

Legal Risk Management in a Global, Electronic Marketplace

Jan Trzaskowski

1 Introduction	320
2 Cross-Border Law Enforcement	322
2.1 Sovereignty of States	323
2.2 Public Law Enforcement	323
2.3 Private Law Enforcement	326
2.4 Directing a Website	329
3 Objections to Cross-Border Law Enforcement	330
3.1 The Internal Market	330
3.2 Commercial Freedom of Expression	331
4 Risk Mitigation	332
4.1 Geographical Delimitation	332
4.1.1 Limitations in the Internal Market.....	334
4.2 Choice of Venue and Applicable Law	335
4.2.1 Choice of Venue	335
4.2.2 Choice of Applicable Law	336

This article discusses how businesses can manage the risk of cross-border law enforcement in connection to its Internet activities. A website is usually available in several jurisdictions and it is not possible to completely avoid the risk of infringing the law of those jurisdictions. In order to carry out legal risk management, the business needs to understand the risks involved and consider measures to handle the risk of cross-border law enforcement, including geographical delimitation and choice of venue and applicable law. This article focuses on the enforcement of unfair competition law.¹

It is found that 1) activities on the Internet are subject to geographical borders, and it is possible to identify factors that are relevant in assessing where activities on a website are directed, 2) private parties are better able to carry out traditional cross-border law enforcement than public authorities, 3) the freedom to provide goods and services in combination with the 2000 E-Commerce Directive restricts the possibilities of cross-border law enforcement, and 4) businesses can mitigate the risks of cross-border law enforcement by applying geographical delimitation and by entering into agreements on forum and applicable law.

¹ This article is based on the author's presentation at the Nordic School of Proactive Law's conference (12-14 June 2005) and the research presented in Trzaskowski, Jan, *Legal Risk Management in Electronic Commerce – Managing the Risk of Cross-Border Law Enforcement*, Ex Tuto Publishing, October 2005, www.legalriskmanagement.net.

1 Introduction

The Internet has made it substantially easier for businesses to reach a global marketplace, but commercial activities which influence different markets are not unlikely to become subject to the legal regime of those states. This article focuses on electronic commerce carried out on the Internet via a website on the World Wide Web. In the absence of globally accepted standards for geographical delimitation of content on the Internet,² the infringement of foreign law is a risk which businesses inevitable will run when carrying out electronic commerce. Compliance with the business's own national laws is rarely sufficient to avoid exposure to legal risks.³ Complying with law on a global basis is, if possible at all, expensive.

It has been suggested that the Internet should be recognised as a virtual world not regulated in a traditional, legal sense.⁴ It is obvious that activities on the Internet influence people, societies and markets in a very tangible way. The Internet is solely a medium which facilitates communication between individuals, but with an enormous potential.⁵ 'The prospect that a website owner might be haled into a courtroom in a far-off jurisdiction is much more than a mere academic exercise, it is a real possibility'⁶

A US study suggests that the risk of getting hauled into court is the biggest fear of companies operating online and that companies, particularly those situated in North America, seek to influence jurisdictional outcomes by using both technological and legal approaches to mitigate risk. The most common approaches were to either eliminate or reduce business activity in higher risk jurisdictions or to target specific jurisdictions that are perceived to be lower risk alternatives. The most commonly used approaches were technical access blocking (50 percent), user registration requirements self-identification, and password protection (40 percent). The most popular approaches to identify users were through user registration or self-identification.⁷

Risk management is usually understood as the process of measuring, or assessing risk and then developing strategies to manage the risk.⁸ Risk management concerns the protection of particular assets – in this case a business.

² See e.g. Vasiljeva, Ksenija, *1968 Brussels Convention and EU Council Regulation No 44/2001: Jurisdiction in Consumer Contracts Concluded Online*, European Law Journal, Volume 10 (January 2004), Issue 1, p. 123 at page 133f.

³ Geist, Michael A., *Is there a There There? Toward Greater Certainty for Internet Jurisdiction*, Berkeley Technology Journal, No. 16, 2002, p. 1345, p. 3.

⁴ Barlow, John Perry, *A Declaration of the Independence of Cyberspace*, 1996: 'Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather'.

⁵ See e.g. Haines, Avril D., *The Impact of the Internet on the judgments Project: Thoughts for the Future*, Hague Conference, Permanent Bureau, Preliminary document 17, February 2002, p. 5.

⁶ Geist, Michael A., *Is there a There There? Toward Greater Certainty for Internet Jurisdiction*, Berkeley Technology Journal, No. 16, 2002, p. 1345, p. 1.

⁷ *Global Internet Jurisdiction*, The ABA/ICC Survey, American Bar Association, Sub-Committee Chair: Professor Michael Geist, April 2004, pp. 2-3 and 14-15.

⁸ "en.wikipedia.org/wiki/Risk_management".

Legal risk management is not a well-established or well-defined concept, which like risk management in general is of a proactive nature.⁹ It is not the purpose of this article to define legal risk management, but rather to provide means to evaluate and manage a particular legal risk. In this context, the risk of being subject to foreign law and the possibilities in mitigating this risk.

In the research behind this article,¹⁰ an imaginary test set-up was created to provide a set of 'facts', upon which the law was examined. The approach was inspired by other areas of science, where experiments are carried to verify or falsify hypotheses. The idea is to maintain the focus of a standardised business ('the Business'). This approach was found helpful in defining the scope of the research, since a number of discussions were excluded by the definition of the test set-up. Through this approach, it was possible to maintain a rather broad scope, dealing in particular with both public and private international law as well as the laws of the Internal Market and more technical issues.

One of the aims of this approach was to examine and discuss the law from a business' point of view rather than providing a general presentation of the law on its own premisses. The approach is not that different from what is applied in the practice of the law, but instead of maintaining the focus of one client, this research intended to reach conclusions which are relevant for a number of businesses. This is in good harmony with the need for providing research which may be utilised in practice by businesses. The applied methodology leans against an economical 'realism', but the economical part was left to be pursued in later work.

The test set-up involves a business ('the Business') which is established in a state which is member of the European Union. It is assumed that the Business has no establishment or goods in other states than the state in which it is established.¹¹ The Business is carrying out electronic commerce on the Internet. The online activities consist of publishing marketing material and selling products (goods or services) to both businesses and consumers ('the User'). The use of the term 'foreign' (as in foreign courts and foreign law) refers to another state than the state in which the Business is established.

The Business is assumed to comply with the law of the state in which it is established. This means that it, in principle, is without interest if a foreign court applies the law of the state in which the business is established. There is in the Internal Market a substantial harmonisation of substantive law, which means that there to some extent in practice are limited difference between the laws of Member States in certain areas. See in particular the 1984 Misleading Advertising Directive,¹² the 1997 Distance Selling Directive,¹³ the 2000 E-Commerce

⁹ See e.g. Wahlgren, Peter, *Juridisk Riskanalys – Mot en säkrare juridisk metod*, 2003, Iversen, Jon, *Legal Risk Management*, Forlaget Thomson, 2005, and Keskitalo, Petri, *From Assumption to Risk Management*.

¹⁰ See Trzaskowski, Jan, *Legal Risk Management in Electronic Commerce – Managing the Risk of Cross-Border Law Enforcement*, 2005.

¹¹ If the Business would have valuables in other states, the risk of being sued there would in most cases be greater, since a judgment can be enforced by seizing the valuables there. See also Geist, Michael A., *Is there a There There? Toward Greater Certainty for Internet Jurisdiction*, Berkeley Technology Journal, No. 16, 2002, p. 1345 at II.

¹² Directive 84/450 (10 September 1984) concerning misleading and comparative advertising.

¹³ Directive 97/7 (20 May 1997) on the protection of consumers in respect of distance contracts.

Directive,¹⁴ and the 2005 Directive on Unfair Commercial Practices.¹⁵ It falls outside the scope to present and discuss this harmonised body of substantive law.

2 Cross-Border Law Enforcement

Cross-border law enforcement can be defined as the enforcement of the legislation of one state on a natural or legal person established in another state. From a state perspective, the question is to what extent it can enforce its legislation on persons who are residing in other states. From a business perspective, the interest in cross-border law enforcement can be formulated as to what extent the law of foreign states can be enforced on the Business and what the Business can do to mitigate or eliminate the risk of cross-border law enforcement.

Law enforcement concerns a variety of activities with a view to compelling observance of legal norms. By ‘enforcement’ is understood imposing sanctions on the infringer of a norm. ‘Law enforcement’ is the enforcement of ‘legal norms’, whereby is meant norms that can, at least in principle, be enforced through the Judiciary. Law enforcement that is carried out through the judiciary is labelled ‘traditional law enforcement’, whereas enforcement of law carried out in other ways is labelled ‘alternative law enforcement’. Alternative law enforcement can for example be carried out through the market (reputation) or by technical means. Law enforcement may be carried out by both public and private entities and is in this context denoted ‘public law enforcement’ and ‘private law enforcement’, respectively. Private entities are entities not exercising public powers. Private law enforcement may be carried out by a party with or without a contractual relationship with the Business.

Traditional cross-border law enforcement normally requires cooperation by the state in which the Business is established. Traditional law enforcement may be carried out 1) if the state, in which the business is established, recognises a foreign judgment, where foreign law is applied or 2) if the state in which the business is established applies foreign law. In more severe crimes, traditional cross-border law enforcement may also be carried out by means of extradition of the offender. Alternative law enforcement is enforcement by other means than those imposed by the judiciary. This could for example be by blocking a website, whereby the citizens of a state are denied access to certain content.¹⁶ Also enforcement through unfavourable commenting may be efficient in terms of imposing sanctions on a business. In this context, it is assumed that alternative law enforcement can be carried out without cooperation by the state in which the Business is established.

¹⁴ Directive 2000/31 (8 June 2000) on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

¹⁵ Directive 2005/29 (11 May 2005) concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council.

¹⁶ See e.g. Dornseif, Maximillian, *Government Mandated Blocking of Foreign Web Content*, “md.hudora.de” and Ramberg, Christina, *Internet Marketplaces, the Law of Auctions and Exchanges Online*, Oxford University Press, 2002, paragraph 2.05.

Taxonomy of law enforcement (examples)

	Traditional Law Enforcement (sanctions)	Alternative Law Enforcement (sanctions)
Public Law Enforcement Carried out by the public prosecutor and similar authorities exercising public powers.	Pecuniary penalties (fines) Custodial penalties (for example imprisonment) Injunctions	Unfavourable commenting Blocking content (injunctions)
Private Law Enforcement Carried out by private parties not exercising public powers, such as customers (including consumers), competitors, organisations (for example consumer and business organisations).	Contractual consequences (for example unenforceable contracts or damages in contract) Damages (in tort) Injunctions	

2.1 *Sovereignty of States*

States are sovereign to prescribe, adjudicate and enforce, as long as this sovereignty is exercised with due respect to the sovereignty of other states. States are not obliged to accept illegal activities affecting the state, just because they are carried out on the Internet.¹⁷ States may take various actions to regulate the Internet.¹⁸ Cross-border law enforcement is often cumbersome, if possible at all, and may only be carried out to the extent it does not violate the sovereignty of other states.

Traditional cross-border law enforcement requires some kind of involvement of and cooperation by the court of the state in which the Business is established. The Business may be sued in many courts, but in order to have judgments enforced against the Business, the rendering state must rely on the forthcoming of the state of the Business, possibly based on a particular agreement or other kinds of legal relation. There are a number of agreements concerning recognition of foreign judgment both within public and private law enforcement.

2.2 *Public Law Enforcement*

The principle of dual criminality ('double criminal liability') is fundamental in recognition of foreign criminal decisions. This principle provides that recognition only can be carried out if the underlying action is an offence in both the state entering the decision and the state in which recognition is sought. In this context, it is assumed that the Business is complying with the legislation of the state in which it is established. Thus, the dual criminality principle will not be satisfied and recognition of foreign criminal judgments is not likely to be carried out to the extent dual criminality is required.

¹⁷ 'A nation's right to control events within its territory and to protect its citizens permits it to regulate the local effects of extraterritorial acts'. Goldsmith, Jack L., *Against Cyberanarchy*, 65 *University of Chicago Law Review*, Fall, 1998, p. 1199 at IV-A.

¹⁸ See e.g. Ramberg, Christina, *Internet Marketplaces, the Law of Auctions and Exchanges Online*, Oxford University Press, 2002, paragraph 2.05 with references.

International law does not impose an obligation on states to apply foreign law,¹⁹ and states are not likely to apply foreign law in matters relating to public law enforcement.²⁰ The geographical scope of application of criminal law must be considered at a national level, and national standards on the scope of application varies from the restrictive principle of territory to more liberal principles allowing application of foreign criminal law.²¹ The country of origin principle in the 2000 E-Commerce Directive provides that each Member State shall ensure that the information society services provided by a service provider established on its territory comply with, in questions which fall within the coordinated field, the national provisions applicable in the Member State.²²

The country of origin principle applies to both public and private law requirements. It is clear from the provision that the state must apply national legislation, also in criminal and administrative matters, on a business established within its territory and within the scope of the country of origin principle. An obligation which applies regardless of where the activity is directed and no matter if the activity is illegal under the law of the state(s) where the activity is directed. The Country of origin principle does on the other hand not necessarily impose an obligation on foreign courts to apply the law of the state in which the Business is established.²³

A tendency of partially abandoning the principle of dual criminality is also found in acts adopted under Title VI (provisions on police and judicial cooperation in criminal matters) of the Treaty establishing the European Union. The first act under these provisions to depart from the principle of dual criminality is the 2002 Framework Decision on the European Arrest Warrant.²⁴ This approach is also pursued in the 2005 Framework Decision on Financial Penalties²⁵ which deals with mutual recognition of financial penalties in the European Union. The framework decision applies to final decisions, requiring a financial penalty to be paid by a natural or legal person, adopted either by a court or by an administrative authority.²⁶ It is emphasised in article 9(3) that a financial penalty imposed on a legal person is to be enforced even if the

¹⁹ See Akehurst, Michael, *Jurisdiction in International Law*, The British Year Book of International Law 1972-73, University Press, Oxford, p. 145 at p. 218f.

²⁰ Hörnle, Julia, *The European Union Takes Initiative in the Field of E-Commerce*, JILT 2000 (3), p. 333 at p. 354.

²¹ Dietrich Oehler in Bassiouni, M. Cherif, *International Criminal Law*, Second Edition, vol 2, Transnational Publishers Inc., 1999, p. 609f.

²² Directive 2000/31 (8 June 2000) on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, article 3(1).

²³ It follows from article 3(2) that Member States may not restrict the freedom to provide information society services from another Member State. This implies that the state may be barred from applying its own law, but not that it is obliged to apply foreign law.

²⁴ Council Framework Decision 2002/584 (13 June 2002) on the European arrest warrant and the surrender procedures between Member States. See also the Council Framework Decision 2003/577/JHA (22 July 2003) on the execution in the European Union of orders freezing property or evidence.

²⁵ Council Framework Decision 2005/214 (24 February 2005) on the application of the principle of mutual recognition to financial penalties.

²⁶ See article 1(a) and Green paper on the approximation, mutual recognition and enforcement of criminal sanctions in the European Union, COM(2004)334 (30 April 2004), p. 23.

executing state does not recognise the principle of criminal liability of legal persons.²⁷

The framework decision departs the principle of dual criminality for a number of offences listed in article 5(1). The law of the issuing state is to be applied to determine whether the act in question falls under one of the categories listed in article 5(1). The list in article 5(1) includes in particular fraud, computer-related crime, racism and xenophobia, illicit trafficking in cultural goods, swindling, racketeering and extortion, counterfeiting and piracy of products, forgery of administrative documents and trafficking therein, illicit trafficking in hormonal substances and other growth promoters, infringements of intellectual property rights and offences established by the issuing state and serving the purpose of implementing obligations arising from instruments adopted under the EC Treaty or under Title VI of the EU Treaty.²⁸

Article 7 provides a list of possible grounds for non-recognition or non-execution which may be invoked by the competent authority. It is clear from the list that the defendant's failure to appear cannot be invoked if the defendant was properly informed.²⁹ An important ground for non-recognition and non-execution is if the decision relates to acts which are regarded by the law of the executing state as having been committed in whole or in part in the territory of the executing state or in a place treated as such.³⁰ In the Danish implementation of the framework decision, it is made mandatory for Danish courts to refuse recognition if the act was committed in whole or in part on Danish territory, provided the act is not punishable under Danish law.³¹ It is most likely that the state in which the Business is established will consider the offence to have been committed, at least partially, in that state, which is also in accordance with the territoriality principle in international law. This means that an attempt of public cross-border law enforcement, as dealt with in this context and under this framework decision, in most cases will leave the possibility of non-recognition under the framework decision.

Another approach to cross-border law enforcement in the Internal Market is provided in the 1998 Injunctions Directive³² which is to ensure that qualified entities may bring proceedings (litigation capacity) before national courts requiring the cessation or prohibition of any act contrary to particular directives

²⁷ Article 6.

²⁸ The mentioned offences do not cover all of the exhaustively listed offences in article 5(1). According to article 5(2), the Council may decide to add other categories of offences at any time, acting unanimously after consultation of the European Parliament under the conditions laid down in article 39(1) of the EU Treaty. The Council is to consider, in the light of the report submitted to it pursuant to article 20(5), whether the list should be extended or amended.

²⁹ 2005 Framework Decision on Financial Penalties, article 7(2)(g)(ii).

³⁰ 2005 Framework Decision on Financial Penalties, article 7(2)(d)(a).

³¹ L 5 (som fremsat): Forslag til lov om fuldbyrdelse af visse strafferetlige afgørelser i Den Europæiske Union (fremsat den 6. oktober 2004), section 20(1)(2).

³² Directive 98/27 (19 May 1998) on injunctions for the protection of consumers' interests. See in general Peidro, L. Marín, Sotomayor, S. Feliu Álvarez De, Giménez, A. Ortega and Sanchez, L. Heredia, *Guide on Injunctions in the Electronic Commerce*, 7 March 2003, Title II.

listed in the annex of the directive.³³ The qualified entities may be either independent public bodies and/or (private) organisations whose purpose is to protect the interests of consumers.³⁴ The directive does, however, not determine the applicable law.³⁵ As mentioned above, it is unlikely that a state will apply foreign public law. Since most of the activities carried out by the Business fall under the coordinated field of the country of origin principle in the 2000 E-Commerce Directive, the courts of the state in which the Business is established is all the more not likely to apply foreign law. It should be emphasised that the choice of law in this context only concerns a harmonised area, and that differences only may occur when a Member State is utilising a minimum clause in one of the listed directives.

2.3 *Private Law Enforcement*

The possibilities in traditional cross-border law enforcement is better in civil and commercial matters than in criminal and administrative matters. This is mainly due to willingness to apply foreign law and the system of mutual recognition of judgments inherent in the Brussels/Lugano System.³⁶

By suing the Business in its home court, there are no problems with enforcement of the judgment, but it requires that that court is willing to apply foreign law in the dispute. This is most likely to happen in cases relating to tort and consumer contracts, whereas other contracts, under normal circumstances, will be treated under the law of the state in which the Business is established. In order to apply foreign law, the case must be linked to a foreign jurisdiction. That can be the case if the Business is actively pursuing marketing activities in other states and is entering contracts with users in those states.

According to the 1980 Rome Convention,³⁷ consumers are granted protection through a mandatory rule which designates the consumer's substantive law in 'certain consumer contracts'. It is a prerequisite for designating the consumer's law under article 5 of the 1980 Rome Convention that the contract concerns the supply of goods or services to a person ('the consumer') for a purpose which can be regarded as being outside his trade or profession, or a contract for the provision of credit for that object and 1) if in that country the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising, and he had taken in that country all the steps necessary on his part

³³ See also Koch, Harald, *Non-Class Group Litigation Under EU and German Law*, 11 Duke J. of Comp. & Int'l L., 2001, p. 355 at p. 356.

³⁴ 1998 Injunctions Directive, article 3.

³⁵ 1998 Injunctions Directive, article 2 (2).

³⁶ The main acts on recognition and enforcement of foreign judgments in Europe are the 2000 Brussels Regulation (Council regulation No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, 22 December 2000), the 1988 Lugano Convention (The EC and EFTA Lugano Convention on Jurisdiction and the Enforcement of judgments Civil and Commercial Matters, 16 September 1988) and the 1968 Brussels Convention (EC Convention on Jurisdiction and Enforcement of judgments in Civil and Commercial Matters, 27 September 1968).¹ These acts regulate both jurisdiction (choice of forum) and mutual recognition and enforcement of judgments.

³⁷ Convention on the Law Applicable to Contractual Obligations (consolidated version), opened for signature in Rome on 19 June 1980. Official Journal C 027, 26/01/1998 p. 0034 - 0046.

for the conclusion of the contract, or 2) if the other party or his agent received the consumer's order in that country.³⁸

It should be noted that the 1980 Rome Convention is to be applied even if the plaintiff is not established in a contracting state. In particular in certain consumer contracts, this means that the law of a foreign state may be applied even though that state is not part of the Internal Market. The homeward trend³⁹ may make it more likely that foreign law is not applied. Differences in law and culture may also make it more likely that foreign law is not applied, possibly with reference to public policy concerns. The same counts for applying foreign law in tort, where the state of the Business does not necessarily have a legal obligation to apply foreign law.

Tort claims may arise from a number of different legal areas, such as unfair competition, defamation and infringement of intellectual property rights. The 1980 Rome Convention does not apply to tort cases. Only a few Member States have codified their conflict of law rules concerning tort.⁴⁰ The dominant approach in Europe concerning choice of law in tort is the 'lex loci delicti commissi', which favours the law of the place where the act was committed.⁴¹ When determining the concrete criteria, according to which the place of the damage must be localised, most writers tend to favour seeking out the market which is affected by the unfair practices (lex injuriae).⁴²

There is in the European Union an ongoing work on a Rome II regulation, which is to approximate the choice of law in tort.⁴³ The proposed regulation confirms, with some exceptions, the lex loci delicti commissi for most non-contractual obligations. Article 3(1) provides that the law of the place where the direct damage arises or is likely to arise shall apply. This will in most cases correspond to the law of the injured party's country of residence. The proposed regulation comprises, in article 5, a specific clause on non-contractual obligations arising out

³⁸ See in general Trzaskowski, Jan, *Legal Risk Management in Electronic Commerce – Managing the Risk of Cross-Border Law Enforcement*, 2005, p. 120ff with references.

³⁹ In general, there has been detected a homeward trend which entails that national courts have a tendency to apply the law of the forum (lex fori). See e.g. López-Rodríguez, Ana, *Lex Mercatoria*, Retsvidenskabeligt Tidsskrift, 2002, p. 46, at p. 51, Lookofsky, Joseph, *International Privatret på Formuerettens Område*, 3. udgave, Jurist- og Økonomforbundets Forlag, 2004, p. 13f. and Nielsen, Peter Arnt, *International Privat- og Procesret*, Jurist- og Økonomforbundets forlag, 1997, p. 96 ('the lex fori tendency').

⁴⁰ Proposal for a Regulation of the European Parliament and the Council on the law Applicable to Non-Contractual Obligations ('Rome II'), COM(2003) 427 (22 July 2003), p. 5.

⁴¹ Lookofsky, Joseph and Hertz, Ketilbjørn, *Transnational Litigation and Commercial Arbitration*, second edition, Juris Publishing and DJØF Publications Copenhagen, 2004, p. 466f. See p. 471ff for a number of cases under European national law. See also Kronke, Herbert, *Applicable Law in Torts and Contracts in Cyberspace, Internet Which Court Decides? Which Law Applies?*, Law and Electronic Commerce, Volume 5, Kluwer Law International, 1998, p. 65 at p. 67ff.

⁴² Note on Conflicts of Laws on the Question of Unfair Competition: Background and Updated, drawn up by the Permanent Bureau, Preliminary Document No. 5, April 2000, p. 21 with references.

⁴³ Proposal for a regulation of the European Parliament and the Council on the law applicable to non-contractual obligations ('Rome II'), COM(2003)427 (22. July 2003). See also Lookofsky, Joseph and Hertz, Ketilbjørn, *Transnational Litigation and Commercial Arbitration*, second edition, Juris Publishing and DJØF Publications Copenhagen, 2004, p. 463ff.

of an act of unfair competition. In such cases the law of the country where competitive relations or the collective interests of consumers are directly and substantially affected shall, as a starting point, apply. Any law specified by the proposed regulation must be applied whether or not it is the law of a Member State.⁴⁴

The Business also runs the risk of being sued abroad. Recognition and enforcement of foreign judgment within private law enforcement is secured through the Brussels/Lugano System, which provides a principle of free movement of judgments within civil and commercial matters between, and with some exceptions, the EU Member States, Iceland, Norway and Switzerland. Foreign law is, as accounted for immediately above, likely to be applied in connection to tort and consumer contracts. In these situations, the Business may also be sued in a foreign court. It should be mentioned that substantial inconvenience and costs may occur in situations where the Business is sued in a foreign court, even though the law of the Business is applied.

Article 5(3) of the 2000 Brussels Regulation, the 1968 Brussels Convention and the 1988 Lugano Convention provides that a person domiciled in a Member State / contracting state may be sued in matters relating to tort, delict or quasi-delict in another Member State / contracting state in the courts for the place where the harmful event occurred [or may occur]. Article 5(3) applies also to jurisdiction in matters relating to unfair commercial practices ('unfair competition').⁴⁵

In the *Karl Heinz Henkel* case,⁴⁶ it was established that a non-profit-making, Austrian-based consumer organisation, *Verein für Konsumenteninformation*, could use article 5(3) of the 1968 Brussels Convention to seek an injunction against a German national's business activity carried out from Germany on the Austrian market. The UK government argued that the consumer protection organisation must be regarded as a public authority and its right to obtain an injunction to prevent the use of unfair terms in contracts constitutes a public law power. The court found that not only was the consumer protection organisation in question a private body, but in addition, the subject matter of the main proceedings was not an exercise of public powers, since the proceedings did not in any way concern the exercise of powers derogating from the rules of law applicable to relations between private individuals. The court concluded that an action of that kind was a civil matter within the meaning of the 1968 Brussels Convention. This decision provides private consumer organisations with better possibilities to exercise cross-border law enforcement than corresponding public authorities have.

The 2000 Brussels Regulation provides for the consumer forum in matters relating to a contract concluded by a person ('the consumer') for a purpose which can be regarded as being outside his trade or profession if the contract concerns a sale on credit or if the contract was concluded with a person who

⁴⁴ Proposal for a Regulation of the European Parliament and the Council on the law Applicable to Non-Contractual Obligations ('Rome II'), COM(2003) 427 (22 July 2003), article 2.

⁴⁵ See Mankowski, Peter, *Jurisdiction and Enforcement in the Information Society*, Nielsen, Ruth, Jacobsen, Søren Sandfeld and Trzaskowski, Jan (editors), *EU Electronic Commerce Law*, DJØF Publishing, 2004, p. 124 at p. 153ff.

⁴⁶ *Verein für Konsumenteninformation vs. Karl Heinz Henkel*, Case 167/00 (1 October 2002).

pursues commercial or professional activities in the state of the consumer's domicile or, by any means, directs such activities to that state, and the contract falls within the scope of such activities. The consumer definition and the inclusion of contract concerning sale on credit is the same as in the 1968 Brussels Convention and the 1988 Lugano Convention. These conventions furthermore include by article 13(1)(3) contracts which 1) in the state of the consumer's domicile were preceded by a specific invitation addressed to him or by advertising and 2) provided the consumer took the steps necessary for the conclusion of the contract in that state.

Under ancillary proceedings, it is possible to include civil claims under criminal proceedings. According to article 5(4) of the acts constituting the Brussels/Lugano System, a person may be sued, in civil claims for damages or restitution, in the court seized of criminal proceedings which are based on an act giving rise to criminal proceedings and provided that the court has jurisdiction under its own law to entertain civil proceedings. A civil claim can thus always be brought, whatever the domicile of the defendant, in the criminal court having jurisdiction to entertain the criminal proceedings even if the place where the court sits is not the same as where the harmful event occurred.⁴⁷ This is of particular interest in connection to tort claims added under criminal proceedings in connection to the infringement of for example unfair competition law.

In the *Krombach* case,⁴⁸ a German national was, before a French court, found guilty of violence resulting in involuntary manslaughter. The act had taken place in Germany, but the French courts declared that it had jurisdiction by virtue of the fact that the victim was a French national. The European Court of Justice established in connection with the enforcement in Germany of the civil compensation awarded to the bereaved, that the court of the state in which enforcement is sought cannot take account for the purposes of the public policy clause in article 27 of the 1968 Brussels Convention, of the fact that jurisdiction was based on the nationality of the victim of an offence.⁴⁹ This makes it clear that the access to objection is limited, even though the (criminal) jurisdiction is based on a principle, which would be deemed exorbitant if used in civil proceedings.

2.4 *Directing a Website*

Traditional cross-border law enforcement is most likely to be carried out in connection to tort, certain consumer contract and fines. In order to carry out traditional cross-border law enforcement in these situations, the Business' activities must have some effect in the state from where enforcement is carried out. A website is by default accessible in all states connected to the Internet, but access is normally not sufficient for the Business to be met with cross-border law enforcement. It is a requirement for entertaining jurisdiction under international law that there is a genuine link between the activity and the state exercising jurisdiction.⁵⁰

⁴⁷ Jenard Report on Convention and Protocol, C59/1979, p. 26.

⁴⁸ *Dieter Krombach v. André Bamberski*, Case 7/98 (28 March 2000).

⁴⁹ *Dieter Krombach v. André Bamberski*, Case 7/98 (28 March 2000), paragraph 34.

⁵⁰ Brownlie, Ian, *Principles of Public International Law*, Sixth Edition, Oxford University Press, 2003, p. 305 with references.

From case law, concerning whereto a website activity is directed,⁵¹ it seems that a number of connecting factors can be identified, i.e. 1) access to the website, 2) magnitude and nature of business activity, 3) the presentation and relevance of the website, 4) marketing measures and 5) the place of business and technical infrastructure. These factors do not provide a complete check-list, and it should be emphasised that the court is most likely to attach importance to the economical reality of the activity.

The mentioned factors provide an indication of relevant factors to examine when one has to determine the connection to a particular state of an activity carried out through a website. It should be emphasised that different law suits may require different degrees of connection.⁵² In tort cases for example, it seems reasonable to expect that the risk of cross-border law enforcement is directly proportional to the amount of harm which occurs in the state in question. In connection to a contract, the circumstances leading to the conclusion of the contract and the obligations under the contract may be more important.

3 Objections to Cross-Border Law Enforcement

If the Business is met with cross-border law enforcement, the Business may to some extent invoke that it is incompatible with the principles of the Internal Market or those concerning freedom of speech.⁵³

3.1 *The Internal Market*

The provisions on free movement of goods and services concern all restrictions which are capable of hindering, directly or indirectly, actually or potentially, intra-community trade. Restrictions may be both legal requirements and other means of restriction such as unfavourable commenting or the blocking of access to the Business' website. Restrictions may be justified if they are necessary ('proportionality') for securing mandatory requirements, which include public policy and the protection of consumers. If an area is harmonised by Community law, it is as a starting point not possible to justify restrictions. The application of a law foreign to the Business is likely to be a restriction either under the provisions on the free movement of goods and services or under the country of origin principle. It is not the application of foreign law itself which is a restriction, but rather the consequences of the concrete application of foreign law.

The European Court of Justice has attached importance to the effectiveness of the medium in question when it assess restrictions. The Internet is of particular importance to achieving the goals of the Internal Market.⁵⁴ This is also the

⁵¹ See in General Trzaskowski, Jan, *Legal Risk Management in Electronic Commerce – Managing the Risk of Cross-Border Law Enforcement*, 2005, p. 168ff with references.

⁵² See *1-800 Flowers Inc v. Phonenames LTD*, UK Supreme Court of Judicature, Court of Appeal (Civil Division), paragraphs 136-138.

⁵³ See in General Trzaskowski, Jan, *Legal Risk Management in Electronic Commerce – Managing the Risk of Cross-Border Law Enforcement*, 2005, chapter 2 with references.

⁵⁴ *Deutscher Apothekerverband eV and 0800 DocMorris NV, Jacques Waterval*, Case 322/01 (11 December 2003), paragraph 74.

political rationale behind the country of origin principle in the 2000 E-Commerce Directive. This principle adds a layer on top of the free movement of goods and services, for those activities that are carried out online. The access to impose restrictions under the 2000 E-Commerce Directive is more limited than under the provisions on free movement of goods and services.

As an objection to cross-border law enforcement, the Business may invoke that the action, taken by a law enforcer within the Internal Market, is a restriction in contravention of the free movement of goods, services and/or information society services. The country of origin principle for information society services in the 2000 E-Commerce Directive adds another test of justification on top of the freedom to provide goods and services. The access to impose restrictions under the 2000 E-Commerce Directive is more limited than under the provisions on free movement of goods and services. These principles apply to both traditional and alternative law enforcement as well as private and public law enforcement.

Certain selling arrangements fall outside the scope of the free movement of goods, provided that those provisions apply to all relevant traders operating within the national territory, and so long as they affect in the same manner, in law and in fact, the marketing of domestic products and of those from other Member States. If a ban on certain advertisement prevents foreign operators from gaining access to a market, the requirements under certain selling arrangements are not met. The country of origin principle of the 2000 E-Commerce Directive applies, however, to restrictions on information society services, which are considered as falling under certain selling arrangements.

A state cannot circumvent the provisions of the EC Treaty by derogating its powers to a private entity. Powerful collective actors, such as organisations, are also limited under these provisions. It is unclear to what extent private natural or legal persons are limited in their activities. The national courts are part of the state, and are obliged, also in private disputes, to observe Community legislation. Member States are further required to control its nationals and thus ensure that private entities are not tampering the functioning of the Internal Market.⁵⁵ To the extent private parties are restricted in carrying out cross-border law enforcement, they may rely on the possible justifications under mandatory requirements.

3.2 Commercial Freedom of Expression

The Business may also rely on the principles of freedom of expression as widely recognised and in particular expressed in the 1950 European Convention on Human Rights. There exists a 'commercial freedom of expression', but this right is not as protect-worthy as for example political expressions.⁵⁶ The case law on this matter shows that states retain a quite broad margin of appreciation in regulating and restriction commercial expressions. The freedom of expression is more likely to be successfully invoked by law enforcers who are criticising the

⁵⁵ See Eugen Schmidberger, *Internationale Transporte und Planzüge v. Republik Österreich*, Case 112/00 (12 June 2003) with references.

⁵⁶ See in particular European Court of Human Rights, *Markt Intern Verlag GmbH and Klaus Beermann* (20 November 1989),

Business as a means of alternative law enforcement as long as it is carried out in a general interest. The 1950 Convention on Human Rights has been ratified by a number of states which are not part of the Internal Market. If the Business is met with restrictions from those states, it may be able to invoke the freedom of expression against such restrictions.

4 Risk Mitigation

In order for the Business to avoid cross-border law enforcement, it may apply risk-mitigation measures. This article focuses on geographical delimitation and the choice of forum and applicable law, but the Business may also adjust its website based on the connecting factors mentioned above.

4.1 Geographical Delimitation

The Internet is a borderless environment.⁵⁷ This means that it, as a starting point, is possible to access information on a website from each and every connected computer, independent of where in the world that computer might be situated.⁵⁸ Geographical delimitation covers the possibility of excluding users from certain states. The focus is mainly on technical delimitation, which is geographical delimitation carried out through technological means as elaborated on below.⁵⁹ It seems common to assess this question in the light of an overall impression of the website. Accepting this approach, it is difficult to provide clear-cut answers to the effectiveness as a means of avoiding particular markets.

It seems reasonable to assume that there is some kind of direct proportionality between users' access to a website and cross-border law enforcement from the state of the users. By employing technical measures, it is possible to limit the legal risk by targeting only particular states.⁶⁰ It has on the other hand been argued that the only way to secure the Internet by technological means may be to build a parallel public international network that focuses on existing sovereignties.⁶¹

Geographical delimitation by technological means ('geo-targeting') enables the Business to reject users from certain jurisdictions. Geo-targeting is not perfect and it is not possible to determine the location of all users. The

⁵⁷ See in general Svantesson, Dan Jerker B., *The Characteristics Making Internet Communication Challenge Traditional Models of Regulation - What Every International Jurist Should Know About the Internet*, International Journal of Law and Technology, Vol 13, No. 1, Oxford University Press, 2005, p. 44ff.

⁵⁸ See Maunsbach, Ulf, *Some Reflexions Concerning Jurisdiction in Cases on Cross-Border Trademark Infringements Through the Internet*, Scandinavian Studies in Law, Vol. 47 ('IT Law'), Stockholm 2004, p. 493 at p. 496.

⁵⁹ See in general Svantesson, Dan Jerker B., *Geo-Location Technologies and Other Means of Placing Borders on the 'Borderless' Internet*, The John Marshall Journal of Computer & Information Law, Fall 2004, p. 101.

⁶⁰ Manolopoulos, Andreas, *Raising 'Cyber-Borders': The Interaction Between Law and Technology*, International Journal of Law and Information Technology, Vol. 11, No. 1, 2003, p. 40 at p. 57.

⁶¹ Spang-Hanssen, Henrik, *Cyberspace & International Law on Jurisdiction*, DJØF Publishing, 2004, p. 531.

application of geo-targeting to carry out geographical delimitation does, however, indicate that the Business is not directing its activities to the states excluded. Other measures of geographical delimitation, such as for example stating the targeted states may also count in the examination of whereto the website activity is directed. It is decisive whether the measure is effective and in particular whether it reflects a genuine interest in avoiding the particular jurisdictions.

The Business can achieve more efficient delimitation if the geo-targeting is combined with asking the User to reveal his identity. In the French Yahoo! case,⁶² experts considered that it would be desirable to ask surfers whose IP address is ambiguous to make a declaration of nationality. The experts did not find that it could be reasonably claimed that such an approach would have a negative impact on the performance and response time of the server hosting the Yahoo! auctions service. The experts concluded that with the combination of geographical identification of the IP address and such a declaration of nationality, it would be possible to achieve a filtering success rate approaching 90 percent, but it has been argued that the identification of the country of the user can be determined with 95% accuracy.⁶³

In connection to the Yahoo! case,⁶⁴ it was noted that 1) the tribunal demonstrated the principal of how technology may be used to make law effective and 2) that although the tribunal's solution was not able to filter approximately 20% of targeted users, it reflected the truism that no law is 100% efficient.⁶⁵

In the case of *Twentieth Century Fox Film Corporation v. iCraveTV*,⁶⁶ it was found that a requirement of typing a Canadian zip-code was not sufficient to avoid infringing US law in connection to the streaming of copyrighted programs. The typing of the zip-code was combined with the requirement of clicking on an 'In Canada' icon (instead of clicking the 'Not in Canada' icon) and agreeing to terms of use including another confirmation of the user being located in Canada. The activity was directed towards Canadian users, but there was nothing barring US users from typing in a Canadian zip-code. It has been emphasised that iCraveTV's Canadian zip-code was posted on the site.⁶⁷ The injunction could probably not be enforced in Canada,⁶⁸ and it should be emphasised that the case

⁶² See interim Court Order 00/05308 (20 November 2000), The County Court of Paris. Based on English translation posted at www.cdt.org/speech/international/001120yahoofrance.pdf.

⁶³ See Spang-Hanssen, Henrik, *Cyberspace & International Law on Jurisdiction*, DJØF Publishing, 2004, p. 333.

⁶⁴ See interim Court Order 00/05308 (20 November 2000), The County Court of Paris. Based on English translation posted at www.cdt.org/speech/international/001120yahoofrance.pdf.

⁶⁵ The legal implications of the Yahoo! Inc nazi memorabilia dispute: an interview with Professor Yves Poulet, January/March 2001, www.juriscom.net/en/uni/doc/yahoo/poulet.htm.

⁶⁶ 2000 U.S. Dist. LEXIS 11670; 53 U.S.P.Q.2D (BNA) 1831; Copy. L. Rep. (CCH) P28,030 (8 February 2000). See also Geist, Michael A., *Is there a There There? Toward Greater Certainty for Internet Jurisdiction*, Berkeley Technology Journal, No. 16, 2002, p. 1345 at I-B.

⁶⁷ Geist, Michael A., *Is there a There There? Toward Greater Certainty for Internet Jurisdiction*, Berkeley Technology Journal, No. 16, 2002, p. 1345 at I-B.

⁶⁸ See Spang-Hanssen, Henrik, *Cyberspace & International Law on Jurisdiction*, DJØF Publishing, 2004, p. 478ff.

concerned copyright which protects concerns other than those involved with unfair competition law.

4.1.1 Limitations in the Internal Market

Article 12 of the EC Treaty provides that any discrimination on grounds of nationality is prohibited. The focus is on whether it is compatible with the rules of the Internal Market for the Business to adopt measures which discriminate between users from different Member States.⁶⁹ The application of geographical delimitation may constitute, directly or indirectly, discrimination on the ground of nationality. It is not clear whether the prohibition on discrimination applies to private businesses. It is assumed that the Business discriminate in order to avoid cross-border law enforcement or as a consequence of strategic business-decisions. The discrimination may concern access to the Business's website in general or access to certain features such as in particular the buying of offered products. This article does not deal with competition law, under which such discrimination under certain circumstances can constitute breach of the EC Treaty provisions on that matter.⁷⁰

It was suggested by the Economic and Social Committee that businesses should be able to restrict their marketing activities to certain countries by actively informing consumers.⁷¹ It has, on the other hand, been noted that restricting marketing activities on a website to certain countries is a clear discrimination between consumers according to their place of residence which is inconsistent with the principles of common market and free movement of goods and services.⁷²

As mentioned above, Member States do have an obligation to control its national, and to the extent private parties are bound by provisions of the EC Treaty, they may also rely on possible justifications of such measures. If the geographical delimitation is, as assumed in the test set-up, carried out as part of a commercial strategy and the reason is to avoid infringing the law of particular states. In the case, *Familiapress v. Heinrich Bauer Verlag*,⁷³ the European Court of Justice seems to accept discrimination by denying, based on domicile, certain users' access to certain features of a product in order to comply with the legal order of the state whereto activities are directed. It should be emphasised that the case law on this matter does not provide a clear-cut answer to this question.

It is not clear to what extent article 12 of the EC Treaty prohibits the Business from applying geographical delimitation. It seems to be justifiable to carry out geographical delimitation if it is done as part of a general business strategy and in order to avoid certain legal risks. This also corresponds with the proposed

⁶⁹ See in general Cruz, Julio Baquero, *Free Movement and Private Autonomy*, European Law Review, volume 24, no. 6, December 1999, p. 603.

⁷⁰ See in general Oliver, Peter, *Free Movement of Goods in the European Union*, Fourth Edition, Sweet and Maxwell, 2003, paragraph 4.26.

⁷¹ Opinion of the Economic and Social Committee on the 'Proposal for a Council Regulation (EC) on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters', OJ C 117 (26 April 2000), p. 10.

⁷² Vasiljeva, Ksenija, *1968 Brussels Convention and EU Council Regulation No 44/2001: Jurisdiction in Consumer Contracts Concluded Online*, European Law Journal, Volume 10 (January 2004), Issue 1, p. 123 at page 132.

⁷³ *Vereinigte Familiapress Zeitungsverlags- und vertriebs GmbH v. Heinrich Bauer Verlag*, Case 368/95 (26 June 1997).

service directive,⁷⁴ which provides that conditions of access may be justified by objective criteria, including extra risks linked to rules differing from those of the Member State of origin.

The country of origin principle limits the risks of cross-border law enforcement, and it may be used as an argument against justification of discrimination, in particular when the Business is not entering contracts with consumers. But the country of origin principle does notably not provide full harmonisation. The country of origin principle of the 2000 E-Commerce Directive has limited the amount of legal risks, but notably not eliminated the risk of being met with legal requirements under foreign law.

4.2 Choice of Venue and Applicable Law

Parties to a contract may as a starting point choose both forum and applicable law (parties' autonomy). This is clear from both the 1980 Rome Convention and the acts constituting the Brussels/Lugano System. It should be noted that the party autonomy is a concept within private law which allow private parties to designate the proper forum and applicable law. Such an agreement will, as a starting point, only have effect upon the User who is subject to the terms presented by the Business. It will in particular not bind other parties, including in particular competitors, private organisations and public authorities insofar as they are not acting as users of the website. Agreements on choice of forum and applicable law do not influence the possibilities in cross-border law enforcement in situations outside of contractual relations. The access to benefit from clauses on choice of forum and applicable law is limited in connection to certain consumer contracts.

4.2.1 Choice of Venue

The choice of applicable law must be determined in accordance with the national choice of law rules of the state in which the court is located. Due to the homeward-trend, the risk of applying a law which is foreign to the Business may be greater when the Business is being sued in a foreign court of law, and the costs and inconvenience is also likely to be higher when litigating before a foreign court. For those reasons the Business may be interested in entering a choice of forum agreement with the User.

It follows from article 17(1) of the 1968 Brussels Convention and the 1988 Lugano Convention that if the parties, one or more of whom are domiciled in a contracting state, have agreed that a court or the courts of a contracting state are to have jurisdiction to settle any disputes which have arisen or which may arise in connection with a particular legal relationship, that court or those courts shall have exclusive jurisdiction. In the corresponding article in the 2000 Brussels Regulation,⁷⁵ it is provided that the jurisdiction is exclusive unless the parties have agreed otherwise. This enables the parties to agree that the jurisdiction is not exclusive.⁷⁶

⁷⁴ See Proposal for a Directive of the European Parliament and of the Council on services in the internal market, Working document of the Luxembourg Presidency, containing clarifications to the Commission's proposal, Interinstitutional File: 2004/2001 (COD) (10 January 2005).

⁷⁵ 2000 Brussels Regulation, article 23(1).

⁷⁶ This additional flexibility is warranted by the need to respect the autonomous will of the

A choice of forum clause under article 17 must be either a) in writing or evidenced in writing, b) in a form which accords with practices which the parties have established between themselves, or c) in international trade or commerce, in a form which accords with a usage of which the parties are or ought to have been aware and which in such trade or commerce is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade or commerce concerned.⁷⁷ The requirements must be strictly interpreted in so far as that article excludes both jurisdiction as determined by the general principle of the defendant's courts laid down in article 2 and the special jurisdictions provided for in articles 5 and 6.⁷⁸

The access to enter an agreement on choice of forum is limited in connection to the specific provisions on certain consumer contracts. These provisions may be departed from only by an agreement: 1) which is entered into after the dispute has arisen, or 2) which allows the consumer to bring proceedings in courts other than those indicated in the section on certain consumer contracts, or 3) which is entered into by the consumer and the other party to the contract, both of whom are at the time of conclusion of the contract domiciled or habitually resident in the same Member State / contracting state, and which confers jurisdiction on the courts of that state, provided that such an agreement is not contrary to the law of that state.⁷⁹ There is no benefit for the Business to provide the consumer with more places to sue the Business.

4.2.2 Choice of Applicable Law

The starting point in the 1980 Rome Convention is that a contract is to be governed by the law chosen by the parties. This principle is recognised in the private international law of most states.⁸⁰ It follows from article 3(1) of the 1980 Rome Convention that the choice must be expressed or demonstrated with reasonable certainty by the terms of the contract or the circumstances of the case.⁸¹ There must be no doubt that it was the parties' intention that the contract should be governed by that particular law, and the examination is still subject to other terms of the contract and the circumstances of the case.⁸²

There are certain limitations when it comes to choice of law in certain consumer contracts. Article 5(2) of the 1980 Rome Convention provides that a choice of law made by the parties in such a contract must not have the result of depriving the consumer of the protection afforded to him by the mandatory

parties. See proposal for a Council Regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, COM(1999) 348 (15 July 1999), p. 18.

⁷⁷ See in general Mankowski, Peter, *Jurisdiction and Enforcement in the Information Society*, Nielsen, Ruth, Jacobsen, Søren Sandfeld and Trzaskowski, Jan (editors), *EU Electronic Commerce Law*, DJØF Publishing, 2004, p. 124 at p. 132ff.

⁷⁸ *Mainschiffahrts-Genossenschaft eG (MSG) v. Les Gravières Rhénanes SARL*. Case 106/95 (20 February 1997), paragraph 14 with references.

⁷⁹ Article 15 of the 1968 Brussels Convention and the 1988 Lugano Convention, and article 17 of the 2000 Brussels Regulation.

⁸⁰ Giuliano-Lagarde Report, Official Journal C 282 1980, p. 1 at p. 15.

⁸¹ See in general Lookofsky, Joseph and Hertz, Ketilbjørn, *Transnational Litigation and Commercial Arbitration*, second edition, Juris Publishing and DJØF Publications Copenhagen, 2004, p. 399ff.

⁸² Giuliano-Lagarde Report, p. 15.

rules⁸³ of the law of the country in which he has his habitual residence. The reference is not to international mandatory rules, as concerned in article 7, and the provision embodies the principle that a choice of law in a consumer contract cannot deprive the consumer of the protection afforded to him by the law of the country in which he has his habitual residence.⁸⁴ The formal validity of such a contract is governed by the law of the country in which the consumer has his habitual residence.⁸⁵

⁸³ Rules which cannot be deviated from by contract.

⁸⁴ Giuliano-Lagarde Report, p. 23.

⁸⁵ 1980 Rome Convention, article 9(5).