IMPLEMENTATION OF INTERNAL MARKET LEGISLATION RELEVANT TO THE INFORMATION SOCIETY: A SNAPSHOT OF THE CURRENT REGIME IN THE EFTA-EEA STATES[1]

Einar Hannesson [2]
The EFTA Surveillance Authority

Abstract:

The internal market of the European Union has coordinated various policies which are relevant to the Information Society among the 25 EU Member States. But the EU has also made a far reaching third dimensional trade agreement, extending the scope of the internal market outside borders of the EU. By the Agreement on the European Economic Area the three EFTA States, Iceland, Norway and Liechtenstein have become part of the internal market. This entails that EU law in the fields of electronic commerce, electronic communications, information society services and data protection, to name a few, has not only been coordinated among the EU 25 Member States, but also the EEA 28 States. For the purpose of these policies, the EFTA EEA States are not regarded as third countries by the EU. However, there are peculiarities to the legal effects of the EEA and both pillars are facing several common challenges in the fields of the Information Society.

I.0 THE EEA AGREEMENT AND IMPLEMENTATION CONTROL WITHIN THE TWO PILLARS

In 1992, the then seven EFTA states [3] and the 12 EC Member States and the European Community signed an Agreement [4] whose aim is to promote a continuous and balanced strengthening of trade and economic relations between the Contracting Parties with equal conditions of competition, and the respect of the same rules, with a view to create a homogeneous European Economic Area (hereinafter 'the EEA')[5]. In order to attain the objectives, the EEA shall entail free movement of goods, persons, services and capital. Furthermore, the same rules on competition and a closer cooperation in other fields apply, such as research and development, the environment, education and social policy.

Less than a year after its entry into force on January 1, 1994, the three EFTA States, Sweden, Finland and Austria, had joined the EU. The Swiss rejected EU membership in a national referendum leaving only Norway, Iceland and Liechtenstein on the EFTA side. Regardless of the growing imbalance in the size of the two pillars, it does entail that the internal

---

[1] The views expressed in this Article are only the personal view of the author and do not necessarily reflect the opinion of the EFTA Surveillance Authority. The article was first published in Complex 3/06 LSPI Conference Proceeding.

[2] Einar Hannesson is an officer in the Internal Market Affairs Directorate of the EFTA Surveillance Authority in Brussels. In his capacity, he is responsible for monitoring implementation of the internal market legislation in the fields of Information Society, Electronic Communications, Postal Services and Maritime Transport into the respective legal orders of Norway, Iceland and Liechtenstein.

[3] European Free Trade Association (EFTA) is an intergovernmental organization promoting free trade and strengthening economic relations. EFTA's Member States are Iceland, Liechtenstein, Norway and Switzerland.

[4] Agreement on the European Economic Area - Final Act - Joint Declarations - Declarations by the Governments of the Member States of the Community and the EFTA States - Arrangements - Agreed Minutes - Declarations by one or several of the Contracting Parties of the Agreement on the European Economic Area Official Journal L 001 , 03/01/1994 P. 0003 - 0036

[5] See, Article 1 of the Agreement on the European Economic Area.

market of the EU is relevant not only to the 28 EEA states but also the 25 EU Member States. The EEA Agreement is the closest and most extensive trade agreement the two trade blocks have ratified to date and the European Court of Justice (hereinafter 'the ECJ') has confirmed in its jurisprudence[6] that when the Agreement contains provisions comparable to the Treaty, the EFTA EEA States should not be considered as third countries by the EU Member States and the European Union[7].

The EEA Agreement has a rather complicated institutional structure which sustains two pillars, on the one hand the EU, and on the other hand, a mirrored EFTA EEA institutional structure with a decision making procedures, surveillance authority and a Court.

The EEA Agreement requires the EFTA States to establish procedures similar to those existing in the Community, including procedures for ensuring the fulfilment of obligations under the EEA Agreement. It further provides that the fulfilment of the obligations under the Agreement should be monitored by, on one hand, the EFTA Surveillance Authority and, on the other, the European Commission. To this end, the EFTA Contracting Parties to the EEA Agreement signed the Agreement on the establishment of a Surveillance Authority and a Court of Justice (the Surveillance and Court Agreement[8]). Thus, the Surveillance and Court Agreement, *inter alia*, lays down the internal organization of the EFTA Surveillance Authority (hereinafter 'the Authority') and its competences.

The main task of the Authority is to ensure that EEA rules are properly enacted and applied by the EFTA EEA States. These rules include the general principles for the free movement of goods, persons, services and capital, cover fields such as foodstuffs, veterinary and phytosanitary matters, energy, intellectual property rights, the environment, mutual recognition of diplomas, social security, consumer protection, financial services and transport. Specific rules apply to trade in fish and in processed agricultural products.

In general, the EFTA EEA States are obliged to notify the Authority of their transposition of EEA provisions into national law. Where an EFTA State fails to comply with EEA law, the Authority has powers to attempt to bring the infringement to an end and may, where necessary, refer the case to the EFTA Court. The legal basis for the Authority's actions for non-compliance is, in particular, Article 31 of the Surveillance and Court Agreement. That provision is intended to give the Authority the same powers as the Commission has under Article 226 of the EC Treaty.

The Authority takes whatever action it deems appropriate in response to possible infringement by EFTA States of their EEA obligations arising either from a complaint (complaint cases) or from another source, which it detects (own initiative cases). Infringement means failure by an EFTA State to fulfil its obligations under EEA law. This may consist either of an action or an omission. The term "State" means the EFTA EEA State that infringes EEA law, irrespective of the national authority - central, regional or local - to which the action or omission is attributable.

---

[6] See, Case C-452/01, Judgment of the Court of Justice of 23 September 2003, Margarethe Ospelt v Schlössle Weissenberg Familienstiftung, [2003] ECRp.I-09743.

[7] See, Case C-452/01, Margarethe Ospelt v Schlössle Weissenberg Familienstiftung, "The Court ruled: '1. Rules such as those of the Vorarlberger Grundverkehrsgesetz (Vorarlberg Land Transfer Law) of 23 September 1993, as amended, making transactions relating to agricultural and forestry plots subject to administrative controls must, where a transaction is in issue between nationals of States party to the Agreement on the European Economic Area of 2 May 1992, be assessed in the light of Article 40 of and Annex XII to the aforementioned Agreement, which are provisions possessing the same legal scope as that of Article 73b of the EC Treaty (now Article 56 EC), which is identical in substance".

[8] The Agreement between the EFTA States on the Establishment of a Surveillance Authority and a Court of Justice ("Surveillance and Court Agreement") (OJ No L 344, 31.12.1994, p.1), adjusted by the Protocol Adjusting the Agreement between the EFTA States on the Establishment of a Surveillance Authority and a Court of Justice signed in Brussels on 17 March 1993 ("Surveillance and Court Adjusting Protocol") and subsequently by the Agreement Adjusting certain Agreements between the EFTA States signed in Brussels on 29 December 1994 ("Adjusting Agreement").

Although EEA Law has many similarities in substance with Community Law, various differences persist, primarily related to the legal effect of EEA Acts in the national legal order of the EFTA EEA states. These differences relate to the aim of the EFTA States at the time of creation of the EEA Agreement, which is not to transfer national sovereignty to supra national institutions. Therefore, EEA Acts do not have supremacy over national rules, nor a direct effect, unlike Community law. National courts of the EFTA EEA States are not obliged to refer issues related to the EEA Agreement to the EFTA Court for advisory opinions, unlike the obligation of national Courts in the EU, in certain situation, to seek preliminary rulings from the Court of Justice.

Still, the application of EEA law has many similarities with Community law. Protocol 35 of the EEA Agreement on the implementation of the EEA rules contains a provision which states that in cases of possible conflicts between implemented EEA rules and other statutory provisions, the EFTA States undertake to introduce a statutory provision to the effect that EEA rules prevail. This is at least an attempt to introduce supremacy to EEA law. The existence of EEA law pre-empts the possibilities of the EFTA EEA states to adopt a national legislation diverging from EEA Acts in the field. It is now an established case law by the EFTA Court, which has been confirmed by national courts in the EFTA EEA States, that non-implementation of EEA Acts, or a wrongful implementation of such acts, can result in state liability in a similar way as a breach of EU law within an EU Member State. Courts can ask for an advisory opinion which is a parallel procedure to preliminary rulings. Finally, the powers of the Authority to enforce EEA Acts within the EFTA EEA States are parallel to the role of the Commission as regard implementation of Community law into the EU Member States.

2.0 RELEVANT ACTS OF THE EEA AGREEMENT WITH CONCERN JURISDICTION, SECURITY AND DATA PROTECTION IN IT

EEA rules relevant to Legal, Security and Privacy issues in IT are generally derived from Article 36 of the EEA Agreement on the free movement of Services. This provision refers to Annexes IX to XI in the Agreement. Annex XI, Telecommunications Services, has the bulk of the internal market directives, regulations and decisions concerning Telecommunications, Data Protection and Information Services. These are acts which require implementation into the internal legal order of the EFTA EEA states. It also contains various soft law measures in the field. Protocol 31 of the EEA Agreement on cooperation in specific fields outside the four freedoms contains several provisions concerning interchange of data and information security. Article 2 has a reference to several Community Acts which are relevant to Information Services and security of information systems and Article 17 to telematic interchange of data between administrations (IDA). These acts usually do not require further implementation effort into the integral legal order, but the EFTA EEA states are participating in the work and are providing financial support to these programs. This is extensive legal framework and, therefore, what will follow, is just a brief discussion of the most relevant issues to the Information Society within the EFTA EEA States.

2.1. Electronic Commerce, Signatures, Communications and Network Security

Legislation relevant to the Information Society forms part of the internal market, including Directives 2000/31/EC on electronic commerce[9], 1999/93/EC[10] on electronic signatures[11] and

[9] See, Joint Committee Decision No 91/2000 (OJ No L 7, 11.1.2001, p. 13 and EEA Supplement No. 2, 11.1.2001, p. 8) e.i.f. 1.6.2001.

[10] See, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, p. 12).

[11] See, Joint Committee Decision No 66/2000 (OJ No L 250, 5.10.2000, p. 48 and EEA Supplement No 44, 5.10.2000, p.2), e.i.f. 1.3.2001.

various acts related to network security, including Regulation (EC) No 460/2004 on the establishment of European Network and Information Security Agency[12].

A Electronic Commerce

The challenges being faced with the emergence of the Internet and electronic commerce revealed the need for a coordinated approach by the EU, which was eventually reached with Directive 2000/31/EC on electronic commerce[13]. The Directive, which was incorporated into the EEA Agreement on October 27, 2000[14], seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.

i. Jurisdiction and the choice of Law in electronic transactions

The Directive contemplates on at least three different stakeholders in electronic commerce: the service provider, the consumer or recipient of service, and the intermediary service provider that enables the communications between the two parties. Finally, it coordinates certain legal aspects between the Member States and the role of national regulation.

When the eCommerce Directive was being drafted, intense discussions took place as to where jurisdiction for consumer protection should be located, and whether it should contain provisions stipulating jurisdiction over service providers in general. In the end, it turned out that it should not establish additional rules on private international law, nor should it deal with the jurisdiction of Courts. The general legal framework concerning jurisdiction is therefore not determined in the Directive but in several inter-European conventions on Private International Law.

The 1968 Brussels Convention[15] laid down a body of rules serving to determine which national court would have jurisdiction in the event of an international dispute and the 1980 Rome Convention [16] harmonized the Member States' private international law rules regarding contractual obligations and the choice of law. In the case referred to in Article 4 of the Convention:

> "a contract is governed by the law of the country of habitual residence of the party called upon to effect the performance characteristic of the contract or, if that party is an association or legal person, the country where it has its headquarters; furthermore, if the characteristic performance cannot be determined, the contract is governed by the law of the country with which it is most closely connected."

Special considerations apply to consumer contracts as is described in Article 5 of the Convention. If such contract has been concluded, the criteria set out in Articles 3 and 4 of the Convention apply, without prejudice to the protection afforded to the consumer by mandatory rules under the law of the country where the consumer had his habitual residence at the time of

[12] See, Joint Committee Decision No 103/2005 (OJ No L 306, 24.11.2005, p. 36 and EEA Supplement No 60, 24.11.2005, p. 23), e.i.f. 1.2.2006.

[13] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ L 178, 17.7.2000, p. 1)

[14] See, Joint Committee Decision No 91/2000 (OJ No L 7, 11.1.2001, p. 13 and EEA Supplement No. 2, 11.1.2001, p. 8) e.i.f. 1.6.2001.

[15] Later superseded by Council Regulation (EC) No 44/2001 of 22 December 2000, in force since 1 March 2002, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. The consolidated text of the 1968 Brussels Convention was published in OJ C 27, 26.1.1998, pp. 1-23. The Convention still applies, however, to relations between Denmark and the other Member States.

[16] Convention on the law applicable to contractual obligations opened for signature in Rome on 19 June 1980 (80/934/EEC), Official Journal L 266 , 09/10/1980 p. 0001 – 0019.

conclusion of the contract, provided that no blame can be attached to the consumer for the other party's ignorance, should that be the case, of the identity of that country. The habitual residence of the consumer in electronic commerce can therefore be the forum for legal dispute, despite contractual obligation stating otherwise. The EU is on its way to adopt a future instrument which will extend the rule to non-contractual obligations as well, specifying exactly what is covered by the concept of 'mandatory rules' in the light of the case law of the Court of Justice.[17]

Similarly, the Brussels Convention has granted consumers in the EU Member States the right to choose the forum in the country of their habitual residence and the EFTA EEA States have applied the same rule by becoming members to the Lugano Convention[18], a parallel to the Brussels convention. The EEA States should therefore have the same rules as regard jurisdiction of courts but, when it comes to the choice of law, the results could diverge because the Rome Convention is only binding the EU Member States.

While the United States abolished sales tax on Internet sale, the EU adopted international jurisdiction for collecting value added tax[19]. To this end, radio and television broadcasting services and electronically supplied services provided from third countries to persons established in the Community or from the Community to recipients established in third countries should be taxed at the place of the recipient of the services. These rules are not part of the EEA Agreement.

While jurisdiction and choice of law is not within the scope of Directive 2000/31/EC, it contains guidance as regard, a related issue, namely where service providers should be considered established. The place of establishment of a company providing services via an Internet website is not necessarily the place at which the technology supporting its website is located or the place at which its website is accessible, but the place where it pursues its economic activity. Further guidance is to be found in the case-law of the Court of Justice according to which the concept of establishment involves the actual pursuit of an economic activity through a fixed establishment for an indefinite period.

ii. Liability of the ISP's

In the late nineties, courts in some of the EU Member States made rulings against ISP's for material which was transmitted over their networks, without them necessarily being aware of its content[20]. The Directive on Electronic Commerce was the logical answer to these developments. When considering liability of intermediary service providers Articles 12, 13, 14 and 15 of the Directive are of most importance. The provisions divide between the following actions of the intermediary service providers, a mere conduit, caching and hosting services. The Articles provide for detailed conditions in each case which could relieve the ISP's from any liability for the content transmitted on their networks, but in short, it boils down to whether they have initiated the communications or modified its content in any way and had actual knowledge of illegal activity. A service provider who deliberately collaborates with one of the recipients of his

[17] The 'Rome II' instrument, which has now been drafted in the form of a proposal for a regulation on the law applicable to non-contractual obligations.

[18] See, 88/592/EEC: Convention on jurisdiction and the enforcement of judgments in civil and commercial matters – Done at Lugano 16 September 1988, Official Journal L 319, 25/11/1988, p. 9.

[19] See, Council Directive 2002/38/EC of 7 May 2002 amending and amending temporarily Directive 77/388/EEC as regards the value added tax arrangements applicable to radio and television broadcasting services and certain electronically supplied services.

[20] On May 28, 1998, in a closely watched international dispute, a former CompuServe official was convicted in Germany of violating local pornography laws. Felix Somm, who headed CompuServe Deutschland operations until he was indicted in 1997, was blamed for not blocking access to pornographic pictures that were available on the Internet. By convicting Mr. Somm, the court appears to be saying that Internet service providers in Germany are responsible for Internet content and must take affirmative steps to block access to objectionable material.

service in order to undertake illegal acts goes beyond the activities of "mere conduit" or "caching" and as a result cannot benefit from the liability exemptions established for these activities[21].

Article 15 is of particular importance, bearing in mind the conditions for non-liability for material transmitted over ISP's network:

> "1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.
>
> 2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements."

By the provision, EEA States are prevented from imposing a general obligation on intermediary service providers to monitor content being transmitted over their network, but such general obligation could endanger the very aim of the Directive to facilitate economic development on the internal market and be in breach with fundamental rights. Finally, a general monitoring of millions of sites and web pages would, in practical terms, be impossible and would result in disproportionate burdens on intermediaries and higher costs of access to basic services for users[22].

Some Member States have opted for transposing Article 15 of the Directive into national law, while others have decided not to. The reason for not transposing the provision has been defended by claiming that it is not intended to provide individuals and undertakings with clear and precise rights or obligations, but merely, preventing a state from introducing an general obligation to monitor. The non-existence of such obligation should therefore be considered sufficient to constitute compliance.

However, there could be difficulties with this approach, since there is a mounting pressure on ISP's to filter, e.g. copyright piracy, defamation, misleading advertising, unfair commercial practices, child pornography etc. In some EEA States, the penal code stipulates a liability for being in possession of illegal digital content, i.e. child pornography. These provisions could have the effect of imposing a general obligation to monitor, since intermediaries could be in violation of these national measures if they were in possession of illegal content, even without their knowledge thereof. This liability, albeit being limited under circumstances stipulated for in Articles 12, 13 and 14, is, nevertheless, a condition leading to a possible liability. Service providers relying solely on an exemption could therefore find themselves in violation with law for illegal content stored on their network or storage equipment. This situation could be an incentive to undertake general monitoring. The lack of Article 15 from the national measure implementing the Directive could therefore create legal uncertainty.

---

[21] See, preample 44 of the Ecommerce Directive.

[22] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee - First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) /* COM/2003/0702 final */

In the light of the incentive to undertake general monitoring, it should be considered whether, Article 15 should not at all times be transposed into the national measures[23]. To rely on interpretation of the Article in order to alter the textual interpretation of national measures is far from transparent and there is a reason to doubt that the legal position under national law is sufficiently precise and clear and that individuals are made fully aware of their rights.

iii. Notice and take down procedures

The Ecommerce Directive exempts ISP's from liability for content transmitted over their networks; however, that does not prevent the possibility of injunctions of a different kind; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it. In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities, has to act expeditiously to remove or to disable access to the information concerned.

Most of the EEA States have adopted some kind of Notice and Take down system to withdraw illegal information. But these systems are not without some qualifications since the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level. The Commission and the Authority ensure that these Notice and Take down systems comply with fundamental rights etc. The European Commission has recently established an expert group on electronic commerce [24] to facilitate exchange of information relevant to Article 19 of the Directive. Extremely few cases have been reported indicating that these procedures were not as urgent as anticipated.

B. Network Security within the EEA

There is a growing degree of attention in EEA law being focused on integrity of electronic communications. Acts concerning Information Security have been part of the EEA since the beginning; however, the form of this cooperation changed with the establishment of a new Community Agency, the European Network and Information Security Agency[25] (ENISA). This agency aims to enhance the capability of the Community, the Member States and the business community and to prevent, address and to respond to network and information security problems. Furthermore, it aims to assist the Commission in its work related to Information Security. Regulation (EC) No 460/2004 introducing the Agency has been incorporated into the EEA Agreement and a specific adaptation text[26] explains how it should be read in EFTA EEA context to include the EFTA States and their public entities. The Agency shall assist the Authority or the Standing Committee, as the case may be, in the performance of their respective tasks.

---

[23] It is a settled case-law, in relation to the transposition of directives into the legal order of a Member State, that it is essential that the national legislation in question effectively ensures that the directive is fully applied, that the legal position under national law is sufficiently precise and clear and that individuals are made fully aware of their rights (Case C-365/93 Commission v Greece [1995] ECR I-499, paragraph 9, Case C-144/99 Commission v Netherlands [2001] ECR I-3541, paragraph 17, and Case C-97/01 Commission v Grand Duchy of Luxembourg [2003] ECR I-05797).

[24] See, Commission Decision of 24 October 2005 establishing an expert group on electronic commerce (2005/752/EC).

[25] See, Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) Official Journal L 077 , 13/03/2004 P. 0001 - 0011 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

[26] See, Joint Committee Decision No 103/2005 (OJ No L 306, 24.11.2005, p. 36 and EEA Supplement No 60, 24.11.2005, p. 23), e.i.f. 1.2.2006.

The EFTA EEA States shall participate fully in the Management Board and shall within it have the same rights and obligations as EU Member States, except for the right to vote. They shall have the same right to access documents, and they contribute to the Agency as the EU Member States. Nationals of the EFTA EEA States enjoying their full rights as citizens may be engaged under contract by the Executive Director of the Agency in the same way as nationals of the EU Member States and the EFTA EEA States apply to the Agency and to its staff the Protocol on the Privileges and Immunities of the European Communities.

2.2. Electronic Communications

Electronic Communications, previously known as Telecommunications, is a part of the EEA and the new electronic communications framework, consisting of Directives 2002/19/EC [27], 2002/20/EC[28], 2002/21/EC[29] and 2002/22/EC[30] has entered into force. At the time of entry into force in the European Communities in July 24, 2003, Iceland and Norway had already aligned their national legislation to the framework; however, its incorporation into the EEA was delayed due to Liechtenstein's inability to lift constitutional requirements[31]. In November 2004, it was adopted and, by December, infringement proceedings had been initiated against Liechtenstein for not implementing the Electronic Communications framework on time.

The new regulatory framework requires much more involvement of the Authority into national communications markets than previous regime. Article 7 of the Framework Directive 2002/21/EC as the core instrument require national regulatory authorities (the NRA's) to notify their draft decisions to the Authority in a number of specified instances before they can enter into force. The Authority, as regards the EFTA EEA States, can, like the Commission towards the EU Member States, veto some of these decisions of the NRA's.

2.3 Privacy in IT

Data protection within the internal market has been harmonized and is part of the EEA[32]. This regulatory framework sustains of the Data Protection Directive 95/46/EC [33] and several Commission decisions which are base on it. A special adaptation text was adopted at the time of incorporation of the Data Protection Directive, stating that Commission decisions pursuant to Article 31 of the Directive, concerning e.g. transfer of data to third countries should apply temporarily as regards the EFTA EEA states without regard to pending incorporation of those Acts into the Agreement, provided that the EFTA EEA states would not decide otherwise and

[27] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) Official Journal L 108 , 24/04/2002 P. 0033 - 0050 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

[28] Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) Official Journal L 108 , 24/04/2002 P. 0021 - 0032 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

[29] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) Official Journal L 108 , 24/04/2002 P. 0033 - 0050 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

[30] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) Official Journal L 108 , 24/04/2002 P. 0051 - 0077 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

[31] See, Article 103 EEA.

[32] See, Joint Committee Decision No 83/1999 (OJ No L 296, 23.11.2000, p. 41 and EEA Supplement No 43, 23.11.2000, p. 112 (I) and p. 81 Del 2 (N)), e.i.f. 1.7.2000.

[33] See, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

inform the Commission accordingly[34]. Decisions of the Commission are therefore binding upon the EFTA EEA states at the same time as the EU Member States.

a. The implication of fundamental rights for the interpretation of the Data Protection Directive 95/46/EC

The ECJ has adopted the approach when interpreting the Data Protection Directive to apply a minimum standard based on the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter 'the Convention'). A typical assessment of whether certain practices are in compliance with the Directive would therefore be to, first, assess whether it is in compliance with Article 8 of the Convention. If a practice is unable pass the test, it should be unable to be justified by overriding justifications pursuant to Community law. However, if practice would not be a breach of the Convention, the Data Protection Directive could still provide for a higher degree of protection.

The Data Protection Directive refers in its preamble to the Convention on more than one occasion. Furthermore, it should be added that Article 6(2) of the Treaty on the European Union (hereinafter 'TEU') states that the Union shall respect fundamental rights, as guaranteed by the Convention and as they result from the constitutional traditions common to the Member States, as general principles of Community law. The ECJ is of the opinion that Article 6(2) TEU only

[34] See the adaptation text in the Joint Committee Decision stating: "The provisions of the Directive shall, for the purposes of the present Agreement, be read with the following adaptations:
(a) The Contracting Parties shall, within the framework of the EEA Joint Committee, exchange the information to which reference is made in Articles 25(3) and 26(3) first paragraph;
(b) If, pursuant to Articles 25(4), 25(6), 26(3) second paragraph or 26(4), the Commission intends to adopt measures in accordance with Article 31, the EFTA States shall be informed in the same way as the EU Member States. If the Commission communicates measures to the Council in accordance with Article 31, the EFTA States shall be kept informed in due time of such a procedure. Any measures adopted in accordance with Article 31 shall be notified to the EFTA States in the same way as to the EU Member States. Pending a decision by the EEA Joint Committee to incorporate such measures into the Agreement,
the EFTA States shall decide, and inform the Commission before the entry into force of the measures adopted in accordance with Article 31, whether they will apply these measures or not.
If an EFTA State has not taken any such decision, it shall apply the measures adopted in accordance with Article 31 at the same time as EU Member States.
If an agreement on the incorporation into the EEA Agreement of measures adopted in accordance with Article 31 cannot be reached in the EEA Joint Committee within twelve months after the entry into force of the measures, an EFTA State may discontinue any application of such measures and shall inform the Commission thereof without delay.
The other Contracting Parties shall, by derogation from Article 1(2) of the Directive, restrict or prohibit the free flow of personal data to an EFTA State which does not apply the measures adopted in accordance with Article 31 in the same way as these measures prevent the transfer of such data to a third country;
(c) Notwithstanding any negotiations by the Commission pursuant to Article 25(5), an EFTA State may enter into negotiations on its own behalf. The Commission and the EFTA States shall keep each other informed and, upon request, shall hold consultations regarding such negotiations within the framework of the EEA Joint Committee;
Procedures for the association of Liechtenstein, Iceland and Norway in accordance with Article 101 of the Agreement:
Each EFTA State may, in accordance with the second subparagraph of Article 29(2) of Directive 95/46/EC of the European Parliament and of the Council, appoint one person, who shall represent the supervisory authority or authorities designated by each EFTA State to participate as observer, without the right to vote, in the meetings of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data.
The EC Commission shall in due time inform the participants of the dates of the meetings of the Working Party and shall transmit to them the relevant information."

restates what has previously been confirmed by the Court, c.f. the *Österreichischer Rundfunk*[35] judgment:

> "It should also be noted that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures (see, *inter alia*, Case C-274/99 P *Connolly* v *Commission* [2001] ECR I-1611, paragraph 37).
>
> Those principles have been expressly restated in Article 6(2) [T] EU, which states that [t]he Union shall respect fundamental rights, as guaranteed by the [Convention] and as they result from the constitutional traditions common to the Member States, as general principles of Community law."[36]

The EEA Agreement does not have a provision identical to Article 6(2) TEU, but states in its first preamble that the contracting parties were "convinced of the contribution that an EEA would bring to the construction of a Europe based on peace, democracy and human rights." The EFTA-Court has relied on the Convention in several cases[37]. Judgment of the EFTA Court in Case E-2/03, the public prosecutor against Asgeir Logi Asgeirsson, Axel Petur Asgersson and Helgi Mar Reynisson of December 12, 2003[38] provides the clearest proof:

> "The Court adds that it has found on earlier occasions that provisions of the EEA Agreement as well as procedural provisions of the Surveillance and Court Agreement are to be interpreted in the light of fundamental rights (see to that extent, Case E-8/97 *TV 1000 Sverige* v *Norway* [1998] EFTA Ct. Rep. 68, at paragraph 26; Case E-2/02 *Technologien Bau- und Wirtschaftsberatung and Bellona* v *EFTA Surveillance Authority*, judgment of 19 June 2003, not yet reported, at paragraph 37). The provisions of the European Convention of Human Rights and the judgments of the European Court of Human Rights are important sources for determining the scope of these rights."

---

[35] See, joint Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others*, [2003] ECR I-0000.

[36] See, joint Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others*, [2003] ECR I-0000, paragraph 68-69.

[37] See, Summary of the Court "Legal framework, case law, and composition - 1994-2003" which states: "The Court of Justice of the European Communities has a longstanding tradition of referring to the European Human Rights Convention and to judgments of the European Court of Human Rights in cases involving fundamental rights (see, for instance, Cases 44/79 Hauer v Rheinland-Pfalz, 1979 ECR, 3727; 63/83 Regina v Kent Kirk, 1984 ECR, 2689; 222/84 Johnston v Chief Constable of the RUC, 1986 ECR, 1651).
The EFTA Court has followed suit in Case E-8/97 TV 1000 Sverige AB v The Norwegian Government, 1998 EFTA Court Report, 68. The Court interpreted the transmitting state principle underlying Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, regulation, or administrative action in Member States concerning the pursuit of television broadcasting activities and referred to the freedom of expression granted by Article 10 ECHR as well as, with regard to the limitations of that freedom, to the landmark ruling of the European Court of Human Rights in the Handyside case (judgment of 7 December 1976, A, vol. 24)." http://www.eftacourt.lu/pdf/LegalFW_CaseLaw_Comp_2004_Inhalt.pdf.

[38] See, Judgment of the EFTA Court in Case E-2/03, the public prosecutor against Asgeir Logi Asgeirsson, Axel Petur Asgersson and Helgi Mar Reynisson of 12 December 2003, paragraph 23.

The line of reasoning used by the ECJ should therefore be applied in the EFTA/EEA context as well despite considerable difference in legal basis. The data protection Directive and the corresponding decisions should therefore be construed for the purposes of the EEA context in the light of the Convention.

b. Privacy and third countries.

Article 25 of the Data Protection Directive states that the Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if the third country in question ensures an adequate level of protection. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

Data Protection issues could restrict operations of service providers in third countries since severe restrictions limit legitimate transfer of personal data to third countries other than those which ensure adequate level of protection[39]. While there are admittedly several derogations permitted from the rule,[40] it is still causing a restrictive factor for third country service providers; consequently, this could be a restrictive factor for ecommerce. As has been stated earlier, EFTA EEA states are not considered third countries by the EU, within fields covered by the EEA Agreement.

In *Bodil Lindquist*[41] it was not considered to be transfer of data to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loaded personal data onto an Internet page which were stored with his hosting provider which were established in that State or in another Member State, thereby making those data accessible to anyone who connects to the Internet, including people in a third country. The court discussed this in a lengthy reasoning with some qualifications and indicating that a different technical infrastructure of the hosting service provider could lead to another conclusion. By deciding this, ECJ took a practical view since the framework for transmission of data to third countries is far too cumbersome to accommodate the nature of the Internet. This could entail that if the data subject knowingly submits information to the controller, and the processing complies therefore with the Directive, it could be published online where everybody can access it, including third country citizens from a country which is not providing sufficient level of protection; however, this same information could not be transferred to the same third country in a traditional way on the basis of Article 25 of the Directive.

Bearing in mind the above mentioned and a recent judgment[42] by the European Court of Human Rights (hereinafter 'the ECHR-court') where it stated that; "*increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data"* [43], one wonders – with the ECJ, taking

[39] See, Article 25 of the Data Protection Directive.
[40] See, Article 26 of the Data Protection Directive.
[41] See, Case C-101/01 Bodil Lindquist, [2003] ECR p. I-12971.
[42] See, Case of *Von Hannover v. Germany* - 59320/00 [2004] ECHR 294 (24 June 2004), § 70.
[43] See, Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy, point 5, and, *mutatis mutandis*, *Amann v. Switzerland* [GC], no. 27798/95, § 65-67, ECHR 2000-II; *Rotaru v. Romania* [GC], no. 28341/95, § 43-44, ECHR 2000-V; *P.G. and J.H. v. the United Kingdom*, no. 44787/98, § 57-60, ECHR 2001-IX; and *Peck v. the United Kingdom*, no. 44647/98, §§ 59-63, and § 78, ECHR 2003-I.

pragmatic approach towards the Internet while the ECHR Court considers it require increased vigilance in privacy protection — whether the two courts are going separate ways. As has been discussed above, the view of the ECHR Court could have direct impact on data protection within the internal market since increased vigilance in interpretation of Article 8 of the Convention could render overriding justifications by the meaning of EEA law obsolete and sets the minimum threshold for interpretation of Data Protection in general.

c. Unsolicited Communications

The Ecommerce Directive Article 7 contains a provision on unsolicited commercial communications; however, it states in Article 1 that it shall not apply to questions relating to information society services covered by data protection[44]. Furthermore, Article 7, on unsolicited commercial communications, refers to the Distance Selling Directive 97/7/EC[45] and Directive 97/66/EC on Data Protection in Telecommunications[46] for further guidance. The latter Directive has now been repealed, but the new measure, currently in force, Article 13 of Directive 2002/58/EC on Data Protection in Electronic Communications[47] is the single most important provision in EEA law relevant to unsolicited commercial communications.

Following a growing concern because of excessive and increasing amount of Spam[48] the community measures have become stricter as the time goes. In the adoption of the Ecommerce Directive in 2000, the EU parliament pressed for severe restrictions on unsolicited communications; however, the EU settled with an opt-out register scheme, allowing Member States to permit unsolicited commercial communication by electronic mail, provided such mails where identifiable clearly and unambiguously as such as soon as it is received by the recipient. The tone had changed in Article 13 of Directive 2002/58/EC:

> "The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent."

Where electronic contact details for electronic mail are obtained from customers, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made,

---

[44] Directives 95/46/EC and 97/66/EC.

[45] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts - Statement by the Council and the Parliament re Article 6 (1) - Statement by the Commission re Article 3 (1), first indent Official Journal L 144 , 04/06/1997 P. 0019 - 0027 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

[46] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector Official Journal L 024 , 30/01/1998 P. 0001 - 0008 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

[47] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) Official Journal L 201 , 31/07/2002 P. 0037 - 0047 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

[48] Unsolicited communications.

or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

Several voluntary projects[49] assisting network administrators to block out illegal Spam are operated and these projects can be of support to national regulators in their law enforcement. Within the governmental sphere the most prominent pan-European project is likely the Contact Network of Spam Authorities (CNSA) which is co-coordinating the efforts to reduce spam and malware though European and international cooperation and by operating a complaint handling system. The EFTA EEA States participate in these networks. Fines have been imposed on spammers in relation to these investigations, however, the amount of spam is constantly increasing and its nature is changing to a criminal intent. One could therefore wonder whether the law is a realistic means to fight unsolicited communications, or whether such legal framework is actually restricting actions of law abiding citizens.

2.4. Intellectual Property Rights

The Treaty provides for the establishment of an internal market and the institution of a system ensuring that competition in the internal market is not distorted. Harmonization of the laws of the Member States on copyright and related rights contributes to the achievement of these objectives. With that in mind, Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society has been adopted by the EU and incorporated into the EEA Agreement[50].

The Directive is hardly though a full harmonization effort since it leaves intact a wide scope of issues to be dealt with nationally, including issues related to collective societies, rights management and the ability of rightholders of trade marks to segment markets internationally since their rights are exhausted within the EEA, and rightholders of copyrights which segment markets into national entities. This has limiting factor on competition. Without regard to the willingness of rightholders to restrict cross-border provision of their rights, it would still be a complicated undertaking to provide services internationally, since right management and collection of fees varies between each country. Copyright legislation within the EEA is therefore, more or less national, making cross-border service provision extremely difficult.

2.5. Draft technical regulation

The Transparency Directive 98/34/EC[51] as it has been amended by Directive 98/48/EC forms a part of the EEA Agreement.[52] The EFTA EEA States are therefore obliged to notify draft technical rules to the Authority in due time before adoption, e.g. within the fields of Information Society. Several draft regulations within the fields of Information Society Services are notified

[49] Inter alia the Spamhaus Project. It operates the SBL Blockinglist, which is a realtime database of IP addresses of verified spam sources (including spammers, spam gangs and spam support services), maintained by the Spamhaus Project team and supplied as a free service to help email administrators better manage incoming email streams. SBL Blocklists suggest that 80% of spam received by Internet Users in North America and Europe is sent by a group of under 200 entities, comprising some 500-600 professional spammers. Almost all of those are listed in ROKSO database which is a register of known hard-line spam operations that have been thrown off Internet Service Providers 3 times or more.

[50] See, Annex XVIII Intellectual Property, Joint Committee Decision No 110/2004 (OJ L 376, 23.12.2004, p. 45 and EEA Supplement No 65, 23.12.2004, p. 30), e.i.f. 1.8.2005.

[51] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations Official Journal L 204 , 21/07/1998 P. 0037 - 0048 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

[52] Heading and point inserted by Decision No 16/2001 (OJ L 117, 26.4.2001, p. 16 and EEA Supplement No 22, 26.4.2001, p.10), e.i.f. 1.3.2001.

annually by the EFTA EEA States since a failure to do so would results in inability to enforce that national measure against individuals[53].

3.0. ISSUES DE LEGE FERENDA

Irrelevance of rules related to the transfer of data to third countries

The Data Protection Directive 95/46/EC contains a detailed set of rules concerning transfer of data to third countries. These rules require a notification by the controller before data is transferred and can impose a significant administrative burden. As opposed to this set of rules applying to data transferred to third countries, downloading of personal data on the Internet does not fall under this set of rules. Such downloading - making that same information available to everyone on the World Wide Web - does not, therefore, constitute a transfer of data to third countries. This approach leaves many questions open since there is a good reason to restrict the flow of personal data, while at the same time it is unrealistic to apply the toolbox of the Data Protection Directive on the Internet. The rules do, therefore, need to be streamlined in order for such rules to be able to cope with reality of the Internet era.

Electronic Commerce and the habitual residence of the consumer

The Directive on Electronic Commerce does not contain any rules concerning the choice of forum in dispute between a service provider and a recipient of service. That relationship is. on the other hand, determined by the inter community Brussels and Rome Conventions as regards the EU Member States, and the Lugano Convention as regard the EFTA EEA States. These Conventions are complicated legal instruments, which have been subject to discordant interpretation of the various national systems[54]. For foreign service providers, it could be a strong incentive to stay away from the European markets if being faced with such set of rules where consumers not only can sue in their own country, but also rely on their national laws concerning consumer protection in that litigation as well. Furthermore, the global tax jurisdiction that the EU has imposed on value added taxes entail complications for electronic commerce. These apply in particular to the EU Member States since the EFTA EEA States are neither part of the Rome Convention, nor the VAT regime.

Fragmentation of markets for Intellectual Property rights

Internal market legislation related to Intellectual Property rights is highly fragmented between the 28 EEA States, making it difficult to provide such services across borders of national markets. European, and preferably international harmonization, of Intellectual Property rights, including rules on remuneration collected by national collective societies and allowing parallel import, could therefore promote service provision of knowledge-based-services on a much broader scale than is currently possible.

4.0. CONCLUSIONS

This Article has discussed how the internal market of the EU 25 Member States has been extended to the three EFTA EEA States, Iceland, Norway and Liechtenstein. This entails that individuals and economic undertakings can expect national legislation in the EEA to be based on the same Directives, Regulations, Decisions or any other *acquis communitaire* which is EEA relevant. This also entails that the competence of the national authorities to introduce a new

[53] See, Judgment of the Court of 30 April 1996, CIA Security International SA v Signalson SA and Securitel SPRL [1996] ECR p. I-02201.

[54] Report on the prospects for approximating civil procedural law in the European Union (COM (2002) 746 + COM (2002) 654 – C5-0201/2003 – 2003/2087(INI)) Committee on Legal Affairs and the Internal Market, A5-0041/2004, page 11.

legislation which diverge from EEA Law have been pre-empted in order to ensure a homogeneous internal market. The national legislation in these states should therefore have been harmonized.

Membership to the EU is however not the same as being party to the EEA Agreement. The scope of the EU is wider and contains the Justice and Home Affairs and Common Foreign and Security policy, in addition to the European Communities which is similar to the EEA Agreement.

There are also differences in the legal effects of Community law on the one hand and EEA law on the other. The EEA Agreement is not intended to transfer any of the EFTA states' sovereignty and therefore lacks direct effect and supremacy over national law etc. Neither have the EFTA EEA States transferred their foreign policy to supra-national organizations. In practice there are, however, some exemptions from that principle, like presumed compliance with Commission Decisions pursuant to Article 31 of the Data Protection Directive, despite them not having been incorporated into the EEA Agreement.

The Article has identified three obstacles hampering further development of Digital Knowledge-Based Economy. Consumer protection and taxes is one of the obstacles since Foreign Service providers could shy away from the European market due to potential high costs of complying with e.g. the Rome Convention. Intellectual Property rights are also causing fragmentation of the market despite Directive 2001/29/EC and the set of rules concerning transfer of data to third countries could be irrelevant, and still incur compliance costs.

References:

1. Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee - First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) /* COM/2003/0702 final

2. Report on the prospects for approximating civil procedural law in the European Union (COM (2002) 746 + COM(2002) 654 – C5-0201/2003 – 2003/2087(INI)) Committee on Legal Affairs and the Internal Market, A5-0041/2004.