instructs Member States to encourage the drawing up of codes of conduct to implement national data protection provisions. The national data protection authorities and Working Party 29 must review the compliance of national or community-level codes of conduct submitted to them.

- In the recital of the \textbf{Audiovisual Media Services Directive}\textsuperscript{170}, it is noted that "experience has shown that both co- and self-regulation instruments, implemented in accordance with the different legal traditions of the Member States, can play an important role in delivering a high level of consumer protection. Measures aimed at achieving public interest objectives in the emerging audiovisual media services sector are more effective if they are taken with the active support of the


\textsuperscript{168} J. CAVE, o.c., p. xiv


\textsuperscript{170} nr. 36
service providers themselves” and that “Member States should, in accordance with their different legal traditions, recognise the role which effective self-regulation can play as a complement to the legislative and judicial and/or administrative mechanisms in place”.

Article 3.7 of the Directive encourages the adoption of broadly accepted co-regulatory and/or self-regulatory regimes at the national level, which provide for effective enforcement.

6. Advantages and limitations of self-regulation

6.1. Advantages of self-regulation

- **Speed** – Self-regulation is typically quicker to establish or change rules, compared to state regulation. Nevertheless, this can diminish with the size and scope of membership and the range of interests represented.

- **Expertise** – States may not always have the necessary technical expertise to deal with complex (cross-border) issues, which makes both the adoption and enforcement of state legislation difficult in more difficult scenarios. Conversely, industry players that are involved in self-regulation typically have a detailed knowledge of the issues at stake, as well as possible solutions. In general, the knowledge and expertise is therefore used more effectively in self-regulation schemes.

- **Maintaining industry reputation** – Self-regulation can maintain the reputation of an industry sector among customers and consumers. By adhering to a code of conduct, service providers may expect enhanced trust and confidence in their services.

- **No unnecessary regulatory costs** – Public policy literatures states that there is always a hidden price for regulation (e.g., in the form of distortion, cost, institutionalisation, agenda creep, etc.). The risk of incurring such societal hidden costs is less pronounced with self-regulation.

- **Reduction in state costs associated with regulation** – States are increasingly keen to shift part of the regulatory costs (drafting and enforcement) to the private sector. Although states frequently contribute to self-regulatory initiatives, self-regulatory initiatives can generally reduce legislation costs.

- **Cross-border enforcement** – Although the effective enforcement of self-regulatory initiatives is a disadvantage rather than an advantage of self-regulation (see below, section 6.2), it should be pointed out that self-regulatory initiatives that integrate realistic sanctions in their enforcement model, can better apply cross-border enforcement, compared to state legislation. Furthermore, state law enforcement agencies do not always have the necessary technical tools and access to enforce the state rules on the Internet.

- **Laying the groundwork** – When states would eventually introduce legislation in an area that is already regulated by self-regulatory initiatives, states often recognise the usefulness of the self-regulation rules, and adopt them in their legislation. Even when state regulation would eventually uphold a different position than the position taken by self-regulation, self-regulation can still be an important source for the

---

171 See, in general, J. CAVE, o.c., p. 48
172 M. BONNICI, o.c., p. 85
173 For example, the UDRP or .EU procedures, where the cancellation or transfer of the disputed domain name is obviously a very effective sanction.
174 M. BONNICI, o.c., p. 75
state position. It will, as a minimum, provide a point of departure for the route state regulation will — or will not — follow\textsuperscript{175}.

**Assisting state regulation enforcement** – Self-regulatory initiatives can assist the enforcement of state regulation, for example by offering “hotlines” and reporting channels where members or third parties can submit complaints of breaches.

### 6.2. Primary disadvantages and limitations of self-regulation

#### 6.2.1. Difficulties to enforce

Even though self-regulation can deliver interesting results when all members comply with the agreed rules, the effective enforcement of the rules by the members remains a brittle point, particularly when the self-regulatory organisation lacks effective sanctions, or lacks the information necessary to verify non-compliance\textsuperscript{176}.

Enforcement can come from different angles:

- **Reputation** – Internet service / access providers cannot afford a bad reputation, because reputation is one of their most significant intangible resources\textsuperscript{177}. They will therefore often be inclined to sign up to a self-regulatory initiative and comply with the agreed rules, in order to preserve their good reputation.

- **State** – In some cases, the state requests compliance with the self-regulatory rules. For example, the Australian Communications Authority requests member of the Australian Internet Industry Association and the Australian Direct Marketing Association to comply with the rules developed by these organisations\textsuperscript{178}.

- **Contract** – Self-regulation organisations may have contractually agreed that a non-complying member will pay monetary damages, or lose certain securities.

- **Code** – Enforcement can also occur through software code. Although this may not be immediately apparent, the technical architecture of the Internet has become an instrument of control. Indeed, software (programming code) can control activities more perfectly and more completely than traditional state rules and sanctions\textsuperscript{179}. Software has therefore assumed a central role in the Internet governance debate\textsuperscript{180}. It can define who can access a certain website, who can access certain content protected by technical protection measures\textsuperscript{181}, etc.

As a result, self-regulatory organisations must not necessarily rely on state authorities to achieve effective enforcement through software code (“self-enforcement\textsuperscript{182}”). When they can make their

\textsuperscript{175} M. BONNICI, o.c., p. 57-58
\textsuperscript{176} J. CAVE, o.c., p. 48
\textsuperscript{177} S.C. ZYGLOPOULOS, “The social and environmental responsibilities of multinationals: evidence from the Brent Spar case”, *Journal of Business Ethics*, Vol. 36, issue 1, p. 141-152
\textsuperscript{178} M. BONNICI, o.c., p. 66
\textsuperscript{179} M. BONNICI, o.c., p. 132
\textsuperscript{180} Summarised in the phrase “code is law”, after Lawrence Lessig’s *Code and Other Laws of Cyberspace*
\textsuperscript{181} See, for example, the Content Scramble System (CSS) used on DVDs, the protection of Adobe Acrobat eBook Readers, or the “FairPlay” content protection system used by Apple’s iTunes.
\textsuperscript{182} PATRIKIOS II, p. 131
members dependent on specific software, they can enforce compliant behaviour through software. Of course, it should be recognised that not all of online behaviour can be controlled through code.  

6.2.2. Getting all players on board  

Related to the issue of enforcement, is the issue that self-enforcement can only be really effective when a majority of relevant entities sign up to the self-regulatory initiative. Even though it is not necessary to attract all players in the first stage – the attractiveness of the self-regulatory regime often attracts remaining players in a second stage – there is the issue that the real "baddies" never join the self-regulatory initiative.

6.3. Secondary disadvantages and limitations of self-regulation  

Protecting the users – Self-regulation is often used as a mechanism by industry players to balance interests, or to prevent state intervention in a certain area. Although self-regulation is at several levels intended to protect users, it should be recognized that it does not always sufficiently protect the fundamental rights of users, who are typically not involved in the drafting process of the rules. Conversely, the democratic institutions of countries are said to ensure a proper degree of user involvement and protection in the drafting process of traditional legislation.

Binding the users – Another criticism is that self-regulation can indirectly bind end-users, although these users have not been involved in the drafting process. It should be pointed out, however, that this indirect binding is not the case for all types of self regulation. In fact, self-regulatory initiatives often leave the decision up to users (as is the case with, for example, privacy filters, content filters and rating systems).

Protecting the public interest – Similar to the objection that self-regulation would not adequately protect the user, it is argued that self-regulation does not adequately protect the public interest, as self-regulation primarily protects the interests of a specific group of industry players.

Legitimacy and accountability – There are concerns about the degree to which self-regulation organisations are willing to adhere to principles of good regulation, such as transparency, accountability, proportionality and consistency.

Anti-competitive effects – Depending on its purpose and participants, self-regulation may have anti-competitive effects. For example, when well-established companies enter into agreements within a co-regulatory framework, this may hinder the market entry of competitors.

Possible lack of clarity – Self-regulatory initiatives are often taken in response to specific issues. Rules of self-regulation may therefore develop in an ad hoc and accidental manner, effectively creating a decentralised patchwork of initiatives. Consumers (and others) may be confused about the level of

183 SCHONBERGER, p. 17  
184 J. CAVE, o.c., p. 29  
185 E.g., codes of conduct that establish how online service providers should deal with a user's personal data.  
186 M. BONNICI, o.c., p. 61  
187 J. CAVE, o.c., p. 50  
188 J. CAVE, o.c., p. 48  
189 M. BONNICI, o.c., p. 67
compliance to expect or the consequences of dealing with non-complying or non-participating firms. The risk of confusion is magnified when industry players are unable to agree on a single code or standard\textsuperscript{190}.

\section*{7. Some examples of self-regulation}

\subsection*{7.1. Internet content}

States are often reluctant to regulate harmful content, as they risk being accused of censorship. Internet content regulation is also problematic on an international level, where countries are often unable to agree on regulation to deal with harmful content\textsuperscript{191}. What can be considered illegal in one country, may be considered merely harmful (or even perfectly legal) in another country\textsuperscript{192}.

Self-regulation can therefore play an important role in the fight against illegal content. Funding self-regulation initiatives can then prove to be a more practical approach\textsuperscript{193}.

Self-regulation is indeed often the first to provide a set of rules to regulate internet content. This has been the case, for example, with the development of notice-and-takedown rules, which were first adopted by internet access providers, and were subsequently adopted in national legislation and the eCommerce Directive\textsuperscript{194}.

\subsection*{7.1.1. EU-level}

The EU has long recognised that the only real option for regulating harmful content is through self-regulation. In the Green Paper on the protection of minors and human dignity on the Internet\textsuperscript{195} it was stated that \textquotedblleft(b)ecause of the varying cultural and social norms, self-regulation (...) will provide the most suitable solution for the regulation of harmful content\textquotedblright. As from 1997, the European Commission has funded initiatives to support illegal content hotlines, with the Safer Internet Action Plan is the most important example.

\subsection*{7.1.2. National level}

On a national level, there are several examples of successful self-regulatory regimes to deal with harmful content.

\textbf{PhonePayPlus} – PhonePayPlus (formerly "ICSTIS") is an independent regulatory body responsible for creating a Code of Practice, which must be complied with by all UK premium rate service providers. There is a range of sanctions than can be imposed (including very powerful financial penalties) if a service provider is found to have breached the Code of Practice. The Code of Practice also includes general requirements for network providers to assist in its regulation of companies offering premium rate services. PhonePayPlus runs a complaints hotline which received over 131,000 calls in 2006 and 2007\textsuperscript{196}.

\begin{footnotesize}
\begin{itemize}
\item J. CAVE, o.c., p. 48
\item See M. BONNICI, o.c., p. 36
\item M. BONNICI, o.c., p. 36
\item M. BONNICI, o.c., p. 46-47
\item M. BONNICI, o.c., p. 82
\item OJ C287, 22 September 1997, p. 11
\item C. MARSDEN, o.c., p. 146
\end{itemize}
\end{footnotesize}
ICRA – ICRA, the Internet Content Rating Association, has developed a set of content descriptors to label or rate content. These descriptors were determined through a process of consultation with various stakeholders. Online service providers can use the ICRA logo (for example, on their website) if the content they publish is in accordance with the ICRA descriptors, and also complies with ICRA’s terms and conditions. ICRA is an example of a filtering system that strives for minimal self-regulation, permitting maximum end-user choice.

There seems to be agreement that ICRA is a technology that is a great idea, but lacks effectiveness due to the lack of mandatory participation. While interest in ICRA was high in the late 1990s, interest seems to have declined since that time.197

NICAM – The Netherlands Institute for the Classification of Audio-visual Media (NICAM) classifies media content in the Netherlands. It grew from a consensus decision on a pan-media system of self-regulation, in order to replace the state regulation model in place. The system is mandated by Parliament, and reports to Parliament. More than 2,200 companies and organisations are affiliated to NICAM, which is considered a transparent and widely adopted system.198

NICAM is responsible for the “Kijkwijzer” scheme, through which media content providers code their programming according to fixed categories of content type. Kijkwijzer warns parents and educators about a television programme or film which can be harmful to children of different ages. Any citizen can complain to the Kijkwijzer system, following which a commission evaluates the complaint. If the complaints are upheld, the Complaints Committee can enforce fines on the participating organisations.199

Although the intention was initially to phase out the involvement of the government, an entirely self-regulatory body was not found to be desirable for classifying audiovisual content. Therefore, it was decided to keep some oversight and financial contributions from the Dutch Ministry.200 Although participation is voluntary, there is strong participation level among audiovisual companies, as companies that do not participate will fall under the governmental regulatory regime.

7.1.3. Japan

In Japan, online malls such as Rakuten (www.rakuten.co.jp) have been developed, on which thousands of retailers are established. Rakuten can be considered a new type of trustmark, as millions of customers trust the online retailers that are admitted to the online mall. Rakuten guarantees that customers get their money back when a product or service would be defect, or when a service provider would go bankrupt.

Rakuten is therefore yet another example of the possible success of trustmarks, and the requirement that trustmarks must give some added value on top of merely suggesting trustworthiness.

7.2. Technical standards

As noted in section 4.3, technical standards have always played an essential role on the Internet. Successful technical standards organisations are therefore not difficult to find.

---

197 Ibid., p. 80
198 Ibid., p. 159
199 Ibid., p. 165
200 Ibid., p. 160
IETF – The principal standards-setting body for the Internet is the Internet Engineering Task Force (IETF), which is an open international organisation of parties involved in network infrastructure. The IETF’s main activity is developing and publishing “Requests For Comment” documents. The IETF is a volunteer organisation which has been enormously successful at driving the continued evolution of the Internet, and introducing many standards. It is also heralded as one of the most open and transparent organisations involved in standardisation.

W3C – Another important organisation involved in technical standards on the Internet is W3C, which has as its central mission the development of standards for the world wide web (e.g., HTML). Contrary to the IETF, the W3C is sometimes criticised for being a victim of its own success, with the accusation that it is captured by its corporate clients, and is not sufficiently focused on developer needs in the start-up community. Even so, it is also recognised for its introduction of many important standards, which are – for example – used in all web browsers.

8. Second-level self-regulation on online platforms

Online platforms are an interesting new territory for the application of self-regulatory principles, as they raise the question to which extent the users of the platforms can take self-regulatory initiatives and/or participate in the governance of the platform. In effect, such initiatives could be called "second-level" self-regulation, as they emanate by the users in the platform. This section 8 provides an overview of self-regulatory initiatives on online platforms, with particular focus on user involvement.

8.1. Social communities

Recently, several self-regulatory initiatives have been undertaken by social community websites:

- **Safer Social Networking Principles** – On 10 February 2009, several leading social community websites — including Facebook, MySpace, Netlog and Google/YouTube — adopted the "Safer Social Networking Principles for the EU", developed in consultation with the European Commission and a number of nongovernmental organisations, in the framework of the "Safer Internet Programme". The Principles focus on the safety and protection of children and young people, with specific focus on cyber-bullying, grooming and risky behaviour, like revealing personal information. The Principles aim to mitigate such risks, *inter alia* by providing a "report abuse" button on the website, making sure that the privacy settings of minors are set to private by default, ensuring that private profiles of minors are not searchable, and guaranteeing that privacy options are prominent and accessible at all times.

- **Facebook user involvement** – In response to fierce user reactions following the surreptitious changing of its terms & conditions, social community site Facebook announced in February 2009 a new approach as to how the company would create future policies that impact user privacy. Facebook has developed a set of self-regulatory controls, and has also invited users to comment on these controls. The new approach is described as "a set of values that will guide the development of the service, and Statement of Rights and Responsibilities that make clear Facebook’s and users’ commitments related to the service." A core part is that Facebook will notify the community of all
policy changes in the website, and will allow a period of time for Facebook users to comment. If these user comments or interest would reach a certain threshold, then the change could even be voted on by the community. Facebook also announced that it would establish a “user council” to participate more closely in the development and discussion of policies and practices.

- **MySpace agreement with US attorney generals** – On 14 January 2008, social networking website operator MySpace announced a joint effort with 49 state Attorneys General to better protect children online. Similar to the EU Safer Social Networking Principles, this effort tries to combat harmful material (such as pornography, harassment, cyberbullying and identity theft), better educate parents and schools about online threats, cooperate with law enforcement, and introduce various other security measures (e.g., mechanisms to protect minors, age verification, as well as an opt-out registry for parents).

8.2. **Wikipedia**

Wikipedia is the well-known free, multilingual encyclopaedia project supported by the non-profit Wikimedia Foundation. Wikipedia’s more than 13 million articles have been written collaboratively by volunteers around the world, and almost all of its articles can be edited by anyone who can access the Wikipedia website. The intrinsic openness of Wikipedia attracted increasing numbers of contributors and quickly developed a life of its own.

**Early governance model** – In the early stages of Wikipedia, Wikipedia’s administrators argued that there was a need for participants more than rules, as well as a need to gain experience with how wikis worked, so the only rule was that “there is no rule” to use Wikipedia. In a first stage, “force of personality” and “shaming” were the only means used to control contributors, which was coined "good natured anarchy".

**Evolving model** – However, in a study on the conflict and coordination costs of Wikipedia, it was noted that there was a significant increase in regulatory costs over time: "...direct work on articles is decreasing, while indirect work such as discussions, procedure, user coordination, and maintenance activity (such as reverts and anti-vandalism) is increasing". To cope with this, the “zero rule” was replaced with a set of permissions, obligations, rules and norms, documented in guidelines and etiquettes, as well as embedded in code. Nevertheless, there are relatively few means of formal control, so that the community mainly relies on informal or "soft" controls. The openness of the wiki platform and the low cost of joining and leaving precludes formal control as a primary means for governance.

**Editing possibilities** – Wikipedia recognises special "editors", who generally have detailed knowledge about specific subjects, hold electable positions and have special rights on the website (e.g., the ability to delete a page or protect it from being edited by others). As a result, editors can exercise a certain degree of authority. However, even editors do not hold privileged positions in the community: many Wikipedia

---


210 C. GOLDSINK, o.c., p. 14
participants consider the editors as mere janitors, whose behaviour is held to certain higher standards, but whose authoritative power is fairly limited.\footnote{P. KONIECZNY, Something wikid this way comes: Wikipedia as a case study of adhocratic governance in the Internet age, July 2008, p. 10, available at www.allacademic.com/meta/p237649_index.html}

After all, even Wikipedia's policy pages can be edited, like any other encyclopaedia article. The prerogatives of the administrators (and the founder) are not well defined. Whenever a user is no longer satisfied with the governance model or evolution of Wikipedia, he can "fork" the project (i.e., take all the content and copy it to a new website).

**Evaluation** – Wikipedia's model of governance seems very difficult to categorize: characterizations range from anarchy to democracy, dictatorship, a hybrid model, or an adhocracy (i.e., self-governing institution).\footnote{P. KONIECZNY, o.c., p. 5} Even so, compared with platforms run by commercial entities, Wikipedia is self-controlled, and allows ample opportunities of user involvement.

### 8.3. Virtual worlds

#### 8.3.1. Overview

Although virtual worlds have existed for quite some time, they have only really taken off since about 2003. The most ubiquitous examples of virtual environments are multiplayer online games such as "Second Life" and Massive Multiplayer Online Role Playing Games (MMORPGs).

For those who are unfamiliar with virtual worlds, these problems may seem largely theoretical or of little economic relevance. However, in-world disputes have the potential to extend into the real world. For example, in 2008, Second Life had over fifteen million users who collectively spent more than twenty million dollars in the virtual world every month. When the virtual banking industry collapsed in Second Life, users lost an estimated $750,000 in real-world money in the virtual economy. Linden Lab initially refused to take action to solve this problem,\footnote{P. STOUP, "The development and failure of social norms in Second Life", *Duke Law Journal*, 2008, Vol. 58, 311, p. 342} although it eventually set up a Second Life Securities Exchange Act, to provide market stability and investor confidence.\footnote{C. MARSDEN, o.c. I, p. 198}

**User participation** – In general, the rules of the virtual world, as well as the possibility for users to participate in the rule making process, are made by the virtual world provider, which does not typically offer any guarantee of transparency or democratic participation to the users.

However, there are also numerous examples of failed attempts to introduce such democratic participation.\footnote{V. MAYER-SCHÖNBERGER and J. CROWLEY, *Napster’s Second Life? The Regulatory Challenges of Virtual Worlds*, September 2005, p. 20} Faced with this issue, providers therefore choose to retain control.\footnote{V. MAYER-SCHÖNBERGER and J. CROWLEY, o.c., p. 23} As a result, virtual world providers find it very difficult to create an enforcement process that is both efficient and responsive to the expectations of users.\footnote{V. MAYER-SCHÖNBERGER and J. CROWLEY, o.c., p. 25; STOUP, o.c., p. 330}

**Enforcement through code** – Virtual world providers can easily rely on software ("code is law") to enforce rules. Participants who violate the rules can be expelled from the virtual world,\footnote{V. MAYER-SCHÖNBERGER and J. CROWLEY, o.c., p. 17} which can be...
an effective enforcement mechanism because participants will incur significant costs when they are forced to leave\textsuperscript{219}.

\subsection*{8.3.2. LambdaMOO}

An early example of a virtual world is LambdaMOO, an online virtual reality system to which multiple users (players) are connected at the same time. It can be considered a predecessor of today's online games.

The Mr. Bungle incident – LambdaMOO is famous for its governance incident regarding a user\textsuperscript{220} called "Mr. Bungle"\textsuperscript{221}, who committed virtual rape against other users of LambdaMOO. While the community was arguing on how to react to these virtual crimes, a senior administrator took unilateral action by destroying the character of Mr. Bungle, thus permanently eliminating the character from the community. This case led to a kind of political awakening on LambdaMOO\textsuperscript{222}, which made users realise that they needed rules to govern their virtual community. As a result, a petition mechanism was installed, which allowed the community to propose and vote on new policies and other administrative actions. However, this system suffered quite a lot of evolution, and was ultimately reduced to a state where administrators ("wizards") took back the control of the users, although the ballot system was maintained as a way for the users to express their opinions\textsuperscript{223}.

\subsection*{8.3.3. Second Life}

Second Life is an online virtual world developed by Linden Lab, which launched in 2003. Its users, ("residents") can interact with each other through their alter ego's ("avatars") to explore the virtual worlds, meet other residents, participate in activities, and create and trade virtual property and services\textsuperscript{224}.

Governance – Linden Lab applies a set of terms & conditions, in which it reserves the right to maintain control of in-world activity by suspending or terminating accounts\textsuperscript{225}. Linden Lab also imposes compliance with the "Community Standards" agreement\textsuperscript{226}. The latter agreement sets forth six behaviours that may result in account suspension or expulsion from Second Life\textsuperscript{227}.

However, Linden Lab has taken the position to minimise its "in-world" authority. It considers itself as a platform, rather than an administrator or government, leaving dispute resolutions to its residents\textsuperscript{228}. Even though Linden Lab encourages the development user governance initiatives, and offers moderators to resolve disputes, it considers Second Life a private space, which should be left to private rulemaking. This should not surprise, because the massive scale of Second Life makes it very difficult for Linden Lab to effectively monitor all user interactions\textsuperscript{229}. In any case, Linden Lab is hesitant to terminate user

\begin{footnotesize}
\begin{itemize}
\item[\textsuperscript{219}] They have to leave their identity (avatar), their virtual property, their network of virtual friends, etc.
\item[\textsuperscript{220}] actually, it concerned a group of undergraduates sharing a single identity
\item[\textsuperscript{221}] See L. LESSIG, Code v 2.0, p. 98
\item[\textsuperscript{222}] See J. GOLDSMITH and T. WU, Who controls the Internet? Illusions of borderless world, p. 15
\item[\textsuperscript{223}] See \url{http://en.wikipedia.org/wiki/Lambdamoo}
\item[\textsuperscript{224}] See \url{http://en.wikipedia.org/wiki/Second_Life}
\item[\textsuperscript{225}] See CHIN, "Regulating Your Second Life: Defamation in Virtual Worlds", Brooklyn Law Review, Vol. 72, No. 4, 2007, p. 1318
\item[\textsuperscript{226}] C. MARSDEN, o.c. I, p. 196
\item[\textsuperscript{227}] intolerance, harassment, assault, disclosure, indecency, and disturbing the peace. See CHIN, p. 1325
\item[\textsuperscript{228}] V. MAYER-SCHÖNBERGER and J. CROWLEY, o.c., p. 25
\item[\textsuperscript{229}] P. STOUP, o.c., p. 328
\end{itemize}
\end{footnotesize}
accounts, as there have already been precedents where state court proceedings have been initiated against Linden Lab due to a dispute with a resident\(^{230}\).

As a result, self-regulation in the form of norms established by users have become very important, and many residents take active part in the monitoring of offending behaviour\(^{231}\). Some argue, however, that Linden Lab should create a more comprehensive penal code, which needs to outline the specific punishment for a particular behaviour. Such penal code would have the additional benefit of educating real-world courts about the important norms or objectives in the virtual world\(^{232}\).

8.4. Conclusion

The creation of legal rules on user involvement of online platforms is largely undiscovered legal territory. Although user involvement initiatives are slowly creeping into online platforms, these initiatives seem to be largely taken out of self-interest, for example due to threats for imminent legislation (e.g., MySpace\(^{233}\)) or for commercial reasons (e.g., the public outcry of Facebook's user community after the surreptitious modification of the terms & conditions).

While these initiatives introduce some democratic elements in the online platforms, the actual participation remains largely superficial. As rightfully pointed out by L. LESSIG: “These [platforms] are all democracy-like. But they are not democracy. Democracy is the practice of the people choosing the rules that will govern a particular place. And with the exception of Wikipedia, and there are very few major Internet or cyberspace institutions that run by the rule of the people”\(^{234}\).

For the time being, the legal terms & conditions of platforms run by commercial entities qualify as the "Constitution" of the online platform, which can be unilaterally changed by the service provider, with only marginal involvement of the users. These terms & conditions are often supplemented by rules of conduct, which dictate the appropriate behaviour and rights of users and the service providers themselves. Together, the terms & conditions and rules of conduct constitute the crossover between cyberspace and the real world\(^{235}\). Although platform owners can use software code to enforce user behaviour, terms & conditions can be more time and cost efficient, if online because codes only limit (do not eliminate) conflicts.

When the social importance of the online platforms will keep growing, the question arises whether this situation should not be regulated — if not by state regulation, then by self-regulation. Although we think it is too early to interfere with these platforms (particularly virtual worlds), this issue should be monitored, as anecdotal evidence suggests that issues are rising.

It may, however, be interesting to adopt self-regulation which creates norms and minimum rights for user involvement in large online communities.

\(^{230}\) P. STOUP, o.c., p. 331

\(^{231}\) P. STOUP, o.c., p. 328

\(^{232}\) P. STOUP, o.c., p. 337

\(^{233}\) For example, the attorneys general with whom MySpace had entered into an agreement, confirmed that they wanted to avoid legal action against social-networking sites, because "litigation is costly, time-consuming, (and) uncertain in its result".

\(^{234}\) L. LESSIG, Code v2.0, p. 285

\(^{235}\) B. CHIN, p. 1317
9. General evaluation of self-regulatory initiatives

9.1. Success criteria

From the analysis above, the following success criteria can be deducted for self-regulation to flourish:

- **Difficulty to receive political consensus** – as the drafting process of the Cybercrime Convention showed, it can be very difficult to achieve a political agreement between a large number of countries. For those situations where regulation is necessary, but political agreements are not viable in the near future (e.g., regulation of harmful content), self-regulation can be an important option.

- **Difficulty to enforce regulation** – Self-regulation can also be an important type of regulation when traditional, state-emanated regulation cannot properly enforce regulation, either due to technical difficulties, or due to the inherent cross-border nature of the Internet.

- **Interference with emerging technologies** – Interfering with emerging technologies is generally not a recommended policy option that enables further maturing of the technology. Self-regulation can constitute an important alternative, as it allows the sector to regulate those areas that are most important, while keeping flexibility options open in the future.

- **National level is too limited** – Self-regulation constitutes an interesting tool for those areas where the national level is too limited. For example, although a Member State could impose various quality criteria on its national web shops, these quality criteria will not increase the trust of foreign consumers. Conversely, EU-level trustmarks or codes of conduct can diminish the threshold for a consumer to shop in foreign web shops.

- **Distribution of monitoring workload** – Self-regulation is also particularly useful when the workload to monitor compliance is very high, as is – for example – the case with labelling harmful content. Self-regulatory regimes can distribute the workload among many parties, and also install “hotlines” where users and other third parties can submit complaints.

9.2. Requirements for all self-regulation initiatives

**Consensus between all stakeholders** – To be efficient, self-regulation must reflect a consensus between all relevant stakeholders. Self-regulatory organisations must involve consumers, enforcement bodies and other stakeholders throughout the preparation of the rules. This is a key success factor in making sure that consumer codes of practice are relevant to real consumer needs.

**Effective sanctions** – Self-regulators must adopt a range of sanctions for handling non-compliance by members. Preferably, more than one possible sanction is adopted, whereby the various sanctions can be escalated (e.g., warning letters, fines, termination of membership, for dealing with non-compliance, ...), or combined. All sanctions must be commensurate with the nature of the breach, as well as the repetition/frequency of breaches by the same member. Furthermore, systems and policies for handling breaches should be built into the design of the self-regulatory initiative.

---

236 For example, the drafting process of the Cybercrime Convention – which took more than five years – demonstrates the (almost) unassailable differences between the treaty states. As regards illegal content, the only consensus reached concerned child pornography.

237 Commission communication B2B, p. 8; Office of Fair Trading, p. 11

238 R. DE BRUIJN et al, o.c., p. 7

239 Office of Fair Trading, p. 40
Dispute resolution – (Where relevant), the self-regulatory initiative must install a low-cost, responsive, transparent and user-friendly alternative dispute resolution mechanism, which is binding on members. Where possible, the redress scheme should be free to consumers, must be independent from the self-regulation organisation, and must not mandate assistance of a legal representative.

Governance – Self-regulation organisations must be accountable and capable of following open procedures. Particularly trustmark schemes must be transparent in order to increase consumer trust. For example, the criteria used to assign a trustmark, and the way in which compliance is verified, must be transparent and effectively applied.

EU-level. Self-regulatory initiatives should, preferably, target the entire EU, and should provide bilingual or multilingual information to foster cross-border confidence.

10. Conclusions

1. As is the case with many other complex issues on the Internet, there is no silver bullet in internet regulation. The digital and cross-border nature of the Internet challenges many of the assumptions underlying traditional regulation, in particular the jurisdictional reach of a country and the possibility to enforce measures.

2. Self-regulation is not a new answer to these challenges, and has actually been part of the Internet since its early conception, although it has not been the sole form of regulation on the Internet. There are several examples where self-regulation has flourished in specific areas, but even more examples where self-regulation has proved to be largely unsuccessful. Hence, self-regulation is still in the learning curve, and there is obvious room for improvement of each characteristic.

3. Self-regulation on the Internet is mainly a bottom-up procedure, where private parties take the initiative to address specific needs. However, states also participate in the creation of self-regulatory rules, either by creating the general background legal framework, by providing financial sponsoring, practical or legal guidance, or other assistance. Self-regulation and state legislation do not merely co-exist: they often complement each other and are intertwined, whereby self-regulation can "plug into" the more general rules set forth by state law.

4. Self-regulation has been recognised as a recommended approach by the European Commission, the Member States. Moreover, it is already recommended by various legal instruments that apply to the online environment, including the eCommerce Directive, the Copyright Directive, the Data Protection Directive and the Audiovisual Media Services Directive.

5. From a legal point of view, the basic framework is already available for most areas where self-regulation can be beneficial. Although the legal framework is available, the actual implementation is often still problematic, particularly in the area of participation, enforcement and proper governance of self-regulatory organisations.

11. Recommendations

240 Office of Fair Trading, p. 30
241 R. DE BRUIN et al, o.c., p. 7
242 R. DE BRUIN et al, o.c., p. 9
243 M. BONNICI, o.c., p. 2
244 M. BONNICI, o.c., p. 216
245 Ibid.
11.1. Supporting self-regulatory initiatives

Both the European Commission and the Member States have supported various self-regulatory initiatives, through financial assistance, assistance with the drafting and enforcement of codes of conduct, training of staff members, promotion of self-regulatory initiatives, etc. As self-regulatory initiatives can be very useful policy tools, we think such support is strongly recommended, and should in fact be further strengthened.

In order to foster the uptake of self-regulatory initiatives, streamline the drafting process and create uniformity between industry players, it could be envisaged to create EU-level self-regulation "templates", in which sound governance principles (such as transparency, accountability and involvement of all stakeholders) are embedded, which are legally compliant and also reflect best practices, as outlined in this section 11. These templates can then be used to efficiently build up EU-wide, national or sector-specific self-regulation initiatives.

11.2. Incorporation in technology

Similar to our recommendation regarding the (re-)launch of a privacy configurations in software\(^{246}\), we think it would be useful to integrate a service provider's compliance with trustmarks and codes of conducts in software. Such software should allow its users to configure his browser for trustmark compliance settings, and subsequently convey warnings when a service to be used is not in line with these predefined settings. Provided the software offers an attractive and user-friendly interface and apply the "lessons learned" from previous (failed) attempts, we think there is a realistic possibility that users and developers will use these features.

11.3. Increased use of standards

As pointed out in section 4.3 above, technical standards can be considered a type of self-regulation. In light of the disadvantages and limitations to self-regulation set out in section 6.2, one can indeed see remarkable similarities between self-regulation (in general) and technical standards. We therefore think it is useful to stimulate a convergence between self-regulation and standards.

**Parallels with standardisation** – Standardisation is a voluntary effort among industry, consumers and public authorities to develop consensus-based technical specifications in a certain domain. The EU has introduced a formal legal framework to support the EU-level standardisation process in certain areas. Three organisations (CEN, CENELEC and ETSI) are formally recognised, each with their own specific area of expertise, and are complemented by national standards bodies\(^{247}\).

The formal EU standardisation bodies have done a good job in the past and have generally reached their objectives, while respecting the principles of openness and neutrality\(^{248}\). However, several factors have come to undermine the standardisation monopoly of the formal EU standardisation bodies. In particular, the ICT sector has witnessed the rise of de facto standards\(^{249}\), i.e. the creation of hundreds of standardisation bodies outside the formal standardisation process, as well as the rise of non-formal ICT standardisation bodies with a global reach.

---

\(^{246}\) See section 8.2.1 of Chapter 4 - privacy and data protection

\(^{247}\) See Annex II to Directive 98/34/EC for a list of recognized National Standardisation Bodies

\(^{248}\) See consideration 24 of Directive 98/34/EC

\(^{249}\) H. SCHEPEL and J. FALKE, *Legal aspects of standardisation in the Member States of the EC and EFTA*, vol. 1, European Communities, 2000, p. 97
As a result, the know-how and technical expertise related to standardisation in the ICT domain is often more available in non-formal bodies than in the formal bodies. Although the formal standardisation bodies have tried to adapt themselves to these new initiatives, it cannot be denied that the standardisation centre of gravity has shifted. At the same time, the non-formal bodies are criticized for their lack of consumer involvement, the underrepresentation of SMEs and the reduced long-term maintenance of standards.

Future model of standardisation – Following the recommendations of a independent study, the European Commission now proposes to launch a high-level policy dialogue platform, where all standardisation stakeholders would be represented, and which would meet several times a year. This platform should then provide the European Commission with expert advice regarding matters concerning ICT standardisation policy and its implementation. The non-formal standardisation bodies would be integrated in the formal procedures. Although the European Commission recognises the importance of private fora and consortia, it worries that non-formal bodies may not offer sufficient guarantees of eligibility.

Link with self-regulation – Considering the striking similarities between standards and self-regulatory initiatives, with respect to both their advantages and disadvantages, we think it can be useful to investigate to which extent self-regulatory initiatives can be linked to standardisation efforts. Such link can, first, be that self-regulatory initiatives are adopted as formal standards, through the new standardisation procedures that are currently being developed by the European Commission. A second possibility would be to mirror some of the new governance structures, for adoption by self-regulatory initiatives.

---

250 Towards an increased contribution from standardisation to innovation in Europe, a.c., p. 5
252 ibid., p. 8
253 Open decision making process, based on collaborative and consensus-based activity, accessible to all stakeholders on a non-discriminatory basis, with all technical information being made available in a transparent way.
12. Recommended uses for self-regulation

Taking into account the success and failure criteria for self-regulation, we recommend the use of self-regulation in the following fields:

12.1. Traditional web shops

Traditional web shops, on which various products and services can be ordered, are the prototypical example of an area where self-regulation can flourish. Although there already exist various trustmarks for web shops in the Member States, these trustmarks are only used by a minority of we shops, and are generally limited to the national level (which does not increase trust for foreign consumers).

We recommend the creation of EU-level trustmarks and codes of conduct, in order to decrease the threshold for a consumer of one Member State to order products or services from a web shop in another Member State. However, all trustmarks must comply with the requirements set out in section 9.2, in particular the governance model, the cross-border nature, and the independence of the trustmark organisation.

Another interesting idea is the creation of trusted online malls, similar to the Japanese Rakuten example described in section 7.1.3 above.

12.1.2. Data protection issues

The internet presents numerous difficulties and complexities in the field of online privacy and data protection. We think that self-regulation can play an important role in the field of data protection, for example with respect to the following issues:

- **Content, style and presentation of privacy policies** – As outlined in the chapter on online data protection, we think that online service providers should be encouraged to draft multi-layered privacy policies, which provides clear and concise information on the use of personal data by the service provider. Taking into account that privacy policies are poorly drafted at this moment, it can be envisaged to develop templates on how privacy policies should be drafted. As these templates can vary between types of service providers (web shops, data storage services, online communities, ...), self-regulatory efforts may prove beneficial.

- **Standards should be developed for specific data protection tasks**, such as the right to access and correction, as well as information obligations. Standards should also be developed for storage terms (per industry sector or per category of personal data) and for data export formats.

- **Self-regulation can also deal with direct marketing and unsolicited commercial communications issues**, particularly for "grey areas", where it is not clear to which extent certain practices are allowed by data protection legislation. Such is, for example, the case with viral marketing initiatives, behavioural advertising and "tell-a-friend" systems.

---

254 See section 9 above


256 See section 7.2.1

257 When the right of data portability would be recognised.

Security – The Data Protection Directive requires data controllers to take security measures that are commensurate with the nature of the data, the costs and the associated risks. As the Directive does not impose any further guidelines or standards, we think there is an interesting opportunity for industry players to develop standards and/or undertake self-regulatory initiatives to provide guidance on which security measures are appropriate for specific online services.

12.1.3. Harmful content

As pointed out in section 7.1, the EU and several Member States have long recognised that the only real option for regulating harmful content is through self-regulation. These efforts should be maintained and further enhanced. The uptake of user rating and labelling systems should be encouraged, preferably on an EU-level or global level.

12.1.4. Social communities

Social communities have mushroomed over the last of couple of years. Children, teenagers and adults spend an increasing amount of their time on these communities.

However, social communities present many challenges, particularly in the field of data protection and child protection. As noted above, the European Commission has already taken initiatives in this regard with the Safer Social Networking Principles. Such initiatives should be encouraged. The effectiveness of self-regulatory initiatives should be monitored, so that social communities can further flourish without overly burdensome state regulation. Such state regulation may, however, become necessary when self-regulation would prove to be ineffective.

12.1.5. Services targeted at children and teenagers

Another area where self regulation can play an important role, is in online services that are targeted at children, teenagers or other target groups that require special protection. Self-regulation initiatives can, for example, provide guidance with respect to:

- age verification systems;
- age labelling systems (e.g., user rating systems such as PEGI);
- information requirements towards the target audience;
- "blacklisted" practices towards the target audience; and
- involvement of parents and guardians.

12.1.6. Online advertising

In light of the cross-border nature of the Internet, EU-level initiatives should be further developed to deal with online advertising, particularly in emerging markets such as targeted internet advertising.

---

259 Note that some Member States also resort to blocking (highly) illegal content at the level of internet access providers, as pointed out in Chapter 7 (net neutrality)

260 See also the keynote speech of EU commissioner M. KUNEVA on 31 March 2009 (SPEECH/09/156): "I invite industry to develop a framework that applies consumer policy principles and that will establish the principles of acceptable behaviour along the lines of what is being discussed today."
Although there already exists a set of international advertising guidelines (ICC code)\(^{261}\), a general pan-European code is not yet in effect. Instead, each Member State applies a set of national rules or principles, in accordance with its local culture, economy and society.

Similarly, there exist well-functioning self-regulatory advertising entities on a national level\(^{262}\), as well as a coordinating European Advertising Standards Alliance. However, these initiatives ultimately boil down to national interpretation and enforcement of rules, which can become cumbersome in real cross-border advertisements. Furthermore, not all of national self-regulatory entities already deal with internet advertising. Also, in some countries, advertising is subject to detailed legislation, to such an extent that the scope left for self-regulation is quite limited.

12.1.7. New technologies

Self-regulation is also recommended to deal with emerging technologies, in order to avoid over-regulation of such technologies in an early state.

This is, for example, the approach followed by the European Commission with respect to RFID. Few technologies have triggered such attention from consumer organisations as RFID devices, which are considered as the building blocks of a global “nervous system” that will make possible new types of applications combining information of the virtual world with a perception of the physical world. In the public debate, serious concerns have been expressed that RFID may endanger privacy, as it can be used to collect information that is linked to natural persons.

Yet, in its Communication of 15 March 2007\(^{263}\) and subsequent Communication of 15 February 2009\(^{264}\), it pointed to self-regulation as a means to regulate this new technology, and would not revert to traditional legislation, unless self-regulation would prove to be ineffective. We think this approach should receive approval, unless new technologies would present an immediate and acute danger to public concerns (such as consumer health). The Commission has recommended Member States to ensure that a framework for privacy and data protection is developed by all stakeholders, which should be submitted for endorsement to the Working Party 29.

12.1.8. Dispute resolution

Finally, online dispute resolution can also greatly benefit from self-regulatory initiatives. This is further discussed in Chapter II.9 (dispute resolution).

12.1.9. Copyright

As explained in Chapter 2 on digital content, Europe’s content sector is suffering from geographical fragmentation, so that parties must undertake costly negotiations to make digital content available online. Self-regulation and cross-industry agreements between industry players can help to maximise the circulation and exploitation of digital content rights\(^{265}\). Furthermore, the European Commission and the

\(^{261}\) E.g., the Consolidated ICC Code of Advertising and Marketing Communication Practice

\(^{262}\) E.g., the Jury d’Ethique Publicitaire in Belgium; the Deutscher Werberat in Germany; the Advertising Standards Authority in the UK; etc.

\(^{263}\) COM (2007) 96 final

\(^{264}\) C(2009) 3200 final on the implementation of privacy and data protection principles in applications supported by radio-frequency identification

Member States must encourage the creation of codes of conduct to address issues such as transparency and fairness of contractual terms. They could also act as an incentive for all stakeholders to voluntarily comply with contractual terms regarding digital content.