COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union ☆

Paul Przemysław Polański *

Kozminski University, Warsaw, Poland

Keywords:
Country of origin principle
Harmful content
Restrictions on information society services
Directive 2000/31/EC
E-commerce directive
Liability of intermediaries

ABSTRACT

The article analyses the country of origin principle of information society services in the light of harmonisation and unification efforts undertaken by the European lawgiver. Although the country of origin principle remains the key element of the construction of freedom to provide information society services, the principle itself suffers a number of both explicit and implicit restrictions which render its practical application a serious challenge. The difficulty is posed by the fact that the Electronic Commerce Directive fails to expressly specify both the scope of harmonisation as regards the principle, and the level of harmonisation of the directive itself. Furthermore, it is understood differently by private international lawyers. In the *eDate Advertising* case the ECJ ruled that the principle is not a conflict-of-laws rule, neither does it require implementation to the national legal systems in this shape. This is not to mean, however, that the debate over the function of the country of origin principle in private international law is over. Last but not least, there are many different types of country of origin principles applicable to various types of services provided via the Internet. This multitude of country of origin principles is perhaps the greatest weakness the regulatory approach adopted by the European lawmaker.

1. Introduction

One of the greatest challenges facing the legal environment of cyberspace is to determine who is to control whom, and on what criteria. Problems surround not only the question whether greater controlling powers should be vested in the country where a service has originated or the country of its receipt, but also by what criteria are the competing legal systems of the member states at issue to be delineated. Private international law has proven largely imperfect in resolving private law problems in cyberspace, let alone the competition in the area of public law, where any such mechanisms would be sought in vain.

Nevertheless, from the perspective of a trader it would be profitable, for the sake of legal certainty, to only apply the legal regime of the country where it is based. On the other hand, from the perspective of the broadly understood consumer

☆ It is an updated and shortened version of the book chapter published in Polish under the title "*Europejskie prawo handlu elektronicznego*" ("*European e-commerce law*") by C.H.Beck.

* *Corresponding author.* Kozminski University, ul. Jagiellonska 59, Warsaw, Poland.
E-mail address: polanski@kozminski.edu.pl.

https://doi.org/10.1016/j.clsr.2017.11.001

protection (e.g. distance contracting, scope of private use under copyright law, personal rights protection, etc.) this is no longer so evident considering the scope of regulatory harmonisation in the area of consumer protection in the European Union. Potential threats in this area may become clearer if one realizes the implications of adopting the exclusive application of the principle of provider's country law, which could lead to providers moving their seats to countries providing the least consumer protection (the so called *race to the bottom*).[1] This line of argument is by no means novel and is in essence a continuation of the many-year disputes over the so called imperative requirements doctrine as put forward by the ECJ in its ruling in *Cassis de Dijon*. This doctrine, however, will be of decreasing importance as the European integration tightens on the basis of the methods of maximum harmonisation and unification of the law.

The aim of this article is to revisit the country of origin principle in the context of information society services in the light of harmonisation and unification efforts undertaken by the European lawgiver. Although the country of origin principle remains the key element of the construction of freedom to provide information society services, the principle itself suffers a number of both explicit and implicit restrictions which render its practical application a serious challenge. The difficulty is posed by the fact that Electronic Commerce Directive fails to expressly specify both the scope of harmonisation as regards the principle, and the level of harmonisation of the directive itself. Furthermore, it is understood differently by private international lawyers. In the judgment in *eDate Advertising* the Court prejudged that the principle is not a conflict-of-laws rule, neither does it require implementation to the national legal systems in this shape. This is not to mean, however, that the debate over the corrective function of the country of origin principle is over. Last but not least, there are many different types of country of origin principles applicable to various types of services provided via the Internet. This multitude of country of origin principles is perhaps the greatest weakness of the regulatory approach adopted by the European lawmaker.

2. The nature and limitations of the country of origin principle

A regulatory mechanism characteristic of information society services is the country of origin principle (French *principe de pays d'origine*, German *Herkunftslandprinzip*). Basically, the country of origin principle entails that it is only the country of service origin that the obligation rests to exercise control over service providers having their seats in its territory, and other countries must not, in principle, interfere in the process recognising the legality of the services provided from the territory of the country in question. It is in this aspect that the regulatory function of the country of origin principle manifests itself with respect to information society services, as it allocates powers to exercise control over content generated by information society service suppliers. Each member state is required to exercise control over traders located in its territory, which entails an obligation to respect the freedom to provide services by suppliers from other member states.

Naturally, there are certain exceptions to this principle thus not rendering the countries where services are received completely helpless towards providers from other member states. For the requirement of mutual recognition of service providers, as well as the scope of controlling obligations at the source, this is restricted as it does not apply to all regulations binding on a given territory, but only to the part thereof which falls within the so called 'coordinated field'. Furthermore, a number of issues are exempted from the country of origin principle, and in individual cases it is always possible for the target state to restrict the provision of a given service where it is justified by the broadly understood public interest. In principle, nevertheless, the leeway provided to the target state is limited for the EU legislator's strategy was to establish a principle of vesting control over services in the country of origin.

Although the country of origin principle delineates the application of different legal regimes within the EU legal framework, its character is radically different from that of rules of conflict in private international law. Directive 2000/31/EC expressly states that it does not seek to establish additional rules of private international law relating to conflict-of-laws.[2] Thus, the principle in question is of public-legal rather than a private-legal nature. Suffice it to say that the principle of autonomy of the will of the parties is not applicable in the context of the country of origin principle. This is not to imply, however, that there are no interesting interrelations between the principle at issue and private international law. Such interrelations arouse upon the emergence of internal market freedoms and EU rules governing conflict-of-laws.[3] Nevertheless, in the present author's opinion, such identification of the principle of control at the source with legal collision rules leads to a misunderstanding, which will be revisited in the latter part of the present article.

Adopting the principle with respect to information society services has been advocated by the European Commission. As early as in the initiative concerning E-commerce[4] and in the draft E-commerce directive[5] European Union perceived it as a key mechanism allowing to base regulation upon internal market freedoms, avoid overregulation, and factor in the actual business backdrop and the urge to quickly answer social needs.[6] A draft of this principle was adopted, in an

[1] *Cf.* e.g. P. R. Weatherill, *Pre-emption, Harmonisation and the Distribution of Competence to Regulate the Internal Market*, [ed.] Barnard, C. and Scott, J., 2002, p. 54.

[2] *Cf.* Art. 1 (4) and recital 22 of the directive.

[3] *Cf.* e.g. C. Twigg-Flesner (ed.) *European Union Private Law*

[4] COM(97) 157 final, 16.4.1997.

[5] One must speak of two drafts, i.e. the original draft Electronic Commerce Directive of 18 November 1998 (COM (1998) 586 final) and the amended draft directive of 17 August 1999 (COM (1999) 427 final). However, since the amended draft brought nothing new as regards the country of origin principle, I shall use the term 'draft' to refer to both versions.

[6] The European Commission has often stressed that the works on the draft were carried out in an intense effort to adopt a relevant instrument by the end of 2000. Ibid., p. 7.

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

essentially unchanged form, in the final version of Directive 2000/31/EC.[7]

In the subsequent parts of the present article I shall analyse the positive aspect, the negative aspect as well as the exemptions from and restrictions of the country of origin principle. In addition, a proper appreciation of its essence require familiarity with the concepts of seat (establishment) and coordinated field, which shall be therefore given separate treatment.

2.1. *Positive aspect of country of origin principle*

The positive aspect of the country of origin principle is set forth in Art. 3 (1) Directive 2000/31/EC, which provides:

> *Each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field.*

Thus, the country of origin principle aims to ensure effective protection of the public interest in the country of origin.[8] A member state must ensure control over service providers established on its territory; however, only to a limited extent specified in the national regulations falling within the coordinated field.[9] Both concepts are vague and require to be construed.

Before moving on to an analysis of these concepts it should be noted that the obligation of control at the source has certain far-reaching implications, of which the administrative bodies responsible for fulfilling tasks of this kind should be aware. Through EU-level "re-regulation" of the national provisions, the country of origin is to ensure protection not only to its own citizens, but to all citizens of the EU, as is expressly stated in recital 22 of Directive 2000/31/EC:

> *Information society services should be supervised at the source of the activity, in order to ensure an effective protection of public interest objectives; to that end, it is necessary to ensure that the competent authority provides such protection not only for the citizens of its own country but for all Community citizens.*

This is a very important reservation, for one must be careful to prevent the effective protection of the public interest by the competent authorities in the country of origin from degenerating into attempts at circumventing the directive by favouring certain traders and "turning a blind eye" to the activities of domestic service providers to the detriment of consumers in other member states.[10] In order to enhance mutual trust among member states, the directive provides for a clear statement of the principles of responsibility of the country of service origin.

The starting point for application of the country of origin principle is the concept of a service provider's establishment.

2.1.1. *Concept of service provider's establishment*

Establishing a criterion which allows to clearly demarcate the areas where national legislation should be applied to online activities undertaken by service providers has long posed one of the greatest challenges facing the law on new technologies. The draft Electronic Commerce Directive itself indicated at least three possible meanings of the concept of a service provider's establishment to be found in member states: 1) the place where the service provider's IT infrastructure is located, particularly the location of website hosting servers; 2) the place from which the service provider's website can be accessed (particularly for the purposes of protection of personal rights of service recipients or third parties); and 3) the place from which a message or communication has been sent (the 'letterbox' principle). [11] In the final version of Electronic Commerce Directive, the EU legislator rejected all the above concepts.

The expression "established service provider" was eventually defined as the place where business is actually carried out rather than the place where the IT infrastructure is located, whether that belonging to a service provider, service recipient or Internet access intermediary. According to the definition adopted in Directive 2000/31/EC, it refers to a service provider who:

> *. . .effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider.*[12] *(emphasis added)*

Thus, Directive 2000/31/EC rejected both the registered seat of a company and the seat indicated in its memorandum of association, giving instead favour to the theory of actual seat in its operating centre variety. This requirement is in line with the CJEU case law and will also be met where a trader is

[7] There are, however, certain differences. In both versions of the draft directive the country of origin principle was set down in two provisions, i.e. Art. 3 and Art. 22, in which reference was made to Annex II. More importantly, both drafts contained Art. 3 (3), which contained an express reference to the rules of private international law: "*Paragraph 1 shall cover the provisions set out in Articles 9, 10 and 11 only in so far as the law of the Member State applies by virtue of its rules of private international law.*" This provision was entirely removed from Directive 2000/31/EC. *Cf.* and also in the discussion of the country of origin principle in Art. 16 of the draft directive on services in the internal market – *Proposal for a Directive of the European Parliament and of the Council on services in the internal market*, Brussels, 5.3.2004, COM(2004) 2 final/3, 2004/0001 (COD).

[8] *Cf.* recital 22 of the preamble to Directive 2000/31/EC.

[9] Similarly with respect to audiovisual services. Under recital 34 of Directive 2010/13/EU "*In order to promote a strong, competitive and integrated European audiovisual industry and enhance media pluralism throughout the Union, only one Member State should have jurisdiction over an audiovisual media service provider and pluralism of information should be a fundamental principle of the Union.*"

[10] Further *Cf.* P. Weatherill, *The regulation of e-commerce under EC law: the distribution of competence between home States and host States as a basis for managing the internal market*, p. 22. The author considers the *ratio legis* of this solution and observes that "*This is the dark side of the picture, painted in its brighter version above, that reserves to national bodies primary competence for administering EC law in preference to establishing a large European bureaucracy. States may cheat.*" [references omitted].

[11] *Cf.* Draft Directive 2000/31/EC, p. 10.

[12] Art. 2(c) of Directive 2000/31/EC.

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

established for a definite period of time.[13] It will be remembered that according to the Court's judgment in *Gebhard*, business activity is characterised by its continuous and permanent, rather than temporary, operation.[14] The directive also provides that where a service provider has several seats, and it is difficult to determine which of those seats is relevant to a given service, the place of establishment will be that where the service provider has its operating centre with respect to a given service.[15]

Doubts may also arise over what steps may be taken by a member state where a service provider established in one country manages all, or a majority, of its activities on the territory of another member state. Where a trader has made such a decision in order to circumvent the law of the state on whose territory it manages all, or a majority, of its activities, such a state retains, by way of exception, the right to take adequate legal steps against such a service provider. [16] Anticipating somewhat the subsequent considerations, it ought to be noted that, as the law stands at present, Art. 3 (4–6) allows, provided certain procedural guarantees are observed, the country of origin to undertake action against traders providing services from a territory of another member state.

The country of origin principle is applicable *ex lege* to all information society services providers established in an EU member state, including in particular hosting services and ordinary transmission services. In the case C 292/10 *G v. Cornelius de Visser*[17], which involved the defendant, an online portal administrator, publishing photographs of the claimant without her authorisation, the Court faced a relatively frequent problem in the Internet, i.e. a hiding defendant. Although the case primarily concerned issues of cross-border jurisdiction, one of the prejudicial questions concerned admissibility of applying the country of origin principle where it is not possible to determine a service provider's place of establishment.[18] In the judgment, the CJEU held that the country of origin principle does not apply to a situation where the place of establishment of the information society services provider is unknown. In a terse justification, the Court emphasised that application of the principle is subject to identification of the member state in whose territory the service provider in question is actually established.[19]

In order to determine the place of permanent establishment in a member state it is insufficient to prove that the service provider uses the technical equipment located on the territory of a given state. This is of particular importance in the context of hosting and cloud services where the data storage and processing infrastructure may be located outside the EU. The directive expressly provides that in ascertaining the place of establishment, neither the place from which a website is available nor the place where the relevant IT infrastructure is located, can be taken into account.[20] Consequently, in order for the country of origin principle to be applicable it is necessary that the place of actual establishment be identified on the territory of a specific member state. Such restriction is caused by the ease of transferring a website from a server located on the territory of one member state to a computer located in another member state, or even outside the EU.

Notably, the principle of disregarding the location of IT infrastructure for the purposes of ascertaining the place of establishment of a business is of international importance. A similar rule will be found in the UN Convention on the Use of Electronic Communications in International Contracts, adopted by the General Assembly of the United Nations on 23 November 2005.[21] The convention makes it specific, in Art. 6 (4), that a location is not a place of business merely because that is where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located, or where the information system may be accessed by other parties. Also, a party's domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country. Instead, the authors of the convention gave effect to the autonomy of the parties' will and created an presumption that a party's place of business is the location indicated by that party, unless another party demonstrates that this is not the case.[22] If, on the other hand, a party has not indicated a place of business or has more than one place of

[13] *Cf.* recital 17 of Directive 2000/31/EC. Similarly with respect to audiovisual media services – *Cf.* recital 35 of Directive 2013/10/EU.

[14] *Gebhard* case, recitals 27–28. This approach renders provision of online services to the freedom of establishment rather than the traditional conception of freedom to provide services.

[15] The latter solution may hardly be considered satisfactory as the largest entities active on the market of online services, such as Google, Amazon or Facebook, will certainly have many centres of activity at their disposal, also with respect to a specific service, e.g. that of natural search.

[16] *Cf.* recital 57 of Directive 2000/31/EC. This solution enjoys a long tradition in Union law. *Cf.* the CJEU judgment of 3 December 1974 in the case C-33/74 *van Binsbergen* [1974] ECR 1299, recital 13.

[17] The judgment of the First Chamber of the Court of 15 March 2012 in the case C 292/10 G against *Cornelius de Visser* (hereinafter *de Visser* case).

[18] "'*Taking account of the [above] judgment [. . .] in Joined Cases C-509/09 and C-161/10 eDate Advertising and Others, are Articles 3 (1) and (2) of [Directive 2000/31] to be interpreted as meaning that, if the place of establishment of the service provider is unknown and it is possible that he is outside the territory of the European Union, the law to be applied in the coordinated field is to be derived solely from the law of the Member State in which the injured person has his domicile or permanent residence, or must it be ensured in the coordinated field under [Directive 2000/31] that the provider of an electronic commerce service is not made subject to stricter requirements than those provided for by the substantive law applicable in the Member State whose nationality the service provider probably holds, or in this case, must it be ensured in the coordinated field under [Directive 2000/31] that the provider of an electronic commerce service is not made subject to stricter requirements than those provided for by the substantive law applicable in all of the Member States?*" *De Visser* case, recital 35.

[19] *De Visser* case, recital 72.

[20] *Cf.* recital 17 of Directive 2000/31/EC.

[21] *The United Nations Convention on the Use of Electronic Communications in International Contracts* became effective with respect to 5 states. EU has not become party to that convention. See A. H. Boss and W. Kilian, *The United Nations Convention on the Use of Electronic Communications in International Contracts. An In-Depth Guide and Sourcebook*. The original text of the convention is available at: http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf, [Accessed 1 November 2017].

[22] *Cf.* Art. 6 (1) of the convention.

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

business, then the place of business is that which has the closest relationship to the contract at issue, considering the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract.[23] Thus, in the case of having multiple places of business, the authors of the convention apply a criterion which is different to the above mentioned conception, developed in EU legislation, of the operating centre with respect to a given service. Although, it appears that these differences will not be of much importance in practice. Nevertheless, the European Union has not acceded to the convention as yet.[24]

It ought to be stated here that the concept of place of establishment for the purposes of the Electronic Commerce Directive will not be identical to the concepts employed thus far in the area of privacy, which is clearly evident from the Data Protection Directive 95/46/EC. Whereas for the purposes of ascertaining the origin of an information society service, it is the place of actual business rather than the location of information infrastructure that is relevant from the personal data protection perspective, on the other hand, the location of ICT systems processing personal data was of far superior importance.[25] This is related to the requirement of determining the physical location where personal data are processed, e.g. with regard to the prohibition of processing personal data in countries which do not ensure an adequate level of data protection.[26] However, as the Court pointed out in its judgment in the case C-101/01 *Lindqvist*[27], Directive 95/46 provides no criteria permitting an unambiguous determination whether operations carried out through hosting services providers are actually carried out where the provider has his place establishment or place of business, or the place, or places, where the computers making up his information infrastructure are located. The judges arrived at the conclusion that the intention may not be attributed to the EU legislator to extend in the future the concept of transferring data to a third country, so as to cover the situation where data is published on a website even if it is thereby accessible to individuals from third countries having the necessary technical means to access such data.[28]

> *Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet.*[29]

The new regulation (GDPR) builds on the original concept of establishment as discussed above.[30] What is relevant is the place where the business decisions do take place. According to recital 22 of GDPR "*establishment implies the effective and real exercise of activity through stable arrangements. The legal form of*

[23] Art. 6 (2) of the convention. *Cf.* also Art. 4 (h) of the convention, which lays down a definition of the seat of enterprise as "*any place where a party maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of goods or services out of a specific location.*"

[24] More on the subject, W. Kilian, *The Electronic Communications Convention: A European Union Perspective* [in:] *The United Nations Convention on the Use of Electronic Communications in International Contracts. An In-Depth Guide and Sourcebook*, (ed.) Boss, A. H. and Kilian, W., Alphen aan den Rijn 2008, p. 407.

[25] This is particularly evident in the context of Art. 4 (1) (c) of the directive 96/46/EC, which states that "Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where : . . .the controller is not established on Community territory and, for purposes of processing personal data *makes use of equipment, automated or otherwise, situated on the territory of the said Member State*, unless such equipment is used only for purposes of transit through the territory of the Community." [emphasis by author] This provision has been transposed into Polish legislation in Art. 3(2) of the Act of 29 August 1997 on the protection of personal data (Journal of Laws No. 133, item 883) whereby: "The Act shall also apply to: 1) non-public bodies carrying out public tasks, 2) natural and legal persons and organizational units not being legal persons, if they are involved in the processing of personal data as a part of their business or professional activity or the implementation of statutory objectives – having the seat or residing in the territory of the Republic of Poland or in a third country, *if they are involved in the processing of personal data by technical means located in the territory of the Republic of Poland.*" [emphasis by author]

[26] Under Art. 25 (1) of Directive 95/46/EC: *"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, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.*"

[27] Pursuant to the CJEU judgment of 6 November 2003 in the case C-101/01 *Bodil Lindqvist*, para. 71 *"there is no "transfer [of data] to a third country" within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is 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."*

[28] *Lindqvist* case, paras. 67–68.

[29] *Ibid.*, para. 69.

[30] *"(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.*"

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect." Location of IT infrastructure is therefore entirely irrelevant in this context. [31] A controller or processor established outside of the EU, who is offering goods or services to data subjects who are located in the EU or who is monitoring their activities by means of e.g. cookies, will therefore fall under the sphere of application of GDPR even if none of his data centres are located in the EU.

2.1.2. *Coordinated field*

Another key concept necessary for the application of the country of origin principle is the issue of coordinated field. The positive instruction addressed to the administration of the state where a service provider has its place of establishment provides that it ensure effective control over the so called coordinated field, which, similarly to the country of origin principle, is defined both positively and negatively. Art. 2 (h) of Directive 2000/31/EC stipulates:

> *"coordinated field": requirements laid down in Member States' legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them;*
>
> (1) *the coordinated field concerns requirements with which the service provider has to comply in respect of:*
> - *the taking up of the activity of an information society service, such as requirements concerning qualifications, authorisation or notification,*
> - *the pursuit of the activity of an information society service, such as requirements concerning the behaviour of the service provider, requirements regarding the quality or content of the service including those applicable to advertising and contracts, or requirements concerning the liability of the service provider;*
>
> (2) *the coordinated field does not cover requirements such as:*
> - *requirements applicable to goods as such,*
> - *requirements applicable to the delivery of goods,*
> - *requirements applicable to services not provided by electronic means.*

The above definition is explained in recital 21 of Directive 2000/31/EC, which clarifies that the coordinated field covers only requirements relating to online activities. The coordinated field thus concerns all provisions relating to (1) the taking up of online activities (e.g. the obligation to register websites providing a newspaper or magazine), and (2) the carrying out of such activities (e.g. prohibition against sending unsolicited mail for the purposes of ESA).

The scope of coordinated field does not include 'non-electronic' aspects of service provision[32], such as control over physical delivery and quality of goods, or requirements applicable to services not provided by electronic means.[33] This does not mean, however, that such matters fall outside the interest of the EU legislator, who has harmonised many of the areas excluded from the coordinated field.[34] Moreover, the scope of coordinated field is of dynamic character and will be subject to change in line with the developments in legislation both at the community and national levels. This is corroborated by the already mentioned recital 22 of Directive 2000/31/EC whereby the scope of coordinated field remains without prejudice to the future harmonisation at the community level of legislation on information society services and future legislation adopted at the national level in accordance with EU law.

The provisions falling within the coordinated field certainly do not comprise a vast majority of legal norms composing the legal systems of particular member states. This particularly refers to provisions incorporated in criminal law.[35] As a result, member states where a service is received may restrict the freedom to provide information society services by virtue of having to enforce penal provisions in effect in the target state.[36]

It appears that, as a result of such approach to the coordinated field, other member states may not raise the objection that the country of origin fails to supervise the areas falling outside its scope. As is evident from the *Ker-Optika* case, the national-level prohibition against offering and concluding contracts for the sale of lenses via the Internet falls within the coordinated field, while the requirements for the delivery of such goods do not.[37] By contrast, the supervision over the manners of distribution of medical products ordered online does not belong to the obligations of the country of origin, remaining instead in the domain of the target state.[38]

---

[31] On the other hand, the challenges relating to the multiple places of business in the area of intellectual property law are well exemplified by the CJEU judgment of 18 October 2012 in the case C-173/11 *Football Dataco Ltd and others v. Sportradar GmbH et Sportradar AG*, which shows complications concerning the qualification of connecting databases located in different member states. The judges found such actions to be 're-utilisation' of data bases: *"The sending by one person, by means of a web server located in Member State A, of data previously uploaded by that person from a database protected by the sui generis right under that directive to the computer of another person located in Member State B, at that person's request, for the purpose of storage in that computer's memory and display on its screen, constitutes an act of 're-utilisation' of the data by the person sending it. That act takes place, at least, in Member State B, where there is evidence from which it may be concluded that the act discloses an intention on the part of the person performing the act to target members of the public in Member State B, which is for the national court to assess."*

[32] Recital 21 of the directive also provides that the coordinated field does not cover the exercise of rights of pre-emption by public authorities concerning certain goods such as works of art, i.e. they are not covered by the obligation of supervision at the source.

[33] *Cf.* recital 21 of Directive 2000/31/EC.

[34] *Cf.* e.g. Directive 2011/83/EU on consumer rights.

[35] So, rightly A. R. Lodder and H. W. K. Kaspersen (ed.) *eDirectives: Guide to European Union Law on E-commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society and Data Protection*, p. 75.

[36] Apart from criminal matters, doubt also arises concerning the question whether member states can freely pass laws on such matters as obligation to publish a website in a specific language, prohibition to offer certain products to minors or prohibition to sell medicines available on prescription. Q. R. Kroes, *E-Business Law of the European Union*, p. 4. The latter issue has already been subject of judicial decision in the already mentioned *DocMorris* case.

[37] *Ker-Optika* case, para. 28.

[38] A. R. Lodder pointed out the fact that a service provider is not required to comply with those provisions of the country of origin which are exempted from the coordinated field. Surprising as it

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

Doubts have been expressed by the jurisprudence as to the nature of the provisions falling within the coordinated field; namely, it is not clear whether it comprises only public law provisions or private law provisions as well.[39] In my opinion, the country of origin principle includes norms of both public and private characters, which follows from its very essence as a model of local service provider control and non-discrimination of service providers from other member states. Hence, member states ought to exercise supervision over service providers fulfilling their obligations both under the substantive civil law (e.g. application of abusive clauses) and e.g. competition law. Moreover, the very definition of the coordinated field is so broad that it is difficult to adduce any arguments for narrowing down its scope so as to include only public law provisions. Let us recall that under the directive, the coordinated field means requirements laid down in Member States' legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them.

However, it must be noted that important exemptions from the coordinated area include consumer law and intellectual property provisions, as well as matters relating to the freedom of choice of law, which were explicitly excluded by the annex to the directive, and provisions of ESA. These matters belong to the sphere of private law, but it would be mistaken to maintain that the coordinated field, and hence the country of origin principle, only comprises provisions of public law. A number of arguments can be adduced in favour of this interpretation. Firstly, the definition of the coordinated field mentions *inter alia* the issues of contracts and liability of intermediaries, which belong to the domain of private law. To this latter domain belong the other provisions which have not been explicitly excluded from the coordinated field, e.g. private international law. Such other provisions fall within the coordinated field, and hence the member state is required to supervise the business activities carried out by traders through their prism.

Thus, the coordinated field covers provisions belonging to private law. The above assertion was fully affirmed by the CJEU judgment in *eDate Advertising*, in which the Court afforded a construction of the term coordinated field:

> *For the majority of the aspects of electronic commerce, however, the Directive is not intended to achieve harmonisation of substantive rules, but defines a 'coordinated field' in the context of which the mechanism in Article 3 must allow, according to recital 22 in the preamble to the Directive, information society services to be, in principle, subject to the law of the Member State in which the service provider is established. In that regard, it must be noted, firstly, that the law of the Member State in which the service provider is established includes the private law field, which is apparent from, inter alia, recital 25 in the preamble to the Directive and from the fact that the annex thereto sets out the private-law rights and obligations to which the Article 3 mechanism does not apply. Secondly, the application thereof to the liability of service providers is expressly provided for by the second indent of Article 2(h)(i) of the Directive.*[40]

Thus, the aim of Directive 2000/31/EC was not harmonisation of all key areas relating to electronic commerce, but rather establishment of a coordinated field which would enable supervision over online businesses at the source. In exercising such supervision, the state should take into account both public and private law, including the civil law.[41] In the light of the above supervision, it should be agreed that the scope of applicability of the country of origin principle is broader than the scope of the Electronic Commerce Directive.[42] Directive 2000/31/EC covers only selected issues related to carrying out business online, and the country of origin principle imposes on member states obligations extending beyond the issues harmonised by its provisions. Thus, services are evaluated on the basis of the entire legal system of the member state where the service provider is established, i.e. both in the light of public law and private law falling with the coordinated field.

Finally, it should be noted that the obligation of supervision at the source also means that a member state may subject an information society service provider to stricter requirements than other member states. Such solution is envisaged in Directive 2010/13/EU on audiovisual media services.[43]

may sound, the author only meant the position of the authors of the directive in this respect. For this obligation may follow from other regulations. So, A. R. Lodder and H. W. K. Kaspersen (ed.) *eDirectives: Guide to European Union Law on E-commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society and Data Protection*, p. 75.

[39] So e.g. M. Świerczyński, *Delikty internetowe. . .*, Warsaw 2006, p. 264 and the literature therein quoted. These doubts, however, arise out of the disputes over the character of the country of origin principle from the perspective of private international law.

[40] The CJEU judgment of 25 October 2011 C 509/09 and C 161/10 in joined cases *eDate Advertising GmbH v X and Olivier Martinez, Robert Martinez v MGN Limited* (hereinafter *eDate Advertising* case), paras. 57–58.

[41] In para. 59 of the above judgment, the CJEU held: "*A reading of Article 3 (1) and (2) of the Directive in the light of the abovementioned provisions and objectives shows that the mechanism provided for by the Directive prescribes, also in private law, respect for the substantive law requirements in force in the country in which the service provider is established. In the absence of binding harmonisation provisions adopted at European Union level, only the acknowledgement of the binding nature of the national law to which the legislature has decided to make the service providers and their services subject can guarantee the full effect of the free provision of those services. Article 3(4) of the Directive confirms such a reading in that it sets out the conditions under which Member States may derogate from Article 3(2), which must be regarded as being exhaustive.*"

[42] *Cf.* e.g. M. Szpunar, *The Country of Origin Principle in the E-commerce Directive* [in:] *Law of E-commerce in Poland and Germany* (ed.) Heiderhoff, B. and Żmij, G., Monachium 2005, p. 113.

[43] Under recital 41 of Directive 2010/13/EU "*Member States should be able to apply more detailed or stricter rules in the fields coordinated by this Directive to media service providers under their jurisdiction, while ensuring that those rules are consistent with general principles of Union law. In order to deal with situations where a broadcaster under the jurisdiction of one Member State provides a television broadcast which is wholly or mostly directed towards the territory of another Member State, a requirement for Member States to cooperate with one another and, in cases of circumvention, the codification of the case-law of the Court of Justice (18), combined with a more efficient procedure, would be an appropriate solution that takes account of Member State concerns without calling into question the proper application of the country of origin principle.*

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

Although it adds even more complexity to international regulation of cyberspace it is actually the very spirit of the country of origin principle. Member states are free to impose higher standards related to e.g. combating illegal content using a specific procedure. They shall not, however, enact a framework, which is even more liberal than e.g. Art. (12–15) of Directive 2000/31/EC, as this would constitute an improper implementation of this instrument. It is especially true these days, in the aftermath of the ECHR *Delfi* ruling.[44]

2.2. *Negative aspect of country of origin principle*

Apart from certain exceptions, the country where a service is received may not restrict services originated from other member states by virtue of the provisions falling within the coordinated field. This is the so called negative aspect of the country of origin principle set forth in Art. 3 (2) Directive 2000/31/EC, which provides:

> *Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State.*

This means, in particular, that the target state may not restrict services originating from other member states only by virtue of the stricter regulations in effect on its territory, provided that such regulations fall within the coordinated field. Such construction would be contrary to the aim of the directive, which sets out to lift all possible barriers to the development of electronic commerce in the EU.[45] The concept of 'coordinated field' is therefore key to comprehending the essence of the country of origin principle, setting, on the one hand, the limits of admissible supervision exercised by the country of origin, and on the other – providing a perspective from which to evaluate the activities of service providers from other member states. For example, a member state where a service is received may not restrict its provision solely on account of more restrictive rules applicable to liability of Internet intermediaries since the provisions governing liability of intermediaries fall within the coordinated field.

As a result, the target state may not demand the application of either its own stricter provisions or of any other provisions at all.[46] It is this very aspect of the country of origin principle that determines its importance for ensuring a free flow of information society services in the internal market. For it is sufficient for an online service provider to establish its business in one member state and comply with the law of that state in order to have other member states tolerate his activities in their respective territories. Nevertheless, the principle may not be applied to situations which are purely internal, i.e. in examining the compliance of a national regulation with EU law insofar as it only concerns economic operators established on the territory of the country of origin, i.e. in situations where the cross-border element does not occur.[47]

The negative aspect of the principle is most clearly evident from the source of the country of origin principle for it stems from the fundamental internal market freedoms, i.e. from the principle of non-discrimination of goods, persons, services or capital originating in other member states. The above opinion is quite common[48], although certain legal theorists have held that there are more differences than similarities between both principles, i.e. the country of origin principle and principle of mutual recognition. [49] It should also be noted that although the essence of the country of origin principle originates in the Treaty provisions and the case law of the Court, its implementation with regard to information society services was implied by the harmonisation objectives as outlined in Directive 2000/31/EC.

It should also be remembered that in contrast to the principle of mutual standard recognition which applies to areas not covered by harmonisation, the country of origin principle will be of greatest significance in areas already subjected to harmonisation. In this sense, the role of the principle of mutual

The concept of rules of general public interest has been developed by the Court of Justice in its case-law in relation to Articles 43 and 49 of the EC Treaty (now Articles 49 and 56 of the Treaty on the Functioning of the European Union) and includes, inter alia, rules on the protection of consumers, the protection of minors and cultural policy. The Member State requesting cooperation should ensure that the specific national rules in question are objectively necessary, applied in a non-discriminatory manner and proportionate." The CJEU judgment cited is the case C-212/97 *Centros v Erhvervs-og Selskabsstyrelsen*, mentioned earlier; the case C-33/74 *Van Binsbergen v Bestuur van de Bedrijfsvereniging*, Rec. [1974] p. 1299; the case C-23/93 *TV 10 SA v Commissariaat voor de Media*, Rec. [1994], p. I-4795, para. 21.

[44] Judgment of the European Court of Human Rights of 16 June 2015 in the Case of *DELFI AS v. ESTONIA* (Application no. 64569/09).

[45] As regards audiovisual media services, recital 36 of Directive 2013/10/EU explains that *"The requirement that the originating Member State should verify that broadcasts comply with national law as coordinated by this Directive is sufficient under Union law to ensure free movement of broadcasts without secondary control on the same grounds in the receiving Member States. However, the receiving Member State may, exceptionally and under specific conditions, provisionally suspend the retransmission of televised broadcasts."*

[46] P. Weatherill, *The regulation of e-commerce under EC law: the distribution of competence between home States and host States as a basis for managing the internal market*, p. 17.

[47] In the context of the protection of minors as the ground for restricting the freedom to provide information society services in the opinion of Advocate General in the case C-244/06 *Dynamic Medien Vertriebs*, para. 29, *et seq*.

[48] Similarly also A. Całus, *Zasada państwa pochodzenia – konkurencja czy uzupełnienie norm prawa wskazującego na właściwość prawa w ramach rynku wewnętrznego (Country of Origin Principle – Competition or supplementation of rules on applicable law in the internal market)* [in:] *Współczesne wyzwania prawa prywatnego międzynarodowego (Contemporary Challenges for Private International Law)*, (ed.) Poczobut, J., Warszawa 2013. The author points out that it is with regard to the country of origin principle that the question arose on the meaning of the principle of mutual recognition as the construction replacing in EU private international law the traditional conflict-of-laws rule.

[49] So A. Całus, *ibid.*, relying on the views of N. Fichtner, who has persuasively argued that it is the deficiencies of the principle of mutual recognition that gave rise to the necessity of creating the country of origin principle. N. Fichtner, *The Rise and Fall of the Country of Origin Principle in the EU's Services Directive – Uncovering the Principle's Premises and Potential Implicationsę,* Essays in Transnational Economic Law 2006 no. 54.

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

standard recognition as regards information society services is played by the principle of notification of draft technical regulations concerning information society services, which was already discussed above. In the opinion of Advocate General Cruz Villalón in the case *eDate Advertising and Olivier Martinez*, the principle epitomizes the more general principle of free flow of services by expressing:

> *(. . .) in an instrument of secondary law a safeguard already provided for in primary law by Article 56 TFEU, and adapts it to the specific features required by the harmonisation of legislation on electronic commerce.*[50]

Although it is often asserted that the country of origin principle has its origin in the freedom to provide services, the Court has frequently emphasised that the home state supervision principle has never been laid down in Treaty provisions.[51] From the perspective of meeting EU objectives, neither the unrestricted home State supervision principle, nor the principle of full country-of-receipt supervision will allow the achievement of the aims of economic integration, and any collision between the two principles must be resolved in a manner seeking compromise between the two extremities.[52]

In the frequently mentioned judgment in the case *Cassis de Dijon*[53], the Court formulated a principle which combines both approaches. The construction of the country of origin principle, therefore, constitutes at the same time an elaboration of the principle of mutual standard recognition, although it must be reiterated that the latter only applies to the areas not covered by harmonisation. It expresses the interests of the country of origin, while also allowing the target state to disapply it in certain clearly defined cases. In other words, the legal norms of the country of origin take priority over the norms of the target state unless the latter proves it necessary to cite one of the grounds from the *Cassis de Dijon* case in order to justify the application of its own provisions in evaluating the legal relationship in question. Consequently, it may be argued that the approach based on a *sui generis* regulatory competence distribution between the countries of origin and receipt has found its new, more sophisticated expression in the country of origin principle.

2.3. *Limitations of country of origin principle*

The country of origin principle is subject to certain substantial limitations. They may be divided into horizontal exemptions and individual exemptions. A separate treatment should be afforded to the matters excluded from the applicability of the entire directive, i.e. tax, privacy protection, gambling and competition protection matters as well as those relating to the activities of notaries and legal representation before courts[54] in addition to the above mentioned regulations falling outside the scope of coordinated field.

2.3.1. *Individual exemptions*

Member states may, under certain circumstances, restrict a specified information society service.[55] Thus, the country of origin principle admits a possibility of blocking the services of a specific service supplier, but not services of a given type. Individual measures must be undertaken in compliance with the prescribed procedure and be both necessary and proportionate with regard to the public policy (in particular the prevention, investigation, detection and prosecution of crime, including the protection of minors and the fight against incitement to hatred on the basis of race, sex, religion or national origin, and also violations of personal dignity concerning individuals), public health protection, public security (including the safeguarding of national security and national defence) and protection of consumers, including investors.

The list of grounds for restricting the activities of a specific service provider is of exhaustive character, which precludes citing any other grounds. This is despite the fact that the CJEU case law has from time to time admitted justifying restrictions of free flow of services on the grounds of e.g. protection of good reputation of the financial services market. [56] Thus, the activities of a given service provider must violate or threaten to violate the above ends, and the member state is required, prior to undertaking such limiting measures, to call upon the member state where the service provider is established to undertake adequate measures, and in the event that such action has proved ineffective, to notify the Commission and the member state in question of its intention to undertake such measures. Only after this

[50] The opinion of Advocate General Pedro Cruz Villalón given on 29 March 2011 in the joined cases C 509/09 and C 161/10 *eDate Advertising GmbH v X* (C 509/09) and *Olivier Martinez and Robert Martinez v Société MGN Limited* (C 161/10), para. 70 (hereinafter Opinion of Advocate Genera in *eDate Advertising* and *Olivier Martinez*).

[51] The CJEU judgment in the case C-233/94 *Germany v. Parliament and Council* [1997] ECR I-2405, para. 64. *Cf.* also P. Weatherill, *The regulation of e-commerce under EC law: the distribution of competence between home States and host States as a basis for managing the internal market*, p. 10.

[52] P. R. Weatherill, *Pre-emption, Harmonisation and the Distribution of Competence to Regulate the Internal Market*."42

[53] The judgment of 20 February 1979 in the case 120/78 *Rewe-Zentral*, known as "Cassis de Dijon", ECR 649. *Cf.* also the judgments: of 10 November 1982 in the case 261/81 *Rau Lebensmittelwerke*, ECR 3961; of 14 July 1988: in the case 407/85 *Glocken et al.*, ECR 4233; in the case 90/86 *Zoni*, ECR 4285. As regards the freedom to provide services and freedom of establishment *cf.* e.g. the judgments: of 17 December 1981 in the case 279/80 *Webb*, ECR 3305; of 4 December 1986 in the case 205/84 *Commission v Germany*, ECR 3755; of 25 July 1991 in the case C 76/90 *Säger*, ECR I 4221.

[54] *Cf.* Art. 1 (5) of Directive 2000/31/WE.

[55] A similar solution is envisaged in Directive 2010/13/EU on audiovisual media services. Under recital 37 of Directive 2010/13/EU *"Restrictions on the free provision of on-demand audiovisual media services should only be possible in accordance with conditions and procedures replicating those already established by Article 3 (4), (5) and (6) of Directive 2000/31/EC."*

[56] The judgment of 10 May 1995 in the case C-384/93 *Alpine Investments BV v Minister van Financien* concerning a prohibition of telephone contacts with individual customers without their prior consent in writing, in order to offer financial services to them. The CJEU found this regulation as restricting the freedom to provide services, which may be, however, justified by reasons of public interest to maintain a good reputation of the national financial sector. *Cf.* also the Commission's Communication on the application of Art. 3(4–6) to financial services, p. 5.

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

procedure has been followed can the member state restrict a given information society service.

Art. 3 (5) of the Electronic Commerce Directive also provides for the possibility of unilateral restriction of a specific online service in the case of urgency without having to meet the above mentioned procedural requirements.[57] In such cases, the Commission and the member state of the service provider must be notified in the shortest possible time with the reasons indicated for which the member state considers that there is urgency. The Commission is required to examine the compatibility of the notified measures with Community law in the shortest possible time; where it comes to the conclusion that the measure is incompatible with Community law, it will ask the member state in question to refrain from taking any proposed measures or urgently put an end to the measures in question.[58]

Despite considerable hopes on the introduction of the above procedure of individual restriction of information society services, the practice to date clearly demonstrates little practical importance of the restriction in question of the country of origin principle. The first Commission Report on the application of the Electronic Commerce Directive indicates that, despite the concerns expressed by some member states, the Commission has been notified only five times under Art. 3 (4–6) of the directive; moreover, all notifications came from the same member state concerning the same matter.[59] Unfortunately, we have no access to any more recent data concerning the application of the mechanism of individual restrictions of information society services under this procedure, which must be deemed as failure on the part of the European Commission to meet the requirements imposed upon it by Art. 21 (1) of Directive 2000/31/EC. [60] The European Commission has only issued a special communication on the application of Art. 3 (4–6) to electronic financial services[61], but even these actions did not help to popularise this method of internal market service regulation.

The lack of practical applications of the possibility of restricting individual information society services on the grounds of the country of origin principle is puzzling inasmuch as it is a common opinion that individuals, whose rights have been infringed in cyberspace, are completely helpless given the global nature of violations committed via the Internet. The mechanism discussed above seems a very important remedy against disseminating unlawful content or hate speech.

Some legal theorists ascribe the lack of use of the above mechanism to the complexity of the country of origin principle itself and the procedure for restricting individual information society services. A. Lodder has observed that the requirement to notify both the member state of service origin and the European Commission may discourage member states from applying the mechanism.[62] Besides the above reasons, which must be agreed with, another important reason may be the broad horizontal exemptions from the country of origin principle, including the exemption of intellectual property matters from the principle in question, which we shall discuss in detail below.

De lege ferenda, it should be postulated that the mechanism of restricting individual information society services be simplified. It is necessary to clearly specify the entity to which an injured person could address with a request to restrict a given information society service. A lack of clear specification of such an entity and of detailed procedure for such notifications may be the basic reason why the mechanism at issue is not functioning in practice. For, in the current state of the law, it is not clear either who should be addressed with such a request, or what such a request should contain.

2.3.2. *Horizontal exemptions*

From a structural perspective, it is the horizontal exemptions that are of the greatest impact on the principle's regulatory character. The Annex to Directive 2000/31/EC lays down eight areas to which the country of origin principle does not apply. The exemption of these areas concerns both the positive and negative aspects of the country of origin principle, which is expressly provided in Art. 3 (3) of the directive.[63] This means that in those areas, member states retain the right to demand that information society service providers meet the legal requirements enforced in the target state. The above restrictions regard the following areas:

1. intellectual property rights, i.e. copyright, neighbouring rights, *sui generis* rights to data bases, semiconductor product topography rights, as well as industrial property rights;
2. the emission of electronic money[64] by certain electronic money institutions[65];

[57] Art. 3 (5) of Directive 2000/31/WE.

[58] Art. 3 (6) of Directive 2000/31/WE.

[59] First Report. . ., p.8.

[60] Pursuant to this provision 1. Before 17 July 2003, and thereafter every two years, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, accompanied, where necessary, by proposals for adapting it to legal, technical and economic developments in the field of information society services, in particular with respect to crime prevention, the protection of minors, consumer protection and to the proper functioning of the internal market."

[61] Communication from the Commission to the Council, the European Parliament and the European Central Bank „ *Application to financial services of article 3 (4) to 3 (6) of the electronic commerce directive*" COM 2003 (259) final, 14 May 2003. Available from: http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0259en01.pdf. [Accessed 23 October 2012].

[62] A. R. Lodder and H. W. K. Kaspersen (red) *eDirectives: Guide to European Union Law on E-commerce. Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society and Data Protection*, p. 76.

[63] The paragraph is worded as follows: "Paragraphs 1 and 2 shall not apply to the fields referred to in the Annex."

[64] This exemption referred to the institutions in the case of which member states applied one the exclusions set forth in Art. 8 (1) of Directive 2000/46/EC Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, which provision was enforced until 30 October 2009. Currently Directive 2000/46/EC has been superseded by Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

3. investment fund advertising, i.e. undertakings for collective investment in transferrable securities (UCITS)[66];
4. insurance law[67];
5. the freedom of the parties to choose the law applicable to their contract;
6. contractual obligations concerning consumer contacts;
7. formal validity of contracts creating or transferring rights in real estate where such contracts are subject to mandatory formal requirements of the law of the member state where the real estate is situated and;
8. the permissibility of unsolicited commercial communications by electronic mail.

The requirement of compliance with the law of the target state entails that businesses must consider the possibility that the target state will impose restrictions in the areas listed above. A question may arise whether the member state of origin of the service is under an obligation to supervise the areas exempted to the extent that such services are directed to the territories of other member states, or whether, in the contrary, the member state of origin of the service is not required to supervise the areas exempted by virtue of the Annex, or even whether it is proscribed from exercising such supervision. In my opinion, the second of the above options is correct.

The exemptions from the country of origin principle are as a result of compromise which is to enable member states to ensure tighter control over certain sensitive areas, such as intellectual property law or consumer protection. Member states offering a higher degree of protection in the exempted areas refused to accept the 'race to the bottom' policy. Adopting this approach entails an obligation on the part of the country of origin to exercise supervision over the coordinated field and to supervise the services directed to its territory which are subject to exemption under the Annex or fall outside the coordinated field.

It is worthwhile to illustrate the above assertion with consumer contract exemption. A determination of the scope of the exemption may have far-reaching implications for the legal certainty of cyberspace trade.[68] For if it is the target state that has exclusive supervisory power over information services addressed to consumers in its territory, then the limitation of the country of origin principle is so substantial, considering the number of Internet websites targeting consumers (B2C), as to justify the assertion that, in essence, the target state principle prevails in the European Union rather than the country of origin principle as regards information society services.

The exemption of consumer contracts from the country of origin principle results in B2C undertakings having to adjust their offers to the legal requirements of the target state. This approach was still justified at the time that Electronic Commerce Directive was being adopted, as the then prevailing approach was based on minimal harmonisation of consumer protection law, which justified vesting the target state with supervision as well as applying protectionist governing law and jurisdiction rules. Upon the adoption of Directive 2005/29/EC on unfair commercial practices and Directive 2011/83/EC on consumer rights, which are based on the maximum harmonisation principle, retaining the exemption of consumer contracts from the country of origin principle does not seem justified any longer. Admittedly, the directives based on minimum harmonisation are still in force, hence perhaps the retention of the exemption. Since, however, a uniform model of consumer protection in the Internet has been adopted, the need to retain the exemption should be reassessed.

De lege ferenda, this exemption ought to be removed by creating uniform European consumer protection law based on maximum harmonisation or unification of the area. The benefits of retaining the exemption have lost its importance as the level of legal protection has risen significantly in addition to

repealing Directive 2000/46/EC, and the counterpart of Art. 8 is currently Art. 9 of Directive 2009/110/EC.

[65] This pertains to the institutions excused by member states from the obligation to comply with certain requirements under Directive 2009/110/EC where the two following conditions are met: "(a) the total business activities generate an average outstanding electronic money that does not exceed a limit set by the Member State but that, in any event, amounts to no more than EUR 5 000 000; and (b) none of the natural persons responsible for the management or operation of the business has been convicted of offences relating to money laundering or terrorist financing or other financial crimes."

[66] Under the currently not binding Art. 44 (2) of Council Directive 85/611/EEC of 20 December 1985 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) "Any UCITS may advertise its units in the Member State in which they are marketed. It must comply with the provisions governing advertising in that State." Since 7 December 2009 enforced is Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) (recast). In accordance with the correlation table the counterpart of Art. 44 of Directive 85/611/EEC is Art. 91(1–4) of Directive 2009/65/EC, whose analysis falls outside the scope of the present work.

[67] Directive 2000/31/EC exempts from the application of the country of origin principle Art. 30 and Title IV of Council Directive 92/49/EEC of 18 June 1992 on the coordination of laws, regulations and administrative provisions relating to direct insurance other than life assurance and amending Directives 73/239/EEC and 88/357/EEC (third non-life insurance Directive), and the provisions of Title IV of Directive 92/96/EEC, Art. 7 and Art. 8 of Directive 88/357/EEC and Art. 4 of Directive 90/619/EEC.

[68] Regardless, it is worth mentioning the problems surrounding the attempts at establishing the impact of this derogation on the rules of private international law. Under recital 55 of the preamble: *"Directive does not affect the law applicable to contractual obligations relating to consumer contracts; accordingly, this Directive cannot have the result of depriving the consumer of the protection afforded to him by the mandatory rules relating to contractual obligations of the law of the Member State in which he has his habitual residence."* The above mentioned recital of Directive 2000/31/EC does not in any case challenge the assertion on the distinction between the country of origin principle and the norms of private international law. However, according to recital 56 of the directive concerned: *". . .those obligations should be interpreted as including information on the essential elements of the content of the contract, including consumer rights, which have a determining influence on the decision to contract."* However, the interpretation of this provision is not easy. It appears that the EU legislator set down certain guidelines for applying self-enforcing provisions to consumer trade. Further details on this subject is discussed in the later part of the present work.

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

considerable approximation, whereas having to respect the exemption only aggravates the difficulty of applying the country of origin principle. In my opinion, the level of harmonisation of consumer protection law is sufficiently high to justify the EU legislator in removing the exemption from the Annex to Electronic Commerce Directive.

Another important exemption from the country of origin principle is the area of broadly understood intellectual property rights. As in the case of consumer rights protection, subjecting the activities of the service providers to the supervision of the target state was necessary mainly on account of the limited scope of harmonisation of IP law in the EU and, at the time the Electronic Commerce Directive was adopted, a lack of the key Directive 2001/29/EC, which was not adopted until a year later. Exempting intellectual property law matters from the country of origin principle may have far-reaching implications, e.g. for Internet intermediaries insofar as their activities violate IP law of the target state. For example, a provider of hosting services established in UK and services on the territories of other member states must take into consideration having to honour the copyright regulations, including fair use which, is well known as not fully harmonised in Directive 2001/29/EC. It may prove that the very sharing of tools for downloading files which infringes copyright will be deemed a copyright infringement in a state which, in accordance with Directive 2001/29/EC, did not implement the fair use doctrine or transpose the respective provision in a very limited form.[69]

The questions relating to exempting IP law-related matters from the country of origin principle fall outside the scope of Directive 2001/29/EC. For example, a number of serious problems have risen in relation to using data bases protected by the far-reaching *sui generis* regime. This particularly concerns the problems relating to secondary use of data bases for the enhanced service purposes, e.g. mash-up services involving combining the content from exclusive right holder data bases with the service provider's own content. Outside the scope of exemption remains the secondary use of public information matters relating to re-use of public sector information regulated by Directive 2003/98/EC. This is not, however, intended to be meant as a result planned for by member states, or as entities providing services from other member states whose business models are based on data from data bases of the target state that necessarily feels secure under the regime of the country of origin principle.

On the contrary, the exemptions from the country of origin principle may even lead one to challenge the assertion that the country of origin principle has simplified the internal market of online services. Without delving at this stage into the controversies surrounding the very nature of the country of origin principle from the vantage point of conflict-of-laws rules, a much more important problem appears to be the fragmentation of the very principle of supervision at the source with respect to such sensitive areas as consumer protection or intellectual property. In addition, it must be remembered that certain areas, key to electronic commerce, have been entirely excluded from the scope of Directive 2000/31/EC, i.e. *inter alia* privacy protection, competition and taxes. Not only did the Electronic Commerce Directive fail to harmonise all the key areas of electronic trade but, even more worryingly, it also did not provide a simple, clear and predictable formula for overcoming problems resulting from having to respect multiple legal regimes concerning information society services.

It may be argued, on the other hand, that certain exemptions have been of diminishing importance over time as the legal regimes of member states have been progressively harmonised and unified. The unification of security and privacy areas—thanks to the eIDAS regulation and the newly adopted GDPR—are the obvious examples. Harmonisation, in turn, has also covered e.g. intellectual property law, including in particular multi-territory licensing, orphan works, software and data base protection, or trademark protection. Of some importance are also the unified areas of intellectual property, such as community trademarks; however, it still appears that too little has been achieved in this field, which will result in hindering of the development of the Digital Single Market.

In summary, an assertion may be put forward that the gradual harmonisation of the law on information society services leads, in the long run, to the strengthening of the country of origin principle. At the present state of the law, particularly the exemption of intellectual property law, consumer protection law and privacy protection may give rise to a considerable increase in legal uncertainty on the internal market.

2.3.3. *Implications of judgment in* UPC Telekabel Wien

In the light of the above mentioned limitations to the country of origin principle, notably with regard to intellectual property matters, one should note the development of alternative means of protection against services from other member states based on court injunctions requiring Internet intermediaries, such as Internet Service Providers (ISPs) or hosting service providers to block certain specific websites, or more widely – certain information society services. Admittedly, the Electronic Commerce Directive failed to harmonise the area, but it expressly permitted member states to impose such prohibitions, promoting at the same time the country of origin principle as the key mechanism in this area.

Under Art. 12 (3) Electronic Commerce Directive, providers of such services, not liable for the content transmitted by the users of their services, do not affect the possibility of a court or administrative authority, in accordance with member states' legal systems, requiring the service provider to terminate or prevent an infringement. A similar solution can be found in Art. 14 (3) of Directive 2000/31/EC whereby the exclusion of liability of hosting providers does not affect the possibility for a court or administrative authority, in accordance with member states' legal systems, of requiring the hosting provider to terminate or prevent an infringement. Nor does it affect the possibility for member states of establishing procedures governing the removal or disabling of access to such information.[70]

On account of the intellectual property matters being exempted from the country of origin principle shall be discussed

[69] A detailed analysis of these issues falls outside the scope of the present article. However, the questions must be answered regarding e.g. the limits of liability of providers of hosting services to other member states on account of the exemption of intellectual property from the country of origin principle, or the limits of using works and other objects of exclusive rights in each country of the EU.

[70] *Cf.* also Art. 13 (2) concerning caching service providers.

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

in detail below, considerable importance has become the question of whether it is possible to impose such injunctions against Internet intermediaries on the grounds of the European IP law.[71] As regards to copyright, the said mechanism was established by Art. 8 (3) of Directive 2001/29/EC whereby:

> *Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.*

The provision was then extended to cover other intellectual property rights by Art. 11 of Directive 2004/48/EC on the enforcement of intellectual property rights.[72]

In the already quoted CJEU judgment of 27 March 2014 in the case C-314/12 *UPC Telekabel Wien*[73], the Court in construing Art. 8 (3) of Directive 2001/29/EC confirmed that a court may require an Internet service provider to deny its customers access to a website infringing copyright or a related right. The case involved a dispute between *UPC Telekabel Wien*, an online services provider, and holders of exclusive rights who demanded that UPC block the *kino.to* service, which enabled downloading or streaming copyright-protected films. The plaintiffs sought an injunction against *UPC Telekabel Wien* to block access to *kino.to* by applying such mechanisms as blocking the domain's DNS or blocking each current IP address of the party arguing that the defendant intermediates in access to unlawfully available content. *UPC Telekabel Wien* objected that the blockade was disproportionate, and in addition neither technically possible nor acceptable. *UPC Telekabel Wien,* was unsuccessful in the proceedings before the first and second instance courts, which ruled that it must adopt adequate measures against future infringements of rights by Internet websites. The lower court ordered specific measures blocking websites to be adopted, whereas the higher court ruled that the effect should be achieved by the website in question being blocked without specifying particular methods of restricting access to the service in question.

UPC Telekabel Wien brought an appeal on a point of law to Oberster Gerichtshof stating *inter alia* that its services could not be considered to be used to infringe a copyright or related right within the meaning of Art. 8(3) of Directive 2001/29 because it did not have any business relationship with the operators of the website at issue and it was not established that its own customers acted unlawfully. Moreover, *UPC Telekabel Wien* claimed that the various blocking measures which may be introduced can all be technically circumvented and that some of them are excessively costly. It will be remembered that, in accordance with the CJEU judgments in *Scarlet*[74] and *Netlog*[75], Internet intermediaries are not required to install, at their own cost, any filtering software dedicated to preventing infringements of intellectual property rights.

The state court asked the CJEU a number of questions, including the key question whether an Internet service provider, such as *UPC Telekabel Wien* is an intermediary for the purposes of Art. 8 (3) of Directive 2001/29/EC. The judges had no doubts that this was the case, citing the judgment in *Tele2*, in which they had already arrived at the conclusion that an Internet access provider, on account of giving access to the web, each time inevitably participates in forwarding an infringement via the Internet between one of his customers and a third party.[76] The argument raised by *UPC Telekabel Wien* that there was no contract between it, as Internet service provider, and the website operator proved to be of no import.[77] One must agree with the Court on this point since, from the perspective of ensuring protection envisaged in Directive 2001/29/EC, the question of contractual relationships, or a lack thereof, between an intermediary and a questioned website operator should be of no bearing.

The judges rejected the arguments raised by *UPC Telekabel Wien* that it was necessary to demonstrate that its customers actually sought for protected content on the questioned website, made publicly available without the consent of legitimate copyright owners. In order for a work to be publicly available it is sufficient, as the CJEU had held in the case C-306/05 *SGAE*, that it be made available to the public, regardless whether any persons belonging to such group had actual access to the work.[78] The judges also held that Directive 2001/29 requires measures which the member states must take in order to conform to that directive aimed not only at bringing an end to infringements of copyright and of related rights, but also at preventing them.[79] The Internet service provider (ISP) was thus deemed an intermediary for the purposes of Art. 8 (3) of Directive 2001/29/EC against whom injunctions may be issued aiming to

[71] *It shall be possible also to impose such injunctions against intermediaries in privacy-related matters. According to Article 2(4) of GDPR: "This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive."*

[72] Pursuant to this provision *"Member States shall ensure that, where a judicial decision is taken finding an infringement of an intellectual property right, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement. Where provided for by national law, non-compliance with an injunction shall, where appropriate, be subject to a recurring penalty payment, with a view to ensuring compliance. Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC."* Pursuant to Art. 1 of the directive "intellectual property rights" include industrial property rights.

[73] The CJEU judgment (Fourth Chamber) of 27 March 2014 in the case C-314/12 UPC *Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH* [hereinafter referred to as *UPC* or *UPC Telekabel Wien* case].

[74] The CJEU judgment (Third Chamber) of 24 November 2011, C-70/10 *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, ECR I-11959 [hereinafter the judgment in the *Scarlet* case].

[75] The CJEU judgment (Third Chamber) of 16 February 2012, C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, ECR 2012 [hereinafter the judgment in *Netlog* case].

[76] Ruling of 19 February 2009 in the case C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, ECR I-1227, para. 44 [hereinafter *Tele2* case].

[77] *UPC* case, paras 34–35.

[78] The judges relied on the CJEU judgment of 7 December 2006 in the case C-306/05 *SGAE*, ECR I-11519, para. 43.

[79] Relying on the already cited rulings in C-70/10 *Scarlet*, para. 31 and C-360/10 *Netlog*, para. 29.

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

restrict access to certain websites that unlawfully place protected content online.

Another question considered by the CJEU was whether the fundamental rights recognised by EU law must be interpreted as a preclusion of a court injunction prohibiting an Internet service provider from allowing its customers access to a specific website when that injunction does not specify the measures which the access provider must take and when that access provider can avoid incurring coercive penalties for breach of that injunction by showing that it has taken all reasonable measures. This also applies to a situation where an Internet service provider can avoid coercive penalties for breach of the injunction by showing that it has taken all reasonable measures to comply with the injunction. Advocate General was of the opinion that it is necessary to indicate specific measures for blocking access to websites which infringe copyright.[80]

At stake, on the one hand, was the right to have one's intellectual property protected (Art. 17 (2) CFR), and on the other – the freedom to conduct a business (Art. 16 CFR) and freedom of expression and information (Art. 11 CFR). We have already witnessed similar conflicts between fundamental rights in the context of online activities. Suffice it to mention the notorious judgment in the case C-275/06 *Promusicae*, in which the CJEU arrived at the conclusion where several fundamental rights collide, member states, in transposing a directive, must give effect to such construction of the directive to ensure adequate balance between the applicable fundamental rights which are protected by the EU law. This is not an easy task given that the above rights and freedoms do not form a hierarchy. Moreover, the authorities and courts of member states are not only required to construe their respective national legislation in line with directives, but they must not rely on such construction of the directives as this would be in conflict with the above mentioned fundamental rights or other general principles of EU law, such as the principle of proportionality.[81]

In the course of its analysis, the CJEU arrived at the conclusion that an injunction, such as that at issue in the main proceedings, restricts the freedom of an Internet service provider to conduct a business, but does not infringe the very substance of the freedom of an Internet access provider to conduct a business. The judges adduced two arguments for the above assertions. First, an injunction of this kind leaves the service provider to determine the specific measures to be taken in order to achieve the result sought, and secondly, it allows him to avoid liability by proving that he has taken all reasonable measures. Thus, the ISP will not be required to make "unbearable sacrifices".[82] Nevertheless, he must ensure that Internet users' rights are protected, including the right of freedom of information; otherwise, such provider's interference in the freedom of information of such users would be unjustified in the light of the objective pursued.[83] This clearly attests to the central role of intermediaries in administration of cyberspace and also to the difficulty of their role.

Bearing in mind the deficiencies of technically blocking websites, the judges concluded that:

> *The fundamental rights recognised by EU law must be interpreted as not precluding a court injunction prohibiting an internet service provider from allowing its customers access to a website placing protected subject-matter online without the agreement of the rightholders when that injunction does not specify the measures which that access provider must take and when that access provider can avoid incurring coercive penalties for breach of that injunction by showing that it has taken all reasonable measures, provided that (i) the measures taken do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available and (ii) that those measures have the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right, that being a matter for the national authorities and courts to establish.*[84]

Thus, Internet service providers will be in charge of the difficult task of ensuring balance between the interests of copyright holders on the one hand and the rights of Internet users to seek information on the latter. The judges' position is in line with both the letter and spirit of the directives harmonising copyright law, and also with the principle of adequate balance for the purposes of the judgement in C-275/06 *Promusicae*.[85] At the same time, the CJEU recognises the complexities associated with providing detailed instructions to ISPs with regard to blocking access to specific types of infringing content. Rather than imposing a specific technical solution on the intermediary, the justices set the goal or goals to be achieved. This approach is yet another reincarnation of the principle of technological neutrality, which underpins numerous IT-related regulatory solutions. In this very context, though, it also seems to give away too much of a regulatory power to private parties with very little control or limits imposed on intermediaries.

From the regulatory perspective the above judgment provides yet another confirmation of the assertion on the limited significance of the country of origin principle as the key mechanism for blocking unlawful content. Administration of member states and the EU unsurprisingly is not the best candidate for a swift management of online content. As a result, for some time now, the discussion over the problems of unlawful content transmission has been centring around the requirements and prohibitions concerning Internet intermediaries rather than the country of origin principle.

[80] *Cf.* the opinion of the Advocate General Pedro Cruz Villalón presented on 26 November 2013 in the case C 314/12 *UPC Telekabel Wien GmbH vs Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft GmbH*, para 110.

[81] The CJEU judgment of 29 January 2008 in the case C-275/06 *Promusicae*, ECR I-271, para. 68.

[82] *UPC* case, paras. 50–53.

[83] *UPC* case, para. 56.

[84] *UPC* case, para. 65.

[85] It is yet another example of a lack of agreement between the opinion of Advocate General and the judges, which is gradually becoming a norm in the judgments of the area of our interest. *Cf.* the already quoted opinion of the Advocate General Pedro Cruz Villalón presented on 26 November 2013 in the case C 314/12 *UPC Telekabel Wien GmbH vs Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft GmbH*, para. 110.

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

3. Country of origin principle and rules of private international law

It should be noted at the outset that the dispute over the impact of the country of origin principle on private international law has enjoyed a long history and it is not likely to be resolved in the near future. Opinions are divided, not only as regards the qualification of the country of origin principle from the standpoint of private international law, but also whether or not the Electronic Commerce Directive precludes the applicability of the rules of private international law.[86] Many authors point to the amorphic, unsettled nature of the principle not yielding to clear classification.[87]

Three approaches have evolved in the legal theory relating to the country of origin principle.[88] The first theory distinguishes categorically the country of origin principle from the rules of conflict-of-laws recognising no impact, or perhaps a limited effect, of the principle on private international law.[89] According to the second view, it is essential that the law determined by the conflict-of-laws rules be adjusted through the application of provisions enforcing their own applicability. The third view, until recently considered as the most prevalent, identifies the country of origin principle with a unilateral conflict-of-laws rule, or posits that it is necessary to establish separate conflict-of-laws rules both in the national and European private international law systems.[90]

The legal-theoretical disputes have had certain implications for the practical transposition of the principle in the legal systems of member states. Some countries have passed laws determining the governing law (e.g. France, Austria, Luxembourg, Portugal, the Czech Republic, Slovakia and Poland), while others opted for transposition based on direct adoption of the mutual recognition principle.[91] A majority of member states thus introduced the country of origin principle in its "pure form", with a minority attributing to it a broader, conflict-of-laws-related significance. Therefore, how Art. 1 (4) of Directive 2000/31/EC is to be construed becomes of paramount importance.

3.1. *Impact of Art. 1 (4) of Directive 2000/31/EC*

It appears *prima facie* that the authors of the directive clearly prejudged the relationship between the country of origin principle and the rules of conflict-of-laws. Directive 2000/31/EC expressly provided that it does not establish:

> *additional rules on private international law nor does it deal with the jurisdiction of Courts*[92]

The autonomy of the traditional rules of private international law is also affirmed by the recitals to the directive.[93] Necessity to treat separately private international law and the country of origin principle is further confirmed by the Services Directive 2006/123/EC, adopted six years later, whose provisions are to be applied subsidiarily to information society services.[94] However, according to recital 23 of Directive 2000/31/EC:

---

[86] Recently, *Cf.* J.-J. Kuipers, *EU Law and Private International Law. The interrelationship in Contractual Obligations*, Leiden-Boston 2012, p. 329. The author maintains that some commentators are of the opinion that the directive "*precludes the application of private laws*." Alas, he does not quote any specific authors.

[87] A. Dickinson describes the country of origin principle as a chameleon changing its colour depending on who, and from which perspective, attempts to analyse it. *Cf.* A. Dickinson, *The Rome II Regulation. The Law Applicable to Non-Contractual Obligations*, Oxford 2008, p. 645.

[88] Three interpretations of this provisions are discussed in e.g. M. Heller, *The Country of Origin Principle in the E-Commerce Directive – A Conflict with Conflict of Laws?*, European Review of Public Law 2004 No. 2 pp. 193–213. *Cf.* also C. Waelde, *Consumers and the Net: A Confusing Maze or a Smooth Path Towards a Single European Market?* [in:] *The New Legal Framework for E-commerce in Europe*, (ed.) Edwards, L., Oxford-Portland 2005, p. 3–30; D. Kot and M. Świerczyński, *Prawo właściwe i jurysdykcja krajowa dla stosunków gospodarczych w Internecie (Applicable Law and National Jurisdiction in Commercial Relationships in the Internet)* #359–472; P. P. Polański, *Usługi społeczeństwa informacyjnego na tle reformy usług w Unii Europejskiej (Information Society Services in the Context of Service Reform in the European Union)*, p. 241.

[89] This view has been recently expressed forcibly by Advocate General Villalón in the case *eDate Advertising* "*In addition, an interpretation of Directive 2000/31 which revealed an applicable rule of law would be invalidated by the current state of secondary law on judicial cooperation in civil matters. It is well known that Regulation No 864/2007 on the law applicable to non-contractual obligations (Rome II) excludes from its scope 'non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation'. (. . .) To my mind, it is at the very least doubtful that Regulation No 864/2007 had to apply an exemption of that kind, since Directive 2000/31 had already laid down a rule harmonising the applicable national provisions in the field.*" (para. 76 of the opinion). *Cf.* L. Bergkamp, *European Community Law for the New Economy*, p. 36. The author deplores the fact that Electronic Commerce Directive did not decide on the question of law applicable to electronic contracts.

[90] The literature on the subject is rich. *Cf.* e.g. M. Heller, *The Country of Origin Principle in the E-Commerce Directive – A Conflict with Conflict of Laws?* In the Polish legal theory the third attitude is advocated by M. Świerczyński, *Delikty internetowe* . . ., p. 285 and the literature therein quoted and the same, *Zasada państwa pochodzenia a prawo właściwe dla zobowiązań związanych ze świadczeniem usług społeczeństwa informacyjnego (Country of Origin Principle and Law Applicable to Provision of Information Society Services)*, Prawo Mediów Elektronicznych – supplement to Mon. Praw. 2006, no. 2, p. 18 et seq. *Cf.* also A. Całus, *Zasada państwa pochodzenia – konkurencja czy uzupełnienie norm prawa wskazującego na właściwość prawa w ramach rynku wewnętrznego (Country of Origin Principle – Competition or supplementation of rules on applicable law in the internal market)*, p. 33.

[91] *Cf.* the Opinion of Advocate General Pedro Cruz Villalón submitted on 29 March 2011 on the joined cases C-509/09 and C-161/10 *eDate Advertising GmbH v X* (C-509/09) and *Olivier Martinez and Robert Martinez v Société MGN Limited* (C-161/10), para. 75. The second category of states includes, according to Advocate General: Belgium, Denmark, the Federal Republic of Germany, Estonia, Finland, Greece, Spain, Italy, Cyprus, Latvia, Lithuania, Hungary, Malta, The Netherlands, Sweden, Romania and the Great Britain and Northern Ireland, United Kingdom.

[92] Art. 1 (4) of Directive 2000/31/WE.

[93] *Cf.* recital 22 of the preamble.

[94] Under Art. 3(1) of Services Directive, the directive does not concern rules of private international law, in particular rules governing the law applicable to contractual and non contractual obligations, including those which guarantee that consumers benefit from the protection granted to them by the consumer protection rules laid down in the consumer legislation in force in their member state.

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

provisions of the applicable law designated by rules of private international law must not restrict the freedom to provide information society services as established in this Directive.[95]

A question thus arises as to whether the EU legislator admitted a certain kind of impact of the rules of private international law on the country of origin principle, given that the norms designated as applicable by the rules of conflict-of-laws must respect the freedom to provide information society services. Moreover, according to recital 22 of Directive 2000/31/EC *in fine*, the service provider should, as a rule, be covered by the legal system of the member state where the service originates:

. . .in order to effectively guarantee freedom to provide services and legal certainty for suppliers and recipients of services, such information society services should in principle be subject to the law of the Member State in which the service provider is established.

The above recitals are not decisive in the determination of the conflict-of-laws nature of the country of origin principle; however, they provide the advocates of this doctrine with certain arguments. Before attempting to evaluate the country of origin principle from the perspective of conflict-of-laws rules, we shall have a closer look at the rules of private international law referred to in Art. (4) of the directive.

First, it must be observed that, at the time Directive 2000/31/EC was being drafted, there were no uniform rules governing jurisdiction and only a limited set of conflict-of-laws rules set forth in the Brussels Convention 1968.[96] The conflict-of-laws rules having bearing on electronic trade were not unified until later years. The most significant from this perspective are the solutions adopted in the regulations Rome I and Rome II and the jurisdiction rules in civil and commercial matters laid down the regulation Brussels I (and Brussels I (recast)). Although an in-depth analysis of the above instruments falls outside the scope of this paper, it may be worthwhile to consider whether, and if so to what extent, the rules of private international law and court jurisdiction, applicable to online trade, could change as a result of applying the country of origin principle.

3.2. *Impact of judgment in joined cases* eDate advertising *and* Martinez

In the CJUE judgment of 25 October 2011 in the joined cases eDate *Advertising GmbH v. X and Olivier Martinez, Robert Martinez v. MGN Limited*[97], the Court addressed *inter alia* the problem of the conflict-of-laws nature of the country of origin principle. The references to the Court for a preliminary ruling from the referring court[98] concerned *inter alia* a determination whether the country of origin principle has a character of a conflict-of-laws rule insofar as it requires the exclusive application of the law applicable in the country of origin (to the exclusion of national conflict-of-laws rules), or whether it operates as a corrective of the law declared to be applicable pursuant to the national conflict-of-laws rules, altering its content to the requirements of the country of origin.[99]

The facts of the first of the joined cases involved *eDate Advertising*, an Austrian company, disseminating on the territory of Germany through an Internet portal, information about Mr. X and his brother being released on a parole from serving a sentence for having killed a famous actor. The contentious post was removed by the sued company, with X asking the German courts *inter alia* to issue an injunction against the owner of the portal to desist from publishing any information concerning his person. The German courts, both of the first and second instances, ruled in favour of X, thereby dismissing the objection, raised by *eDate*, of German courts not having jurisdiction in the case.[100]

The Grand Chamber of the Court of Justice of the EU agreed with the position of Advocate General holding that Art. 3 of Directive 2000/31/EC does not require transposition of the country of origin principle in the form of a specific conflict-of-laws rule. The above conclusion was arrived at by the Court's judges, not only based on the wording of the provision, but also its context and the objectives of the regulation in question. They indicated on that occasion that the normative part of an EU legal instrument must not be considered in abstraction from its justification, which entails that it must be construed in accordance with the motives which led to its enactment.[101]

Nonetheless, as regards the question of the corrective function of the country of origin principle, the Court's position was not as unambiguous as that of Advocate General *P. Cruz Villalón*, who argued that the country of origin principle be entirely separated from conflict-of-laws rules. It did not preclude the possibility of correcting the designated applicable law by relevant provisions of the country of origin, yet indicating that

[95] Recital 23 of Directive 2000/31/EC.

[96] Under Art. 293 indent four of the Treaty, member states entered into on 27 September 1968 Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters, whose text was amended by Convention on the accession of new Member States to the convention. Member states and EFTA states entered on 16 September 1988 into Lugano Convention on jurisdiction and the enforcement of judgments in civil and commercial matters, which constitutes a convention parallel to Brussels Convention 1968. The convention has been subject to revisions.

[97] The CJEU judgment of 25 October 2011 C 509/09 and C 161/10 in joined cases *eDate Advertising GmbH v X* and *Olivier Martinez, Robert Martinez v MGN Limited* (hereinafter *eDate Advertising* case or *eDate Advertising and Martinez* case).

[98] In the same judgment the Luxembourg Court admitted of a possibility that an action for infringement of personality rights be brought before the courts of the member state of the injured party's centre of interests.

[99] An identical question was asked by Landgericht Regensburg in a somewhat later judgment of the First Chamber of the Court of 15 March 2012 in the case C 292/10 *G v Cornelius de Visser* (hereinafter *de Visser* case), but withdrew it upon the discovery of the judgment in the *eDate Advertising* case.

[100] The facts of the case brought by O. and R. Martinez against the publisher of the Sunday Mirror involved disseminating gossip about the claimant's private life, who suffered a violation of his right to privacy and image right. Since in the French court did not refer a question concerning the interpretation of the country of origin principle in this case, it will not be subject of analysis in the later parts of the present work.

[101] *Ibid.* para. 55. Citing e.g. the judgment of the ECJ of 29 April 2004 in the case C-298/00 P *Italy v the Commission*, ECR I-4087, para. 97 and the case law therein cited.

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

the directive does not expressly provide for such a solution.[102] Although the Court did not address expressly the "corrective function" of the country of origin principle, it did state that:

> *. . .within the coordinated field, the directive precludes, subject to derogations authorised in accordance with the conditions set out in Article 3(4), a provider of an electronic commerce service from being made subject to stricter requirements than those provided for by the substantive law in force in the Member State in which that service provider is established.*[103]

The judgment is of paramount importance for the construction of the country of origin principle and its interrelations with private international law. The CJEU prejudged that the country of origin principle is neither a conflict-of-laws rule, nor does it require transposition of the provision in the form of a specific conflict-of-laws rule.[104] The judges of the Court found that the arguments for the applicability of the substantive law of the country where the service provider is established, must not lead one to deem the principle as a private international law norm, as it is not the aim of the country of origin principle

> *. . .to resolve a specific conflict between several laws which may be applicable.*[105]

CJEU reiterated that Art. 3 (1) of the directive principally imposes on member states the obligation to ensure that the information society services provided by a service provider established on their territory comply with the national provisions applicable in the member states in question which fall within the coordinated field, whereas Article 3 (2) of the directive prohibits member states from restricting, for reasons falling within the coordinated field, the freedom to provide information society services from another member state.[106]

As a consequence, the Court affirmed the freedom of member states to designate, pursuant to their private international law, the substantive rules which are applicable "*so long as this does not result in a restriction of the freedom to provide electronic commerce services*".[107] It seems that such interpretation does not conflict with Art. (2) (g) of the Rome II regulation[108], which exempts from its applicability non-contractual obligations resulting from infringement of the right of privacy or other personal rights, including defamation. This exclusion, however, has resulted in a lack of harmonised rules concerning designation of applicable law with respect to this category of torts.[109]

The latter element may, however, have far-reaching implications also in the area of private international law.[110] A proper interpretation of the Court's judgment poses some difficulty, since two opposing views may be adopted. On the one hand, the Court did not expressly provide for a possibility of correcting the designated law by the law of the country of origin, which may lead one to the conclusion that the prohibition on subjecting service providers from other member states to stricter requirements enforced in the target state is only applicable in the areas covered by the country of origin principle rather than those covered by conflict-of-laws rules. On the other hand, the position may be adopted that the above assertion admits of a possibility of the law designated pursuant to the conflict-of-laws rules being corrected by the law enforced in the country where the service provider is established, which in practice amounts to the necessary application of the country of origin law as enforcing its applicability.

Whereas the CJEU unambiguously prejudged the country of origin principle, this precludes a service provider from being made subject to stricter requirements than those provided for by the substantive law enforced in the member state in which the service provider is established.[111] The judges stated that Art. 3 of the directive must be interpreted so as to ensure that the aims of the directive be achieved, i.e. ensure free movement of information society services, and for this reason it is necessary to ensure legal security to the service providers, meaning that they will be precluded from being subjected by the target state to requirements stricter than those governing in the country of origin. The Court also reiterated that it must be possible to apply mandatory provisions which are necessary in achieving the objectives of the internal market, such as the country of origin principle, "notwithstanding a choice of different law".[112] Certain grounds for such reasoning may be provided by the awareness of certain imperfections in the country of origin principle, notably of the exemptions from the principle which give rise to a situation where service providers are forced to comply with stricter requirements of the target state.

From the above, it follows that a service provider may only exceptionally be subjected to the stricter requirements of the target country. Such circumstances may occur where a target

---

[102] *"Consequently, the German legislature has the power to lay down such derogations either by means of substantive measures or also, where appropriate, by means of provisions acting as correctives to the applicable law."* Opinion of Advocate General, para. 80.

[103] *Ibid*. para. 54, relying on the judgments: of 19 September 2000 in the case C 156/98 *Germany v the Commission*, ECR I-6857, para. 50; of 7 December 2006 in the case C-306/05 *SGAE*, ECR I-11519, para. 34; and also of 7 October 2010 in the case C-162/09 *Lassal*, hitherto unpublished in the ECR, para. 49.

[104] *Ibid*., para 63.

[105] *Ibid*., para 61.

[106] According to the CJEU, Art. 3 (1) imposes "on Member States the obligation to ensure that the information society services provided by a service provider established on their territory comply with the national provisions applicable in the Member States in question which fall within the coordinated field."

[107] *Ibid*., para 62.

[108] Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) (OJ EU L of 2007.199.40).

[109] Legal theorists, however, have deemed this solution as favourable to both injured parties and service providers. *Cf.* P. D. Mora, *Jurisdiction and Applicable Law for Infringements of Personality Rights Committed on the Internet,* EIPR no. 5, p. 353.

[110] Advocate General described the above issues as Bundesgerichtshof seeking to establish "*the scope and effect ('corrective [effect] at a substantive law level') which Directive 2000/31 has on German private international law, which would then be the law applicable to a case like the one in eDate Advertising*. Opinion of Advocate General P. C. Villalón, para. 70.

[111] *eDate Advertising*, para. 67.

[112] Ibid. para. 65. *Cf*. also the judgment of 9 November 2000 in the case C 381/98 *Ingmar*, ECR I 9305, para. 25 and the judgment of 23 March 2006 in the case C 465/04 *Honyvem Informazioni Commerciali*, ECR I 2879, para. 23.

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

member state has undertaken measures necessary with respect to a specific information society service under Art. 3 (4) of the directive. It appears, however, that such restriction should not result in the legal situation of such service provider deteriorating; specifically, it ought not to lead to him being deprived of the mitigating effect of the corrective function of the country of origin principle. Otherwise, providers of online services could never be certain of their liability under the law designated pursuant to conflict-of-laws rules, as the application or the less strict provisions of the country of origin would become conditional on the member state authorities undertaking action. Therefore, it must be concluded that the above restriction only reasserts the possibility that specific information society services may be restricted on account of public interest protection, with the proviso that a member state undertaking such action should not be precluded in applying the less strict provisions of the country of origin which enforce their own applicability under such circumstances.

In summary, the Court has prejudged that the country of origin principle must not be identified with conflict-of-laws rules, which require the classical instruments of private international law be applied in designating the applicable law. At the same time the judges prejudged that member states must tolerate the more liberal provisions of the country where the service provider is established and where they fall within the coordinated field. An analogy comes to mind with the provisions of private international law enforcing their own applicability; however, it must be remembered that member states are not required to tolerate the provisions exempted from the country of origin principle, or specific service providers violating vital interests of the target state. Thus, despite the quite unambiguously stated assertions in the judgment, the opinion ultimately prevailed in the Court admitting that the country of origin principle have impact on the application of the classical conflict-of-laws rules.

In the light of the above, the country of origin principle must, firstly, be clearly distinguished, as a rule of public European law, from conflict-of-laws rules, which are principally of national character. The aims of the rules, as well as their constructions and scopes of applicability differ. The country of origin principle lays down,

> *. . .the conditions under which Member States must regulate an economic sector which is part of the internal market,*[113]

whereas rules serve to designate the law applicable in evaluating a specific legal relationship from among the competing legal systems. Neither do the constructions of the connector in private international law and the country of origin principle exhibit any similarities, nor do their scopes of applicability.

Secondly, the country of origin principle has its origin in the Treaty, i.e. in the fundamental treaty freedoms, while conflict-of-laws rules stem from private international law. The principle is neutral from the point of view of private international law.[114] The neutral character is best seen in the above mentioned Art. 1 (4) of the directive and the recitals. The country of origin principle concerns the supervision over the service provider rather than designating the law applicable to the assessment of a legal relationship.[115]

Thirdly, it may not be categorically stated that the country of origin principle will have no bearing on the application of conflict-of-laws rules, since the provisions of the applicable law must not restrict the freedom to provide online services. Nevertheless, the country of origin principle should not be unnecessarily identified with conflict-of-laws rules within the framework of private international law. The proponents of this assertion rely on recital 22 in the preamble to the directive which states that in order to effectively guarantee freedom to provide services and legal certainty, online services

> *. . .should in principle be subject to the law of the Member State in which the service provider is established.*[116]

However, the above recital may only be interpreted in the context of both the positive and negative aspects of the country of origin principle rather than as an intention to bestow upon it a conflict-of-laws character. It is the more so since the directive prejudged that the hitherto established private international law instruments must be applied rather than creating new conflict-of-laws rules. The above discussion is largely confirmed by the key CJEU judgment in the joined cases *eDate Advertising* and *Martinez*.[117]

4. Multitude of country of origin principles

One of the weaknesses of the current regulatory philosophy concerning Internet-mediated services is the lack of its homogeneity. There are many different types of Internet services, ranging from classical e-commerce services, such as e-shops or portals to video streaming services to identification services to numerous value-added services, which companies continue to develop and market in cyberspace.

One of the great initial ideas of the European lawgiver was to subject them to the country of origin principle. Such services are provided at a distance and therefore it would be more feasible to control them at the origin rather than force service providers to comply with various domestic legal regimes. Yet, the country of origin principle assumes the existence of exceptions, which in reality force service providers to comply with national laws of the country of destination. This assumption could be regarded as one of the inherent weaknesses of the Internal Market Principle.

[113] Opinion of Advocate General Villalon in the case *eDate Advertising*, para. 72.

[114] Opinion of Advocate General Villalon, paras 73–74. *Cf.* also D. Martiny in: *Münchener Kommentar zum Bürgerlichen Gesetzbuch,* vol. 10, TMG § 3 Herkunftslandprinzip, 5. Aufl., München 2010, para 36.

[115] So, rightly J.-J. Kuipers, *EU Law and Private International Law. The interrelationship in Contractual Obligations*, pp. 334–336.

[116] Sentence 2 recital 22 of Directive 2000/31/EC.

[117] Similarly also J.-J. Kuipers, *EU Law and Private International Law. The interrelationship in Contractual Obligations*, p. 336. *Cf.* also D. Martiny, *TMG § 3 Herkunftslandprinzip [in:]: Münchener Kommentar zum Bürgerlichen Gesetzbuch, vol.* 10, 5 ed., München 2010.

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

However, an even more compelling weakness results from adopting numerous country of origin principles for various services provided at a distance. The Electronic Commerce Directive was not the first legal instrument to make use of the country of origin principle. Specifically, conditional access services regulated by Directive 98/84/EC[118] or the audiovisual media services laid down in Directive 2010/13/EU[119] have also been covered by the country of origin principle.[120] Their analysis clearly shows a gradual evolution towards ever more complicated legal constructions. For it had been evolving gradually and admitting ever more elaborated catalogues of exceptions to it as well as providing for case-by-case restrictions of services on account of an important public interest.

On the other hand, the eIDAS regulation[121] sets out a far more simplified version of the country of origin principle. Under Art. 4 (1) of the regulation: "*There shall be no restriction on the provision of trust services in the territory of a Member State by a trust service provider established in another Member State for reasons that fall within the fields covered by this Regulation.*", whereas under paragraph 2 of that Article: "*Products and trust services that comply with this Regulation shall be permitted to circulate freely in the internal market.*" However, the obligations imposed on the authorities supervising the provision of trust services were significantly broadened.

This approach can be sharply contrasted with the newly adopted General Data Protection Regulation, which does not contain a country of origin principle, but instead establishes a broad territorial scope of application, which extends beyond the territory of the European Union and affects undertakings localized in other countries.[122] Recital 22 of the GDPR is structured *prima facie* similarly to the positive aspect of the country of origin principle, in the sense that it applies to service providers established in the EU:

> *Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.*

There are considerable differences in relation to the country of origin principle, however. Firstly, there are no exemptions from that principle that a country of destination could invoke, as is the case with information society services. Secondly, there is no urgency procedure that could be utilized by the country of destination to block a specific information society service provider breaking rules of the country of receipt. Last but not least, the regulation applies to service providers not established in the EU. This extra-territorial application of the GDPR is probably one of the most important rules established in the regulation. Recitals 23 and 24 make it clear that the GDPR will be applicable to foreign companies even if their on-line services are not directly provided for remuneration[123] or they are limited only to monitoring the behaviour of customers located in the EU by means of e.g. cookies or similar technologies.[124]

---

[118] Art. 3 stipulates: 1. Each member state shall take the measures necessary to prohibit on its territory the activities listed in Article 4, and to provide for the sanctions and remedies laid down in Article 5. 2. Without prejudice to paragraph 1, Member States may not: (a) restrict the provision of protected services, or associated services, which originate in another Member State; or (b) restrict the free movement of conditional access devices; for reasons falling within the field coordinated by this Directive.

[119] *Cf.* Art. 4 of Directive 2010/13/EU, which bears the closest resemblance to the approach adopted in Directive 2000/31/EC. Under recital 33 of the directive: "*The country of origin principle should be regarded as the core of this Directive, as it is essential for the creation of an internal market. This principle should be applied to all audiovisual media services in order to ensure legal certainty for media service providers as the necessary basis for new business models and the deployment of such services. It is also essential in order to ensure the free flow of information and audiovisual programmes in the internal market.*"

[120] *Cf.* P. P. Polański, *Usługi społeczeństwa informacyjnego na tle reformy usług w Unii Europejskiej (Information Society Services in the Context of Service Reform in the European Union)*, p. 241.

[121] *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73–114), which with some exceptions entered into force from 1 July 2016.*

[122] *According to Art. 3 (1) of the 016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), which will enter into force in May 2018, it applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*

[123] "(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union."

[124] "(24)The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the Internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001

The country of origin principle is always applicable only to EU establishments.

Various types of country of origin principles might lead to further over-complication of an already complex legal regime in the EU concerning information society providers. For instance, information society service provider wishing to combine e-commerce, audiovisual and trust services in one commercial offer would be required to take into consideration three country of origin principles with their varying individual and horizontal exceptions.

5. Conclusion

The country of origin principle constitutes one of the pillars of the electronic commerce market in the European Union. In a model approach it allows service providers to offer goods or services from one member state, in which they have decided to establish. It also allows the target state to block a specific service provider if his services pose a threat to the interests of that state, which may be at the same time justified by the requirements indicated in Electronic Commerce Directive or the Treaty. It is surprising in this context how rarely these mechanisms have been used by member states and individuals, who hardly ever employ this mechanism of regulating the freedom to provide online services.

However, the principle has substantial limitations. Certainly, it is not of absolute character in the sense of protecting the service provider from having to learn about the laws of the target state. There are a number of exemptions from its application, particularly with respect to intellectual property law. The power of the principle is weakened by the limited harmonisation of copyright law caused by wide differences between the legal traditions of the member states, concerning *inter alia* such contentious issues as admissibility and extent of private use (also known as fair use, fair dealing in various jurisdictions). The areas which have been exempted from the principle include the consumer law of the target state, which is fundamental to the vast majority of those who sell via the Internet. Service providers must thus take into account national differences in this respect, which are only to a limited degree alleviated by Directive 2011/83/EU on consumer rights, based on maximum harmonisation. For it allows to keep in force the previously existing legal solutions in this respect.

The country of origin principle is not in opposition to the mechanism of harmonisation of member states' laws, which is often the case with respect to actions taken concerning the free movement of goods, where the EU often faces a dilemma: mutual recognition or harmonisation. It supplements the harmonisation mechanism being at the same time its first-born child. For it is enacted by the Electronic Commerce Directive and a number of other directives having considerable impact on the online services market in the EU. In this context it must be emphasised that its character is not homogeneous because there are a number of versions of the principle created and developed by subsequent EU directives. A heterogeneous character of the principle has certainly contributed to the difficulties with its application as with respect to each of the services which are relevant for our purposes e.g. a different catalogue of exemptions from the principle will have to be applied. Perhaps in the future, with the increasing unification of the EU law, the principle itself will become simplified, which direction seems to be indicated by the way in which this principle is framed in the eIDAS regulation.

Acknowledgement

This article has been financed by NCN grant "Fighting illegal and harmful content on the Internet" nr DEC-2014/15/B/HS5/03138.

Author Information

Paul Przemysław Polański, PhD (Melbourne University), a lawyer and a computer scientist, Professor at Kozminski University, Warsaw, Poland and the President of FREE Foundation.

Please cite this article in press as: Paul Przemysław Polański, Revisiting country of origin principle: Challenges related to regulating e-commerce in the European Union , Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.001