EU study on the

Legal analysis of a Single Market for the Information Society

New rules for a new age?

7. Electronic payments
8. Electronic contracting

November 2009

DLA PIPER

Table of contents

This study was commissioned by the European Commission's Information Society and Media Directorate-General, in response to the invitation to tender OJ 2007/S 202 244659 of 19/10/2007. The study does not, however, express the Commission's official views. The views expressed and all recommendations made are those of the authors.

Chapter 7
Electronic payments

1. Introduction

In 1999, eBay acquired Billpoint, an electronic payment service which could reduce the time required for eBay members to complete a transaction with several days. Billpoint was to become the "master merchant" for processing member transactions[1]. However, the service failed substantially, due to its poor business plan, hostility from eBay sellers and competition from PayPal.

Billpoint's failure was an illustration of the apparent lack of a market for e-payment systems. Oddly enough, the overwhelming majority of commercial transactions facilitated by the Internet use a conventional payment system. Even in 2002, shoppers made at least 80% of Internet purchases with credit cards. The early days of the Internet heralded a variety of proposals for entirely new payment systems—generically described as electronic money—that would use wholly electronic tokens that consumers could issue, transfer, and redeem.

But years later, no electronic-money system (other than PayPal) has gained a significant role in commerce – even the most famous of the electronic-money providers, DigiCash, eventually filed for bankruptcy. Those that exist, only make up for a tiny fraction of money being circulated.

This chapter will therefore assess the impediments for a further development and improvement of the e-money payment system caused by EU e-money legislation, taking into account the new eMoney Directive, adopted on 16 September 2009.

2. High-level overview of e-payments

2.1. Why is there a need?

Dominance of credit cards – The introduction of e-money led some to believe that conventional cash would be to an important extent replaced by e-money, so that society would become "moneyless" in the distant future[2]. However, against expectations, the use of traditional payment systems for online purchases still prevails over the use of online payment systems. Online purchases in Europe are being dominated by payment methods which are also customary in the offline world, such as credit cards[3].

Whereas credit cards were originally developed for payments made in the context of a direct physical interaction between buyer and seller at the point of sale, they were also increasingly used for remote payments, such as transactions via telephone. Credit cards maintained their popularity for remote payments when the widespread introduction of the Internet entailed remote online shopping[4].

---

[1] T. CLARK, "eBay acquires two firms", *CNET News*, May 1999

[2] G. PAPADOPOULOS, *Electronic money and the possibility of a cashless society,* Working Paper 18 February 2007, available at http://ssrn.com/abstract=982781

[3] S. HENG, "E-payments: modern complement to traditional payment systems", in *Deutsche Bank Research*, E-conomics, 6 May 2004, No. 44, p. 2, available at www.dbresearch.com/PROD/DBR_INTERNET_DE-PROD/PROD0000000000079835.PDF

[4] European Central Bank, *E-payments without frontiers,* Issues paper for the ECB Conference on 10 November 2004, p. 46, available at www.ecb.int/pub/pdf/other/epaymentsconference-issues2004en.pdf

Nevertheless, the use of traditional payment methods in an online context seems to have reached its limits, particularly due to the high transaction costs and the security risks. For example, the transaction costs relating to payments of less than 10 EUR for multimedia content cannot be recovered if such payments are made by credit card[5].

Arrival of e-money – Together with the rise of the Internet, several promising new payment techniques, including e-money, were developed to deal with the specificities of an online context. However, e-money continues to play a very limited role in the online payment sector in the EU. Despite a gradual increase in the period 2005–2007, the total amount of electronic money in circulation remains less then 1% [6]. Expressed in enterprise turnover, e-money only accounts for 4.2% of all EU enterprise turnover[7]. Only a limited number of electronic money issuers (20) have been created in the European Union[8], although 127 waivers were also granted[9].

Besides the main issue of the legal hurdles imposed by the eMoney Directive, the limited penetration of e-money also results (although to a lesser extent[10]) from technical and psychological barriers. E-money systems are often not interoperable, nor standardised. In addition, they cannot always guarantee the security of transaction, nor the anonymity of its users[11]. Consequently, e-money schemes suffer from a lack of market confidence[12], and although a market for e-money payments does exist within the EU, it is of limited importance[13].

Mobile payment – Another example of new payment techniques are mobile payment services (*e.g.,* payment by cell phone), which have the advantage that they can be easily used in both an online and an offline context, enhancing their accessibility. Indeed, mobile devices can be carried around permanently and are personalised and designed to be connected. Moreover, the use of mobile devices is widely diffused in Europe, even more so than the use of computers and Internet[14].

In the late 1990s and early 2000s, hundreds of mobile payment systems were being introduced worldwide. Even after the burst of the Internet hype, mobile payment services remained a hot topic[15]. However, many mobile payment systems failed to reach their potential in the EU, due to their inability to attract customers, merchants and banks. Their limited success was partly caused by the fact that mobile technologies were not sufficiently mature and not easy to use[16]. In addition, mobile payment services

---

[5] S. HENG, *o.c.*, p. 2

[6] Impact assessment for the new eMoney Directive (SEC(2008)2573), 9 October 2008, p. 6, available at http://ec.europa.eu/internal_market/payments/docs/emoney/sec-2008-2573-impact_ass_en.pdf (hereafter called the "Impact assessment")

[7] Impact assessment, *o.c.*, p. 7

[8] The most important one, PayPal, has adopted the status of a credit institution.

[9] Impact assessment, *o.c.*, p. 10

[10] Impact assessment, *o.c.*, p. 6

[11] Whereas cash is anonymous, certain types of e-payments require at least to counterparties which both have knowledge as to what goods are services are being purchased, namely the seller and the financial institution effecting the payment.

[12] P. ATHANASSIOU and N. MAS-GUIX, "Electronic money institutions current trends, regulatory issues and future prospects"*, European Central Bank Legal Working Paper Series,* No. 7, July 2008, p. 11

[13] *Ibid.*, p. 10

[14] European Central Bank, *E-payments without frontiers, o.c.*, p. 18

[15] T. DAHLBERG, N. MALLAT, J. ONDRUS and A. ZMIJEWSKA, *Mobile Payment Market and Research - Past, Present and Future, Proceedings of Helsinki Mobility Roundtable,* Sprouts: Working Papers on Information Systems, p. 1, available at http://sprouts.aisnet.org/6-48

[16] *Ibid.*, p. 2

were subject to a vague and unclear legal framework. In Japan, on the other hand, mobile payments have gained large adoption, and are still increasing in user base.

New technologies for mobile payments, including contactless vending and ticketing and RFID, now seem to stimulate a renewed interest in mobile payment services[17]. However, given the lack of standards and the immaturity of the market, it is doubtful whether these services will now be more successful. Financial institutions and mobile operators are trying to overcome these issues by launching isolated initiatives to respond to current specific market needs[18].

2.2. Requirements for successful electronic payment systems

Critical mass – The success of a payment scheme depends on the number of users, both as regards merchants and consumers, as financial institutions. Especially merchants play a crucial role in the development of payment schemes, as their acceptance of e-payment systems creates the market for such schemes. Providers face the so-called "chicken and egg" problem, as merchant acceptance equally depends on customer acceptance[19].

Adoption at the EU-level – In order to foster cross-border payments in the Internal Market, it is essential that payment schemes are developed that apply across the EU. Merely national payment schemes will not increase cross-border e-shopping, because foreign customers cannot pay abroad with these national schemes. Payment schemes that are limited to the national level, should at least try to enter into cross-national associations to gain customer and merchant recognition.

Limited costs – The cost of using an electronic payment system should be limited to a minimum, so as to increase merchant and customer acceptance. This particularly holds true for low-value transactions, which must be facilitated by low transaction costs. (For example, the online purchase of a ringtone of 1 EUR should not result in the need to pay an additional 0,40 EUR for transaction costs.)

User friendly / low effort – Electronic payment systems should be user-friendly and should allow users to personalise the system to integrate their every day activities and personal financials. Simplicity is key to gaining wide acceptance, especially to persuade new Internet users who lack both experience and confidence to cope with complicated protocols[20].

> *In Japan, for example, most electronic payment systems only require the user to enter a unique set of 16 digits for authentication and payment finalisation purposes.*

Speed – Electronic payment systems should be able to process transactions very rapidly. Their speed allows them to be differentiated from other (offline) payment schemes such as credit cards, which are often subject to transaction terms of several days. Settlement of transactions in real time allows customers to be informed of their available funds at any moment.

Security – Fraudulent payment card transactions represent losses of roughly 1 billion EUR per year in the SEPA area[21]. Moreover, given their virtual nature, e-payment schemes do not allow to see the money physically represented, which often results in the feeling of having no control[22]. It is therefore essential

---

[17] *Ibid.*

[18] *Ibid.*, p. 10

[19] European Central Bank, *E-payments without frontiers, o.c.*, p. 24

[20] R. GUTTMANN, *Cybercash - the coming era of electronic money*, 2003, p. 89

[21] Commission Staff Working Document, *Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 EU action plan*, SEC/2008/0511 final

[22] *Ibid.*, p. 94

that e-payment systems provide a sufficient level of security, both on a technological level as on a psychological level.

Balance of interests – The current financial crisis has demonstrated the importance of controlling financial institutions. Payment instruments which transfer substantial amounts of money, should be strictly regulated, regardless of the fact whether they constitute online or offline payment systems. However, there also is a need for balance. Strict compliance requirements could cripple the further development of e-payment systems, particularly if small money transfer would also be subject to such requirements. Hence, a balance between innovation incentives and the protection of consumers is required.

Protection of privacy – As is possible with cash payments, consumers will want to have at least the option of remaining anonymous in relation to e-payments[23]. Moreover, the possibilities of profiling based on financial transaction data should be limited. For example, the use of transaction-related data outside the initial business context, of the sale of such data to third parties could lead to customer discrimination. Such practices should therefore be contained by legal privacy provisions[24].

Transparency – Electronic payment schemes must be transparent to consumers, in particular with respect to their personal financial data being handled by both merchants and financial institutions. Transparency requires merchants and financial institutions to describe the way in which an electronic payment system works, and how they intend to process any transactions requested by consumers.

Predictability – For adapted legal rules to be effective, it is required that e-payment systems are generally intelligible, clear and predictable to all actors involved[25]. Any laws applicable to e-payment systems must therefore clearly establish which services do and which do not fall within their scope.

Trust – Both the electronic payment schemes themselves and the applicable legal framework must present a trustworthy system. Customers and merchants will refrain from using such payment schemes if the applicable laws cannot guarantee the protection of their interests. Equally important is the need to address the issue of perceived trust: the public must be convinced that cybercash is unforgeable.

Reliability – The legal framework applicable to electronic payments must be consistent in its effects on all participants. In case of a dispute, the application of such laws should be predictable, and the expected outcome of the dispute should be reliable.

3. Legal instruments

3.1. Previous eMoney Directive

3.1.1. Background to the Directive

The emergence of e-money on the European market occurred in the non-financial sector. Non-bank companies were the first to issue pre-paid payment cards. The previous eMoney Directive[26] represented

---

[23] R. GUTTMAN, *o.c.*, p. 87

[24] European Central Bank, *E-payments without frontiers, o.c.*, p. 34

[25] A.E. KELLERMAN a.o., *Improving the Quality of Legislation in Europe*, Kluwer,1998, p. 89

[26] 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, *O.J.* L 275 , 27 October 2000, p. 39

a response to the emergence of these new pre-paid electronic payment products[27]. The legislative process preceding the adoption of the previous eMoney Directive lasted over two years, especially due to the intensive interaction between the Commission and the European Central Bank (ECB) with respect to some key issues[28].

The Commission focused on competition issues and found it *"necessary to coordinate and harmonise Member States' laws"* [29]. The Commission also found it important to create a legal framework that would allow further innovation, and found it *"desirable to provide a regulatory framework that assists electronic money in delivering its full potential benefits and that avoids hampering technological innovation in particular"* [30].

The ECB maintained a different approach, however. The ECB was of the opinion that the legal framework should, amongst other things, ensure the protection of customers merchants, guarantee the stability of financial markets, protect participants against criminal abuse and avoid market failures[31].

Caught between the cautious approach of the ECB and the more liberal stance of the European Commission, which placed greater emphasis on innovation and competition, the eMoney Directive became a compromise[32]. The previous eMoney Directive intended to create a clear legal framework designed to strengthen the Internal Market and stimulate competition, whilst at the same time ensuring an adequate level of prudential supervision[33].

3.1.2. Most important issues under the previous eMoney Directive

The previous eMoney Directive was adopted in response to the emergence of new categories of pre-paid payment instruments, in the context of the rapid changes in the business environment linked to the information technology revolution[34]. Despite the Commission's intention to create a legal framework that would allow and enhance technological innovation, an evaluation of the application of the Directive shows that it rather *impedes* the further development of e-payment techniques. As a result, in most of the Member States, e-money is not a credible alternative to cash.

> *For example, with respect to mobile payments, Commissioner Reding declared in a recent speech: "Today, the lack of common EU-wide standards and rules for "m-cash" leaves the great potential of "m-commerce" and the mobile web unexploited. We have more than 500 million mobile users in Europe.*

---

[27] Commission Staff Working Document on the Review of the E-Money Directive (2000/46/EC), 19 July 2006, p. 3 available at http://ec.europa.eu/internal_market/payments/emoney/index_en.htm

[28] Evaluation of the E-money Directive (2000/46/EC), Final Report, available at http://ec.europa.eu/internal_market/payments/emoney/index_en.htm

[29] Commission Proposal for a European Parliament and Council Directive on the taking up, the pursuit and the prudential supervision of the business of electronic money institutions, COM(1998) 461 final, 21 September 1998, *OJ* C 317, 15 October 1998, p. 7

[30] *Ibid.*

[31] European Central Bank, *Report on Electronic Money*, August 1998, available at www.ecb.int/pub/pdf/other/emoneyen.pdf, p. 13-17

[32] P. ATHANASSIOU and N. MAS-GUIX, *o.c.*, p. 16

[33] Commission Staff Working Document on the Review of the E-Money Directive (2000/46/EC), *o.c.*, p. 3

[34] Explanatory Memorandum to the Proposal for a Directive of the European Parliament and of the Council 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 repealing Directive 2000/46/EC, 9 October 2008, COM(2008) 627 final.

> *This means that Europe has the economies of scale to offer for an innovation-friendly environment that will allow transforming the mobile phone into an electronic wallet."* [35]

This section 3.1.2 provides a summary of the most important issues under the previous eMoney Directive. A detailed overview of all issues can be found in the Commission's Staff Working Document on the Review of the E-Money Directive[36] and its Final Report on the Evaluation of the E-Money Directive[37].

1. The first problem relates to the unclear **definition of electronic money** and the scope of the Directive, which generates legal uncertainty and hinders the development of the market. The definition of electronic money is so unfettered that it was predestined to foster divergent interpretations of what is a key determinant of the eMoney Directive's applicability[38].

The definition of "electronic money" included in article 1.3(b) of the previous eMoney Directive sets forth three criteria to determine whether or not a product constitutes e-money:

- stored on an electronic device;
- issued on receipt of funds of an amount not less in value than the monetary value issued; and
- accepted as means of payment by undertakings other than the issuer.

As regards the first criterion (storage on an electronic device), the previous Directive intended to include a technology-neutral definition, which would avoid the need to constantly revise the directive to keep pace with technological changes. However, since the Directive's adoption, new business models were developed for which it is uncertain whether they fall within the scope of the Directive, such as mobile telephone prepaid payment cards, retail customer 'loyalty cards', re-loadable or one-off voucher-type electronic cards and employee-scheme electronic cards[39]. In addition, the reference to "electronic device" raises the question whether this would include server-based e-money[40].

The second criterion (receipt of funds) has raised concerns that the inclusion of this criterion could constitute a potential loophole, as schemes issuing e-money at a discount would fall outside the scope of the definition. Several Member States have modified this criterion, so as to avoid that the issuance of e-money at a discount would not be subject to the Directive. For example, Ireland included an explicit prohibition on issuing e-money at a discount[41].

The legitimate purpose of the third criterion (*"accepted as means of payment by undertakings other than the issuer")* is to demarcate e-money products from payment instruments accepted by their issuer only. Nonetheless, it has been identified correctly by the Commission in its Staff Working Document as the criterion which is most open to misinterpretation[42]. The question arises which number of entities is

---

[35] V. REDING, EU Commissioner for Telecoms and Media Digital Europe - Europe's Fast Track to Economic Recovery, The Ludwig Erhard Lecture 2009 Lisbon Council, Brussels, 9 July 2009

[36] Commission Staff Working Document on the Review of the E-Money Directive (2000/46/EC), 19 July 2006, available at http://ec.europa.eu/internal_market/payments/emoney/index_en.htm

[37] Evaluation of the E-money Directive (2000/46/EC), Final Report, available at http://ec.europa.eu/internal_market/payments/emoney/index_en.htm

[38] P. ATHANASSIOU and N. MAS-GUIX, *o.c.*, p. 19

[39] *Ibid.*, p. 18-19

[40] Commission Staff Working Document on the Review of the E-money Directive, *o.c.*, p. 11

[41] Final Report on the Evaluation of the E-money Directive, *o.c.*, p. 48

[42] Commission Staff Working Document on the Review of the E-money Directive, *o.c.*, p. 12

required to accept the e-money, and what sort of relationship needs to exist between issuer and accepting merchants[43].

2. The second problem relates to an inconsistent legal framework with a **disproportionate prudential regime**. To counterbalance the less cumbersome features of the prudential supervisory regime applying to e-money institutions, e-money issuers are subject to more stringent provisions than those applying to other credit institutions, notably as regards restrictions on the business activities they may carry on and, particularly, prudent limitations of their investments aimed at ensuring that their financial liabilities related to outstanding electronic money are backed at all times by sufficiently liquid low risk assets[44].

Whereas some cases of failure of e-money institutions occurred, none of them appeared to have impacted any consumers detrimentally. A strong body of opinion therefore finds that the abovementioned stringent rules are disproportionate to the risks[45].

3. The third problem relates to **inconsistent waivers and passporting procedures**. Article 8 of the previous eMoney Directive gave Member States the possibility to allow their competent authorities to exclude the application of the Directive to certain small businesses and to institutions of which the e-money is only accepted by affiliates or by a small number of companies. Article 8 further provides that e-money institutions which have been granted such waiver, cannot benefit from the mutual recognition procedures.

The waiver possibility included in article 8 leaves room for appreciation and therefore creates legal uncertainty. Again, the question arises which exact number of entities is required to accept the e-money, and precisely what sort of relationship needs to exist between issuer and accepting merchants, for an institution to qualify for a waiver[46].

In addition, substantial differences exist in the implementation of the waiver provision by the different Member States. Several Member States did not implement the provision at all, while others limited the implementation to some criteria included in article 8. Some Member States even imposed additional conditions. Among those Member States that have implemented article 8, important divergences exist between the application process for a waiver and the "waivable" provisions[47].

Whereas the Commission intended to create a legal framework that would enhance competition[48], evidence suggests that the inconsistent application with respect to waivers between Member States creates competitive distortions within national borders[49].

4. It is **problematic for e-money institutions to be profitable**, since article 1.5 of the previous eMoney Directive strictly limits the type of activities e-money institutions may perform. In addition to issuing e-money, these institutions may only provide closely related financial and non-financial services, and the storing of data on the electronic device. The issuance of e-money at a premium is thus, practically, the only source of return for e-money issuers[50].

---

[43] P. ATHANASSIOU and N. MAS-GUIX, *o.c.*, p. 22

[44] Recital 12 of the previous eMoney Directive

[45] Commission Staff Working Document on the Review of the E-money Directive, *o.c.*, p. 5

[46] See also third element of the definition of "electronic money"

[47] Final Report on the Evaluation of the E-money Directive, *o.c.*, p. 59 et seq.

[48] See section 3.1.1 on p. 6

[49] Commission Staff Working Document on the Review of the E-money Directive, *o.c.*, p. 6

[50] P. ATHANASSIOU and N. MAS-GUIX, *o.c.*, p. 27

Consequently, e-money institutions mostly gain their profits from transaction fees. Only by charging transaction fees to merchants and/or consumers, e-money institutions can be profitable. A second consequence of the restriction of activities is the need for so-called "hybrid" companies to split up their activities into separate legal entities. This often constitutes a very costly and inefficient process.

3.2. New eMoney Directive

3.2.1. Overview

The new eMoney Directive[51] has been adopted on 16 September 2009, and Member States are required to implement the Directive by 30 April 2011.

In its proposal for the new Directive, the Commission recognised the shortcomings of the previous Directive. The Commission found that e-money is still far from delivering its full potential benefits, and that some provisions of the previous eMoney Directive seem to have hindered the take-up of the e-money market. The Commission therefore proposed to focus on modernising the eMoney Directive[52].

3.2.2. Issues addressed

The text of the new eMoney Directive indeed addresses several of the issues under the previous eMoney Directive.

1. The new Directive has **clarified the scope** of the Directive. Article 1.5 of the new Directive provides that it shall not apply to the situations described in article 3(l) of the Payment Services Directive, which states that it "*shall not apply to services based on any telecommunication, digital or information technology (IT) device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services".*

It was further clarified by the first reading of the European Parliament that this exception envisages "*the situation where a mobile phone or other digital network subscriber pays the network operator directly and there is neither a direct payment relationship nor a direct debtor-creditor relationship between the network subscriber and any third-party supplier of goods or services delivered as part of the transaction"* [53].

As indicated by article 1.5 of the new Directive, the same exception – which describes the negative scope of the Directive – has been included in identical wording in article 3(l) of the Payment Services Directive. Consequently, payments relating to the purchase of digital services such as ring tones, music or digital newspapers which are sent to a mobile phone (or some other digital device e.g. a computer) are not covered by the new eMoney Directive and the Payment Services Directive when the telecom provider does not act as a mere intermediary[54].

---

[51] 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 repealing Directive 2000/46/EC, *OJ* L 267, 10 October 2009, p. 7

[52] Proposal for a new E-money Directive, COM(2008) 627 final, p. 2

[53] Recital 6 of the Proposal for a new E-money Directive, EP First reading, 24 April 2009, available at www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P6-TA-2009-0322

[54] Europe Press Release, *Payment Services Directive: Frequently Asked Questions*, 24 April 2007, MEMO/07/152

The scope of the new Directive is further clarified by the exception included in article 1.4, which provides that it shall not apply to the situation set out in article 3(k) of the Payment Services Directive. Accordingly, the new Directive *"shall not apply to services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under commercial agreement with the issuer, either within a limited network of service providers or for a limited range of goods or services".*

This additional exception clarifies to a certain extent the third element of the e-money definition under the previous eMoney Directive: *"accepted as means of payment by undertakings other than the issuer"*. The new eMoney Directive gives a hint as to the number of undertakings required ("a limited network"), and the required relationship between the issuer and such undertakings ("under commercial agreement") to fall outside its scope.

2. The new eMoney Directive also acknowledges the need to **clarify the application of redeemability requirements**. In its proposal for the new Directive, the Commission stated that consumers should have the right to redeem funds at all times[55]. Article 11.3 of the new Directive now provides that the contract between issuers and electronic money holders must clearly and prominently state the conditions of redemption, including any fees relating thereto. The electronic money holder must be informed of these conditions before being bound by any contract or offer.

Articles 11.4 and 11.7 of the new Directive further specify that redemption of a consumer may only be subject to a fee, if stated so in the contract between the issuer and the consumer, and only in one of the following cases:

- redemption is requested before termination of the contract;
- the contract provides a termination date and the consumer terminates the contract prior to that date; or
- redemption is requested more than one year after the date of termination of the contract.

3. Article 6 of the new eMoney Directive **extends the possibility to deploy other activities** for e-money institutions. In addition to the provision of payment services, operation of payment systems, granting of credit and the provision of closely related services, e-money institutions may also pursue business activities other than the issuance of e-money, having regard to applicable Community and national law. This possibility to perform additional activities is subject to the requirement of safeguarding any deposited money.

4. Finally, the new eMoney Directive further **clarifies the prudential rules**. The Commission found the previous prudential rules to be excessive with regard to the risk of the activity. The initial capital requirement has been lowered from 1 million EUR to 350 000 EUR[56], and the ongoing capital requirements have been replaced with new methods of calculation, based on the nature and the risk profile of e-money institutions[57].

3.2.3. *Evaluation*

The new eMoney Directive seems to resolve a number of important issues under the previous eMoney Directive. Nonetheless, the question arises whether all issues have been resolved, especially with respect to the scope exceptions included in the Directive. (Note: as these exceptions are also included in

[55] Article 5 of the Commission Proposal for a new E-money Directive

[56] Article 4 new E-money Directive

[57] Article 5 new E-money Directive

identical wording in the Payment Services Directive, this section equally applies to the Payment Services Directive.)

Limited network of service providers – Article 1.4 of the new eMoney Directive and article 3(k) of the Payment Services Directive hold that the Directives shall not apply to services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under commercial agreement with the issuer, either within a limited network of service providers or for a limited range of goods or services. Recital 5 adds that *"An instrument should be considered to be used within such a limited network if it can be used only either for the purchase of goods and services in a specific store or chain of stores, or for a limited range of goods or services, regardless of geographical location of the point of sale. Such instruments could include store cards, petrol cards, membership cards, public transport cards, meal vouchers or vouchers for services (such as vouchers for childcare, or vouchers for social or services schemes which subsidise the employment of staff to carry out household tasks such as cleaning, ironing or gardening), which are sometimes subject to a specific tax or labour legal framework designed to promote the use of such instruments to meet the objectives laid down in social legislation."*

However, the criteria for what constitutes a "*limited"* network are still not entirely clear. The questions arises which number of service providers exceeds the threshold for being qualified as a "limited" network (four service providers, five or thirty-five?). A similar question arises with respect to a *"limited"* range of goods or services. For example, does a payment instrument which allows to pay for any type of software constitute a limited range of goods or services? As the preparatory works of the Directives provide little or no guidance for the interpretation of the concept "limited", a clarification will need to be provided by case-law.

It is also unclear what exactly is meant by a "commercial agreement with the issuer". The question arises whether a mere formal agreement is sufficient to fall within the scope of this exception, or whether a certain balanced content of such agreement is required.

Value added services – Article 1.5 of the new eMoney Directive and article 3(l) of the Payment Services Directive provide that the Directives shall not apply to services based on any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services.

This exception is particularly vague, but seems primarily intended to allow telecom providers to sell ringtones, wallpapers, games and similar content for cell phones, without becoming subject to the requirements of the E-money or Payment Services Directive. However, the broad wording ("*any telecommunication, digital or IT device*") and limited conditions for the exception to apply (it suffices that the provider *does not act only* as an intermediary), seem to entail that this exception also applies to other services. It appears that the only requirement is that the supplier providers additional services, beyond the payment service. The question is, however, as from which moment a provider becomes more than a mere intermediary. Is it sufficient to offer a "web portal" or search engine through which customers can select products or services? Is it sufficient for a network operator to install a customer complaint line, through which customers can cancel a transaction? Both cases illustrate that, due to the sheer lack of guidance in this regard, case law will likely diverge between Member States.

It is therefore likely that this provision creates a loophole for numerous service providers, and vagueness for many other service providers. For example, several new e-shops for smartphones have been

launched during the previous months, such as the Apple iTunes shop for iPhone[58]. The service providers of these e-shops do not act only as financial intermediaries, but also provide software back-ups, selection tools, user reviews and ratings, digital shop windows, etc. Consequently, these service providers could fall within the exception of article 1.5 the new eMoney Directive and article 3(l) of the Payment Services Directive. This new type of e-shop is increasingly popular, is starting to become a "platform" which acts as a central hub between consumers and content providers, and consumers often deposit and store large amounts of money in their online accounts for these e-shops. Whereas it could be acceptable to subject this type of service providers to a waiver regime when only small amounts are stored in each account, it should be avoided that they completely fall outside the scope of the Directives. Further, both with respect to the exception relating to limited networks and the exception regarding value added services, it is unclear whether money used in virtual worlds and online platforms (such as the hi5 coins system and the Nintendo Wii Points Card) falls within the scope of the exception. A more detailed analysis is set out in sections 4.4 and 4.7.

Mobile payments – As discussed above, it is not clear to which extent mobile payments relating to the purchase of ringtones, wallpapers, games and similar content for cell phones from telecom providers, fall within the scope of the new eMoney Directive.

On the other hand, similar types of typical mobile payments, such as the purchase of parking tickets or public transportation tickets via SMS, will be subject to the provisions of the eMoney Directive[59]. Contrary to mobile payments relating to ringtones and similar content, such payments cannot fall within the scope of the value added services exception, since they do not relate to goods or services purchased which are to be used through a telecommunication, digital or IT device.

Accordingly, telecom operators issuing prepaid cards which can be used for such payments, will be considered as issuers of e-money, and hence, will need to comply with the eMoney Directive. This entails that telecom operators are, *inter alia*, subject to the limitation to deploy other activities, and are thus often forced to establish a separate entity for the purposes of issuing prepaid cards.

Waivers – As is the case for the previous eMoney Directive, waivers will only apply on a Member State level under the new eMoney Directive. Furthermore, waivers do not exempt payment providers from all obligations of the eMoney Directive (national supervising authorities can decide which prudential rules, capital requirements, fund requirements and safeguarding requirements do not apply to a particular e-payment provider).

While waivers significantly reduce the administrative and regulatory burden for new e-payment providers, they do not reduce this burden entirely, as e-payment providers must still prepare and submit files to the national supervisory authority, must initiate discussions with the supervising authority, and possibly change some aspects of its intended payment scheme due to recommendations of the authority. While this is still manageable on a national level, it becomes prohibitive when the waiver must be requested in many Member States.

> ***Practical example: anonymous e-payment cards.*** *A Belgian start-up company was looking to enter the market of e-payments with an innovative, user-friendly e-payment scheme. The scheme would allow for anonymous online payments, by allowing customers to buy pre-paid scratch cards in local shops (e.g., a supermarket). The special code on the scratch card would then be entered into an online account, through which online payments can be made to affiliated online merchants.*

[58] Other examples include Google Android Market, BlackBerry App World, Nokia Ovi shop, Java shop as announced by Sun and Microsoft app store.

[59] to the extent made with prepaid cards

The company spent over 80,000 EUR in legal fees, of which over 50,000 EUR was spent on preparing the waiver and investigating the costs and benefits of a full e-money license (eventually a waiver for Belgium was obtained). An important part of the remaining 30,000 EUR was spent on other regulatory issues (including consumer protection issues), to which any company dealing with sensitive products and services is generally subject.

These costs were, obviously, almost prohibitive to a new start-up, for which the cash flow in the start-up phase is problematic due to a "chicken-and-egg" problem of attracting at the same time sufficient customers and merchants.

Considering the crucial importance of having EU-level waivers, we are of the opinion that a second waiver scheme must be introduced, in addition to – or as a replacement of – the current optional, national waiver scheme set forth in article 10. This waiver scheme would apply on an EU-level, and would consist of a mere notification duty (similar to the notification duty for internet access providers[60]), whereby e-payment providers would be exempted from all financial regulations in the Payment Services Directive and eMoney Directive. However, in order to strike balance with consumer interests, this waiver scheme would only apply when the individual account held by each user, stores a maximum value of 150 EUR.

3.3. Payment Services Directive

3.3.1. Overview

The Payment Services Directive[61] intends to establish a modern and harmonised legal framework to enable payments to be made more quickly and easily throughout the whole EU[62]. The Payment Services Directive constitutes an attempt to remove legal obstacles for the creation of a Single Payments Market, so as to enhance payment system competition and the creation of economies of scale. The Directive further intends to boost consumer confidence in payment systems such as electronic payments[63]. As is the case with the eMoney Directive, the Payment Services Directive intends to achieve a balance between consumer protection and market liberalization[64].

3.3.2. Relation to e-money

In its Staff Working Document on the review of the eMoney Directive, the Commission acknowledged the need to ensure consistency between the eMoney Directive and the Payment Services Directive[65]. Considering the direct linkages between these two legal acts, and bearing in mind the undesirability of a

---

[60] Article 3 of Directive 2002/20 on the authorisation of electronic networks and services provides that Member States may require internet access providers to submit a notification prior to beginning their activities.

[61] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, *OJ* L 319, 5 December 2007, p. 1

[62] Europe Press Release, *Payment Services Directive: Frequently Asked Questions*, 24 April 2007, MEMO/07/152

[63] S. MERCADO-KIERKEGAARD, "Harmonising the regulatory regime for cross-border payment services", *Computer Law & Security Report* 2007, 23, p. 177

[64] *Ibid.*, p. 177

[65] Commission Staff Working Document on the Review of the E-money Directive, p. 14

proliferation of directives dealing with similar or overlapping issues (namely, payment services), it is a lost opportunity that the new eMoney Directive was not incorporated in the Payment Services Directive[66].

Even so, it should be noted that the new eMoney Directive is clearly drafted to complement the Payment Services Directive, and to exclude any contradictions and overlapping issues between both directives.

3.3.3. *"Payment institutions"*

The Payment Services Directive introduces a new category of service providers which are subject to a different prudential regime than e-money institutions and credit institutions, namely the payment institutions. Payment institutions are legal persons that have been granted authorisation to operate in accordance with Article 10 of the Payment Services Directive, and which execute payment services.

A list of services which are considered as "payment services" has been included in an Annex to the Directive, and includes, *inter alia,* services enabling cash to be placed and to be withdrawn from a payment account, the execution of payment transactions and money remittance. Payment institutions cannot use the funds received from payment service users and specifically accepted in connection with a payment service to support other business activities other than payment services[67].

This new category was introduced to remove legal barriers to market entry and to establish a single license for all providers of payments services which are not connected to taking deposits or issuing e-money[68]. The general underlying purpose of the introduction of this category is to remove the black economy by registering the identity and whereabouts of all persons providing payment services[69].

4. Types and modalities of electronic payments

This section assesses the legal issues under the new eMoney Directive and the Payment Services Directive with respect to electronic payment schemes frequently used in today's society, as well as an assessment of several modalities of e-payments.

4.1. Smart cards

4.1.1. *Overview*

A first type of e-money consists of so-called "electronic purses" in the form of smart cards. These cards resemble other types of plastic money, except that they have an electronic microchip embedded in a small gold plate in front of the card rather than a magnetic strip in the back[70]. Smart cards for e-payments use the microchip to store a certain amount of value by use of encryption algorithms that can only be decoded by an adequate reader[71].

---

[66] P. ATHANASSIOU and N. MAS-GUIX, *o.c.*, p. 37

[67] S. MERCADO-KIERKEGAARD, *o.c.*, p. 181

[68] *Ibid.*, p. 180

[69] *Ibid.*, p. 181

[70] R. GUTTMAN, *o.c.*, p. 112

[71] A. GUADAMUZ, *Electronic Money: A viable payment system?*, p. 3, available at http://www.era.lib.ed.ac.uk/bitstream/1842/2255/1/electronicmoney.pdf

These card-based e-purses are generally intended for small payments. They allow the payment of exact amounts at unstaffed locations such at vending, parking and ticketing machines[72]. Smart cards can also be used for online purchases if the consumer has a card reader attached to their computer. This card reader will unlock the value in the card and send the information to the online retailer, facilitating an anonymous e-commerce transaction[73].

The smart-card-based electronic wallet is known as Proton in Belgium, as Avant in Finland, Danmont in Denmark, Chipknip in the Netherlands, MEP in Portugal, Minipay in Italy, Minicash in Luxembourg, Moneo in France, Monedero 4B in Spain and GeldKarte in Germany[74]. Whereas smart cards have been relatively successful in the Benelux countries, the take-up in most other European countries has been slow[75].

4.1.2. Legal assessment

There never seems to have been any doubt or dispute as to whether smart cards constitute e-money under the previous eMoney Directive. The modifications brought by the new eMoney Directive do not entail any additional terms or conditions that would change this situation.

Smart card providers often benefit from a waiver granted by their national authority under article 8 of the previous eMoney Directive. For example, the e-money institutions operating under a waiver in Germany include a smartcard scheme in a sports stadium[76].

4.2. Server based e-money

4.2.1. Overview

Server based e-money was developed almost simultaneously with the rise of card-based e-money, driven by the opportunities offered by the Internet[77]. The most successful server based e-money systems consist of pre-funded personalised payment schemes, involving the transfer of funds stored on a personalised online account[78], similar to bank deposits. Server based money can be accessed via websites, e-mail or SMS. The innovative nature of these schemes lies in the fact that accounts can be opened and money can be sent by simple use of e-mail addresses or mobile phone numbers[79].

The most well-known and successful example of server based e-money is PayPal, an online payment system launched in the US in 1999. The main reason for its success lies in the fact that it suffices for online vendors to have an e-mail address and a PayPal account in order to receive payments; it excludes a complex credit card processing system as a prerequisite for online trading. Also, the PayPal system does not require consumers to transfer their credit card number to unknown vendors, as PayPal acts as a secure third party facilitating the payment.

---

[72] Final Report on the Evaluation of the E-money Directive, p. 22

[73] A. GUADAMUZ, *o.c.*, p. 3

[74] S. HENG, *o.c.*, p. 6

[75] European Central Bank, *E-payments without frontiers, o.c.*, p. 49

[76] Final Report on the Evaluation of the E-money Directive, p. 37

[77] *Ibid.*, p. 29

[78] *Ibid.*

[79] European Central Bank, *E-payments without frontiers, o.c.*, p. 48

4.2.2. *Legal assessment*

The previous eMoney Directive was very unclear as to whether server based e-money falls within its scope. In the new eMoney Directive, the Commission clarified that *"the definition* [of electronic money] *should cover electronic money which is (…) stored remotely at a server and managed by the holder through a payment account with the payment service provider"* [80]. The new definition of e-money now provides that e-money is *"stored electronically"*, hence clarifying that server based e-money falls within the scope of the new eMoney Directive.

Server based e-money may fail to meet the requirement of security, which was identified as an essential requirement for the success of electronic payment schemes. Although account based systems such as PayPal cannot be hacked in the same way as smart card technology, they do suffer from other security threats, for example, a type of online fraud known as "phishing" [81].

4.3. Disposable and virtual pre-funded cards

4.3.1. *Overview*

Disposable and virtual pre-funded cards are a type of server based e-money which physically appear in the form of a card. Contrary to smart cards, the deposited funds are not stored on the card itself, but on a server. They typically imply a transfer of centrally stored anonymous claims that have been purchased in advance[82]. These cards are often issued as scratch cards with a hidden identifying number, or sent as virtual cards via SMS. The received number must be entered into the issuer's website to activate the anonymous "card account", or can be used directly for paying at a content provider's website[83].

These disposable and virtual pre-funded cards typically target individuals that do not possess debit or credit cards (such as minors) and persons who wish to remain anonymous when making online purchases. Accordingly, they are being used increasingly in niche markets such as online entertainment, including gaming and adult entertainment[84].

Examples include PaySafeCard in Austria and Germany and SNAP Card and SplashPlastic in UK[85].

4.3.2. *Legal assessment*

This type of cards addresses the essential requirement of privacy and allows consumers to make anonymous purchases. As a form of server based e-money, these disposable and virtual pre-funded cards fall within the scope of the new eMoney Directive[86].

---

[80] Proposal for a new E-money Directive, COM(2008) 627 final, p. 11

[81] See Chapter 11 - Cybercrime

[82] European Central Bank, *E-payments without frontiers, o.c.*, p. 48

[83] *Ibid.*

[84] Final Report on the Evaluation of the E-money Directive, p. 30

[85] *Ibid.*

[86] See section 4.2.2

4.4. Platform payment systems

4.4.1. Overview

"Platform payment systems" concern payment systems and virtual wallets created by online platform operators, which allow users of the platform to purchase various goods, usually (but not necessarily) related to the platform itself.

For example, social communities often allow their users to store money on their user accounts, in order to purchase digital services related to the community (*e.g.,* tokens to buy applications to be displayed on the user's home page and tokens to pay for premium places). An example of platform payment systems include the hi5 coins system and the Wii Points Card which can be purchased from local Nintendo retailers or via the Wii Shop.

Shops such as Apple iTunes and the Google Android Market can also be qualified as a type of platform payment systems, as these shops are increasingly becoming a central services hub that connects content providers to content consumers.

4.4.2. Legal assessment

The question arises whether such platform payment systems fall within the scope of the new eMoney Directive and the Payment Services Directive, taking into account the scope of the exceptions relating to "limited networks" of service providers and value added services[87].

Limited networks exception – Article 1.4 of the new eMoney Directive and article 3(k) of the Payment Services Directive provide that the Directives shall not apply to services based on instruments that can be used to acquire goods or services only within limited networks or for a limited range of products of services. The question arises whether the network of providers offering their services via a platform constitutes a *limited network*, similar to a chain of stores[88]. Similarly, it is unclear whether the limited range of payable services and products offered via such platforms qualify as a *limited range* of goods or services.

Value added services exception – As regards value added services, article 1.5 of the new eMoney Directive and article 3(l) of the Payment Services Directive provide that the Directives shall not apply to service providers that do not merely act as an intermediary. Platform operators generally provide several services other than payment services. It is unclear, however, which criteria should be used to determine whether such services should be considered as additional services within the meaning of the article 1.5 of the new eMoney Directive.

Receipt of funds – Also, the definition of e-money as included in article 2.2 of the new eMoney Directive provides that products must be "*issued on receipt of funds*" to qualify as e-money. Accordingly, platforms that allow collection of credits or points by performing certain activities distinct from the direct purchase of such credits or points, fall outside the scope of EU e-money legislation. The question arises then what is the status of platforms where the same credits or points can be both purchased and earned, since these platforms generally store purchased and earned credits in one user account.

---

[87] See section 3.2.3

[88] Recital 5 of the Commission Proposal for a new E-money Directive: *"An instrument should be considered to be used within a 'limited network' if it can be used only for the purchase of goods and services in a specific store, a chain of stores (…) Instruments which can be used for purchases in stores of listed merchants should not be exempted as such instruments are typically designed for a network of service providers which is continuously growing."*

4.5. Mobile payment systems

4.5.1. Overview

A large variety of mobile e-payment schemes have been developed. One can distinguish between schemes that are funded via a prepaid account and schemes that are added to telephone bills ("post paid"). These mobile payment systems can either debit payments from the holder's credit card or from his bank account.

Mobile transactions can also be carried out via e-money schemes. Such e-money can either be integrated into mobile devices, or can be stored on a card or server[89]. Mobile payment schemes are typically popular with minors, to performs purchases of limited value, such as the purchase of ringtones.

Another distinction to be made is between **proximity** payments and **distance payments**. The first type of mobile payments allows contactless transmission of the payment order, for example via radio frequency, as is used in public transportation[90]. These represent one of the most important innovations in the banking system, increasing speed, simplicity and convenience when purchasing goods[91]. The distance type of mobile payments usually requires the help of an SMS or automatic voice message.

So far, there is little progress visible on the standardisation and interoperability of payment solutions between mobile network operators in the national markets, and even less at the European level[92].

4.5.2. Legal assessment

The application of the previous eMoney Directive to **prepaid payment services** by mobile operators for third party offerings was controversial[93]. In implementing the Directive at national level, some Member States decided that in certain circumstances, by supplying pre-paid phone cards, mobile operators in practice issue electronic money and that therefore they should comply with existing EU rules concerning its issuance[94]. However, other Member States found that mobile operators should not be considered as e-money institutions.

To avoid further impediments to the Internal Market, caused by these divergent interpretations, the Commission carried out an analysis in 2003 so as to establish a common interpretation. According to that analysis, prepaid phone cards are covered by the Directive when the electronic value stored on them is used to purchase products and services offered by third parties (such as ring tones, news, games, CDs, books and ticketing services) rather than directly by the phone companies[95].

Value added services exception – The new eMoney Directive further clarifies the issue of mobile operators, by introducing an exception relating to value added services. Payments relating to the purchase of digital services such as ringtones or music which are sent to a mobile phone, are not covered by the eMoney Directive, nor by the Payment Services Directive when the telecom operator

---

[89] European Central Bank, *E-payments without frontiers, o.c.*, p. 52

[90] For example, Oyster in London

[91] D. SHANNON, "The emergence of prepaid cards in Europe", *Card Technology Today,* Volume 20, Issue 4, April 2008, p. 11

[92] European Central Bank, *E-payments without frontiers, o.c.*, p. 52

[93] *Ibid.*, p. 39

[94] EU Press Release, *Electronic money: Commission consults on how the E-Money Directive applies to mobile phone services*, 10 May 2004, IP/04/620

[95] *Ibid.*

does not act as a mere intermediary. However, as pointed out above, this new exception is highly ambiguous, and promises to introduce a significant level of legal uncertainty.

Security and privacy – Another legal issue is that proximity contactless payments using RFID technology raise several security and privacy related issues. Traditional credit cards require visual access or direct physical contact for retrieving information such as the cardholder's name and the credit-card number. RFID technology on the other hand makes these and other sensitive data available via radio frequency[96].

For example, a study of sample RFID credit cards found that the cardholder's name, card number and expiration are often leaked to unauthenticated readers, and that RFID-enabled credit cards are susceptible to a range of traditional RFID attacks such as skimming and relaying[97]. In addition to this risk of unauthorised disclosure of personal data, the potential exists for this technology to be used to monitor individuals via the RFID applications they hold[98].

Although RFID operators are already subject to the strict security requirements set out in the Data Protection Directive and the consumer protection requirements set out in the Payment Services Directive, the risks created by RFID payment applications illustrate the need for additional standards. In this respect, the Commission recognised that RFID will only be able to deliver its economic and societal benefits if effective measures are in place to safeguard personal data protection and privacy. It therefore recommended that Member States should ensure that operators take appropriate technical and organisational measures to ensure the protection of personal data and privacy[99].

4.6. Vouchers and gift cards

4.6.1. Overview

Building on the popularity of frequent-flier miles and coupons, a number of internet start-ups started designing their own online currencies for use as a marketing tool to attract more customers to sites and entice them to shop there[100]. Similarly, different issuers of paper vouchers and gift cards showed an interest in switching their products to an electronic format[101]. As such, electronic coupons, vouchers and gift cards emerged, which can be used to purchase products and services from participating merchants.

Electronic vouchers and gift cards are one of the strongest growth markets for prepaid cards, particularly because they allow parents to enable their children to pay for services online without the use of an adult's credit card[102]. Typical examples of electronic gift cards include the iTunes Gift Card and Amazon Gift Card, which can both be bought online.

Vouchers and gift cards are very similar to smart cards and disposable and virtual pre-funded cards. However, they are typically obtained as a present or via a third party other than the issuer. In addition,

---

[96] T.S. HEYDT-BENJAMIN et al, *Vulnerabilities in First-Generation RFID-enabled Credit Cards*, October 2006, p. 2, available at prisms.cs.umass.edu/~kevinfu/papers/RFID-CC-manuscript.pdf

[97] *Ibid.*

[98] Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, (C(2009) 3200 final)

[99] *Ibid.,* p. 3 and 6

[100] R. GUTTMAN, *o.c.*, p. 124

[101] Final Report on the Evaluation of the E-money Directive, p. 33

[102] D. SHANNON, *o.c.*, p. 12

vouchers and gift cards are not always issued on receipt of funds. They may also be acquired by performing certain activities, such as collecting points or bringing in new customers.

4.6.2. *Legal assessment*

There is considerable legal uncertainty as regards the question whether electronic vouchers and gift cards constitute e-money under the previous eMoney Directive. In principle, they seem to fulfil all criteria of the definition. However, some of their inherent features are incompatible with the Directive, such as the redeemability requirement included in article 3, which provides that *"a bearer of electronic money may, during the period of validity, ask the issuer to redeem it at par value in coins and bank notes or by a transfer to an account"* [103].

Under the new eMoney Directive, vouchers and gift cards will generally not fall within its scope, pursuant to the limited network exception, which exempts *"instruments that can be used to acquire goods or services only in the premises used by the issuer or under commercial agreement with the issuer, either within a limited network of service providers or for a limited range of goods or services"*[104]. Vouchers and gift cards can typically only be used for products and services of a limited number of participating merchants.

In its first reading, the European Parliament further clarified that social vouchers — such as vouchers for services such as childcare vouchers, or services voucher schemes which subsidise the employment of staff to carry out household tasks — should not be covered by the Directive. The agreed text of the Directive emphasises that, where such a specific purpose instrument develops into a general purpose instrument, the exemption should no longer apply[105].

4.7. Money in virtual worlds

4.7.1. *Overview*

Similar to platforms such as Netlog and hi5, virtual worlds have created their own currency which allows their users to operate within their world. The most well-known virtual world is Second Life, an online 3D world imagined and created by its residents. Within Second Life, there is a marketplace where residents trade virtual goods and services. The Second Life economy has become one of the world's largest user-generated virtual economies[106].

Transactions within Second Life are based on the Linden dollar, Second Life's own virtual micro-currency. Residents can buy and sell Linden dollars on LindeX, the official virtual currency exchange of Second Life. Linden dollars may also be freely distributed, at Second Life's operators' discretion. It is also interesting to note that the Second Life Terms of Service further clearly state that *"Second Life 'currency' is (…) not redeemable for monetary value from Linden Lab"* [107].

---

[103] Final Report on the Evaluation of the E-money Directive, p. 33

[104] Article 1.4 new eMoney Directive, which refers to article 3(k) of the Payment Services Directive

[105] Recital 5 of the Proposal for a new E-money Directive, EP First reading, 24 April 2009

[106] See http://secondlife.com/whatis/marketplace.php

[107] See http://secondlife.com/corporate/tos.php

4.7.2. *Legal assessment*

The question arises whether currencies created by virtual worlds, such as the Linden dollars, fall within the scope of the new eMoney Directive. As regards the definition, virtual world currencies seem to comply with all criteria: they are stored electronically, are issued on receipt of funds, for the purpose of making payment transactions, and are accepted by other residents, *i.e.* natural or legal persons other than the issuer.

Limited network exception – It is, however, not clear whether virtual worlds which issue their own money, fall within the scope of the exception set out in article 1.4 of the new eMoney Directive and article 3(k) of the Payment Services Directive. These articles provide that the Directives shall not apply to services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under commercial agreement with the issuer, either within limited networks or for a limited range of products of services.

Furthermore, it is unclear whether a virtual world can be considered as "premises" in the sense of these articles. Similar to meal vouchers issued by a building owner that can only be used within such building, money issued by virtual worlds can typically only be used within that community.

The question also arises whether the other residents of a virtual world offering their products and services constitute a *limited network.* Similarly, it is unclear whether the limited range of payable services and products offered via such virtual worlds qualify as a *limited range* of goods or services.

Value added services exception – As regards value added services, article 1.5 of the new eMoney Directive and article 3(l) of the Payment Services Directive provide that the Directive shall not apply to service providers that offer additional services beyond the payment service. The services that are offered by virtual worlds in addition to any payment services, generally constitute services that are delivered to and are to be used through a computer. It is, however, unclear whether virtual worlds therefore fall outside the scope of the new eMoney Directive and Payment Services Directive.

Receipt of funds – Finally, the definition of e-money as included in article 2.2 of the new eMoney Directive provides that products must be "issued on receipt of funds" to qualify as e-money. The question arises as to what is the status of money issued by virtual worlds if it is not necessarily and not always issued on receipt of funds.

4.8. Escrow services

4.8.1. *Overview*

Issue – Contrary to point-of-sale transactions, remote transactions imply by definition a time interval between payment and delivery of goods, and hence, create a conflict of interest between buyer and seller. Neither party is interested in transferring its assets (be it money or goods), before receiving the other party's agreed asset. This conflict is especially pertinent in an online context, where the remote nature of transactions is often accompanied by unknown or anonymous trade partners, which aggravates the lack of trust between trade partners.

Online consumer-to-consumer environments in particular pose serious challenges to trust between trade partners. For example, an online auction such as eBay allows its users to remain nearly completely anonymous, which facilitates fraud. Although these platforms often take trust enhancing measures, such as the eBay feedback system, consumers' trust remains very low.

Solution – A solution to the diverging interests of buyers and sellers, be it consumers or merchants, is the use of Trusted Third Parties (TTP) as intermediaries to the transaction. A TTP can overcome the lack of synchronisation of delivery of the goods and payment[108]. Buyers can submit their payment to a TTP, which will only release the payment to the seller upon receiving the buyer's confirmation of receipt of the goods. Hence, the benefit of TTP intermediaries lies in the reduction of fraud possibilities. However, they also entail increased transaction costs.

An example of a TTP escrow service provider is escrow.com, which is eBay's approved escrow service. Local escrow service examples include Pay&Deliver in Belgium, PayDutch in the Netherlands and Iloxx in Germany.

4.8.2. Legal assessment

Online escrow services may be subject to the Payment Services Directive, depending on their underlying transaction scheme. If, and to the extent, the TTP operates as a mere escrow agent, its services shall not be considered as payment services. For example, in the Pay&Deliver scheme, the buyer's payment is transferred to an account which is administered by a third party, legally independent from Pay&Deliver. Hence, the payment is not executed by Pay&Deliver.

However, if the TTP actually effects the payment, such service will be qualified as a payment services as defined in the Payment Services Directive. Consequently, the TTP will be considered as a payment institution, and be subject to the authorisation as set out in the Payment Services Directive.

5. Comparison with the United States

MSB state laws – In the United States, regulation of non-bank financial service providers has been left to state banking regulators. A majority of the U.S. states has laws for so-called money services businesses (MSBs), which are non-banks that provide money services. As regards e-payment intermediaries, states have generally modified their existing regulatory frameworks for MSBs, rather than implementing a new legislative framework to deal with the specificities of e-payments[109]. MSBs (including e-payment providers) operating in the United States, must comply with the laws of each state in which they operate.

UMSA – As these state laws vary considerably in their requirements imposed on MSB's[110], the National Conference of Commissioners on Uniform State Laws (NCCUSL)[111] approved the Uniform Money Services Act (UMSA)[112] in 2000.

The UMSA contains a recommended common framework for licensing and regulating MSBs, including e-payment providers, throughout the different states in the United States[113].

---

[108] European Central Bank, *E-payments without frontiers, o.c.*, p. 32

[109] J.K. WINN (ed.), *Consumer Protection in the Age of the 'Information Economy',* Ashgate, 2006, p. 322

[110] NCCUSL, *Uniform Money Services Act with prefatory note and comments,* p. v, available at www.law.upenn.edu/bll/ulc/moneyserv/ms00ps.htm

[111] The NCCUSL is a body of lawyers, judges, and law professors, typically appointed by the governor of each state. Although influential, the NCCUSL does not have any direct legislative power itself; uniform acts become laws only to the extent they are enacted into law by state legislatures.

[112] Text available at www.law.upenn.edu/bll/ulc/moneyserv/ms00ps.htm

[113] *Ibid.*, p. 324

Stored value – Similar to the EU e-money concept, the UMSA defines "stored value" as monetary value that is evidenced by an electronic record, whereby "monetary value" is a medium of exchange, whether or not redeemable in money[114]. The comments to the UMSA further state that "medium of exchange" connotes that the value that is being exchanged be accepted by a community, larger than the two parties to the exchange.

The comments to the UMSA further specify that, with Internet payments, the regulators will also have to make the same type of determination as to when a certain type of monetary value has become widely accepted as to constitute a medium of exchange. As regards Internet payment systems that involve Internet scrip or points (*e.g.,* frequent flier or bonus points), it will be up to the state regulators to grapple with how widely circulating such points are, whether they are redeemable, and whether they can be used to purchase or acquire a wide range or products and services.

This definition of stored value is very similar to the definition of e-money under EU laws. In fact, the comments to the UMSA even explicitly refer to the eMoney Directive with respect to stored value. However, other than the eMoney Directive, and as indicated by the definition of monetary value, UMSA does not require stored value to be redeemable.

Money transmission – "Money transmission" is defined as the selling or issuing of payment instruments, stored value, or receiving money or monetary value for transmission (excluding the provision solely of delivery, online or telecommunications services, or network access)[115].

The comments to the UMSA clarify that Internet payment services that hold customer funds or monetary value for their own account rather than serve simply as clearing agents, fall within the definition of money transmission. However, entities that simply transfer money between parties as clearing agents fall outside the scope of a safety and soundness statute. The definition also excludes entities that solely provide delivery services (*e.g.,* courier or package delivery services) and entities that act as mere conduits for the transmission of data (such as internet access providers). These exclusions are similar to the exclusion set out in the new eMoney Directive[116].

Licensing and prudential supervisory regime – Similar to e-money issuers under EU law, money transmission business must obtain a license prior to commencing their activities[117]. As in the EU, this license needs to be obtained in each state in which a business operates, as UMSA is implemented on a state level, rather than on the federal level.

Although UMSA does not include any capital requirements, it does provide for a similar prudential supervisory regime as the eMoney Directive. Any business obtaining a license for money transmission, must be able to present a surety bond, letter of credit or other similar security acceptable, in the amount of $50.000, plus $10.000 per location, not exceeding a total of $250.000[118]. Section 701 UMSA further specifies that money transmitters are required to maintain a certain level of investments that is equal to the value of their outstanding obligations as a means of protecting individual consumers.

---

[114] Section 102 UMSA

[115] Section 102 UMSA

[116] Which states that it "*shall not apply to services based on any telecommunication, digital or information technology (IT) device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services"*

[117] Section 201 UMSA

[118] Section 203 UMSA

6. Comparison with Japan

Overview – In comparison with the EU, private players are rushing into e-payment systems in Japan. There are currently more than twenty different e-payment providers in Japan, which enjoy significant popularity. This success is attributed to a combination of factors, such as the ease of use[119], attractive bonus schemes[120], the possibility to make anonymous payments, and the suitability for small payment transactions[121].

Due to the relatively large amount of online payment providers, the providers are currently trying to build associations, in order to reduce fragmentation.

Legal framework – Japanese financial law makes a distinction between offline and online e-payments. While offline payment providers are currently subject to a prudential regime, online payment providers are not. However, online payment providers will soon also be subject to a prudential regime.

Evaluation – While an extensive comparison is beyond the scope of this study, it is important to recognise that – contrary to the EU – the Japanese e-payments market flourished. An important reason is that these e-payment providers were not subject to strict legal rules, and could develop their services without any regulatory burden. Japanese consumers have now adopted e-payment systems for various only payments, and the new regulatory framework will not likely change this situation. The reverse situation applies in the EU, where strict rules were enacted at the moment e-payment providers started to appear on the market.

7. Conclusions

1. The European framework for electronic money is **rapidly developing**. The 2007 **Payment Services Directive** is being implemented by Member States, and will enter into force in most Member States in November 2009[122]. The previous **eMoney Directive** has been revised, and the new eMoney Directive has been signed on 16 September 2009. Also, the recent Commission Recommendation regarding RFID technology illustrates that specific legislation relevant for **contactless mobile payments** is in the making. Given the state of development of all e-payment legislation, it is not yet possible to draw any general decisive conclusions as regards its implementation and application in practice.
2. As recognised by the Commission in its proposal for the new eMoney Directive, the **previous** e-payment legislation, drafted around the year 2000, contained many legal problems, such as the unclear definition of electronic money, the unclear scope of the Directive, a disproportionate prudential regime, inconsistent waivers and passporting procedures, and difficulties for e-money institutions to be profitable.
3. The revision of the eMoney Directive constitutes a prime example of the authorities' acknowledgment of the need for modernization of its legislation. However, some **ambiguities are still not resolved** by the new Directive (e.g., the question to which extent a prepaid mobile phone card is e-money when used), and several new ambiguities are introduced (such as the exemption

---

[119] customers only need to type in a 16-digit code in order to make a payment — no physical card or other multi-layered security system is used

[120] *e.g.*, receiving airmiles when using the e-payment systems

[121] *e.g.,* for buying a cell phone ringtone)

[122] An overview of the transposition of the Payment Services Directive is available at http://ec.europa.eu/internal_market/payments/framework/transposition_en.htm

for e-money used in a "limited network" of service providers, and the exemption for value-added services).

Furthermore, the new eMoney Directive does not fundamentally change the waiver regime, which still does not apply on a European level, and does not exempt the e-payment provider from all regulatory compliance issues. These **waivers are still too burdensome** in many cases: the exemption must be applied for on a national basis, and generally involve extensive administrative overhead for the e-payment provider.

4. As a result, the legal treatment of several types of e-payment services (particularly platform payment systems and mobile payment systems) is not clear. Interestingly, precisely these types of e-payment services seem to be the future of online payments.

5. We are therefore of the opinion that the improvements brought by the new eMoney Directive will not be sufficient to trigger an uptake of the e-payments market, and that **a more fundamental revision of the eMoney Directive is necessary**.

8. Recommendations

Taking into account that the Payment Services Directive is not yet transposed in all Member States, and its national rules will not enter into force until November 2009, and also taking into account the very recent adoption of the eMoney Directive, it should be noted that it is difficult to make general recommendations with respect to EU e-payment legislation.

Clarification of the scope of the eMoney Directive – As indicated throughout this document, the scope of articles 1.4 and 1.5 of the new eMoney Directive (relating to limited networks and value added services) is unclear, especially in relation to newly developing services (such as online platforms and virtual worlds). These articles must therefore be clarified, because the current rules will lead to much legal uncertainty for many emerging online payment services.

Add a new waiver scheme – We recommend to introduce an additional waiver scheme. Each waiver would automatically apply on an EU-level, and would consist of a mere notification duty (similar to the notification duty for internet access providers[123]), whereby e-payment providers would be exempted from (part of the, or ideally all) financial regulations in the Payment Services Directive and eMoney Directive. However, in order to strike balance with consumer interests, this waiver scheme would only apply when the individual account held by each user, stores a maximum value of 150 EUR.

Limiting this waiver scheme to a maximum stored value of 150 EUR significantly reduces the possible negative impact in case of fraud by the issuer, security breaches or other situations which could lead to a loss of the stored value. As such, the benefits of e-payment, which allows cheap and quick transactions, will most likely outweigh the risks entailed by the waiver regime. In this context, this waiver scheme must require payment operators to take all necessary measures to prevent customers from using multiple accounts, so as to avoid a bypass of the 150 EUR limit and to avoid an increased financial risk for customers.

Such a waiver scheme would be particularly relevant for telecom operators to the extent the value stored on their prepaid cards is limited to 150 EUR. As such, they would no longer be subject to the provisions of the eMoney Directive for typical mobile payments such as the purchase of parking tickets or ringtones via SMS[124]. Considering that online e-payment systems have become very successful in countries that

[123] See note 60

[124] See section 3.2.3 with respect to value added services and mobile payments

did not apply strict regulatory rules (such as Japan), we are convinced that this new waiver scheme will significantly foster private initiatives to create new e-payment systems.

Voluntary accreditation – While we think a strict regulation of *all* e-payment service providers cripples the uptake of e-payment services (hence our recommendation to add another waiver scheme), we think it could nevertheless be useful to introduce a voluntary accreditation system for e-money issuers in order to enhance consumer trust. By joining such an accreditation system, e-money institutions would assure consumers that the use of their e-money is safe and that transactions are secured in accordance with certain standards. Voluntary accreditation also entails a type of self-control, as members of an voluntary accreditation system will usually be reluctant to interact and trade with a member that fails to comply with any applicable standards and codes of conduct.

Supervise online payment providers that process important transactions – Services and systems which imply considerable financial transactions, must be subjected to a supervisory authority.

> *For example, in 2008, Second Life had over fifteen million users who collectively spent more than twenty million dollars in the virtual world every month. If such substantial amounts of e-money are being put into circulation, it is recommended that the issuers be supervised and controlled, and subject to a variety of consumer and privacy related obligations. There has, indeed, already been a bankruptcy of an "in-world" financial institution of Second Life in 2008*[125].

To the extent the individual accounts of such services and systems only allow storage of a value of maximum 150 EUR, these services would need to be subject to our proposed additional waiver scheme.

Mutual recognition for all waivers – The current principle of mutual recognition for waivers must be reversed, so that waivers for e-payment providers will be mutually recognised across all EU Member States (unless in specific cases).

Privacy implications – Some types of e-payment schemes imply significant privacy and data protection related issues, in particular RFID technology based applications. Conversely, other schemes (including disposable prefunded cards and gift cards) can guarantee the user's privacy and even anonymity, while still being easy to use in both the online and offline environment. The creation of such prepaid cards should therefore be further encouraged and stimulated, as this technology facilitates payment and transactions, and strongly enhances consumer trust.

Online escrow services – Online financial escrow services equally enhance consumer trust, as they ensure a correct transaction between buyer and seller, through a trusted third party. The development of such escrow services should therefore be stimulated, so as to increase their use and acceptance, and lower the transaction costs involved. As such services are particularly relevant for important financial transactions, it is recommended that they are subject to control and supervision (unless their involvement would be limited to transactions below a certain threshold), to the extent they do not fall within the scope of the Payment Services Directive.

Merge – As pointed out in section 3.3.2, we recommend to merge the Payment Services Directive and the eMoney Directive.

[125] www.wired.com/gaming/virtualworlds/news/2007/08/virtual_bank

Chapter 8
Electronic contracting

1. Historic evolution

Electronic commerce in its early stages consisted of digital transactions between and among businesses and individuals. With the development of the Internet and the increased number of dot com companies, e-commerce became the use of the Internet to conduct business. Initially emerging from the Electronic Data Interchange (EDI) several major steps and changes have occurred to get it to its current point.

EDI – The first step came from the development of EDI, which is a set of standards developed in the 1960's to exchange business information and do electronic transactions. While at first there were several different EDI formats that businesses could use, in 1984-1985 the ASC X12 standard became stable and reliable in transferring large amounts of transactions[126].

Web – The next major step occurred in 1992, when Mosaic[127] – the first "point and click" internet browser – was made available. Mosaic was quickly adapted into a downloadable browser, Netscape, which allowed easier access to electronic commerce[128]. Christmas of 1998 also became a major milestone for e-commerce: American internet provider AOL, for example, had sales of 1.2 billion USD over the 10 week holiday season from online sales[129].

E-commerce – With the development of new technologies and business models, the Internet continued to grow as a very powerful technology for the development of e-commerce. The European e-commerce market was worth 106 billion EUR in 2006 (although 70% of the turnover was concentrated in the UK, Germany and France)[130]. Between 2004 and 2008, the percentage of individuals who had ordered goods and services over the Internet for private use in the past year in the EU rose from 22% to 34%. In 2008, 32% of individuals in the EU had ordered online in the past year. However, there is a significant variation across EU Members States in the level of e-commerce[131].

M-commerce – With the popularity of mobile phones and smartphones on the rise, mobile data and Internet services are following the same pace. Text messages have become the universal mobile data service for the masses, because it does not require special downloads or configuration as it is already embedded in over 98% of all cell phones[132]. In relation to mobile Internet there are more than 40 million active monthly users in the U.S. alone[133]. By 2013, it is expected that 125 million Europeans will use mobile Internet services[134]. Moreover, at a worldwide level, there are 800 million users of Web-capable

---

[126] J. WEISMAN, The Making of E-Commerce: 10 Key Moments, available here: www.ecommercetimes.com/story/4097.html

[127] Mosaic is the web browser credited with popularizing the World Wide Web. More information available at http://en.wikipedia.org/wiki/Mosaic_(web_browser)

[128] J. WEISMAN, *Ibid.*

[129] *Ibid.*

[130] Report on cross-border e-commerce in the EU, SEC(2009) 283 final, p. 5, available at http://ec.europa.eu/consumers/strategy/docs/com_staff_wp2009_en.pdf

[131] *Ibid.*

[132] www.cellsigns.com/industry.shtml

[133] www.ecommercetimes.com/story/66795.html

[134] www.forrester.com/ER/Press/Release/0,1769,1203,00.html

handsets[135]. This mobility trend is further accelerated by the popularity of modern smart phones (such as iPhones and BlackBerrys), which are fully internet-enabled.

The future? – While mobile applications are the current trend, the next trend may be "intelligent" software and "smart agents", which enter into transactions on behalf of their human owner, within the limits specified by their owner.

2. Electronic contracting in the eCommerce Directive

This section 2 provides a description and analysis of the regime established in Articles 5.1, 9, 10 and 11 of the eCommerce Directive.

2.1. Background

Fragmentation – By the end of last century, during the golden era of the Internet, *"a clear divergence in Member States' approaches to e-commerce and e-contracting was developing. Some countries such as Germany had already forged ahead with new permissive legislation. Others, such as the UK, were lagging behind mired in the process of consultation"* [136]. This was the perfect scenario to justify a Directive covering e-contracting issues in order to reduce the level of uncertainty, internet users' fears[137], and the lack of cross-border harmony. Moreover, as e-commerce would help to promote the Single Market goals, it was important to guarantee that local laws on e-contracting would not create barriers to cross border transactions. In fact, prior to the Directive, twelve Member States did not have clear legislation on the legal status of an electronic contract[138].

Initial proposal – In its Proposal[139] for the Directive, the European Commission had identified *"specific obstacles restricting the possibility of concluding on-line contracts across frontiers*", especially because *"[p]articular acts performed by the parties with a view to concluding electronic contracts may result in considerable legal uncertainty as to the conclusion of the contract. In particular, the same act of clicking on the "OK" icon may have different legal implications in different Member States (does it constitute acceptance of an offer to provide a service or a customer's offer to contract?) and can give rise to uncertainty as to the time when the contract was concluded (the time of receipt or of sending the acceptance?). This major divergence between the national legal systems, linked to the specific nature of the technological context, results in uncertainty in cross-border contractual relations – particularly for consumers – and is inimical to the development of the trust which is necessary for electronic commerce (one party may consider, on the basis of his own legal system, that the contract has been concluded while the other party, on the basis of his national rules, believes that he is not yet bound)"*.

Moreover, the Commission had also noted that *"some formal requirements prevent contracts from being concluded electronically, or result in a considerable lack of legal certainty as to their lawfulness or*

---

[135] www.ecommercetimes.com/story/66795.html

[136] *Ibid.,* pp. 67-92

[137] In its original French version: "*aux inquiétudes de l'internaute",* J. BERLEUR and Y. POULLET, "Réguler Internet", *Études* 2002/11, Tome 397, p. 472

[138] Study on the economic impact of the E-commerce Directive prepared for the Expert Group on electronic commerce by Copenhagan Economics, dated 8 September 2008, available at http://ec.europa.eu/internal_market/e-commerce/docs/expert/20080915_study_en.pdf

[139] Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market, Brussels, 18.11.1998, COM(1998) 586 final, p. 12

validity. This may take the form of requirements which obviously rule out electronic contracts, (for example, a requirement that a contract be drawn up on paper), or more frequently, difficulty arising from the interpretation to be given to requirements such as "in writing" (i.e. on paper), "in a durable medium", "an original". Such legal uncertainty clearly works against on-line transactions; some Member States are therefore considering amending their rules and the courts have already given rulings on this matter. At Community level, the recent proposal for a Directive on electronic signatures does not deal with formal requirements other than signature".

The Community, nevertheless, had already been involved in regulating electronic commerce for decades. In 1987, the TEDIS Electronic Data Interchange (EDI) programme was established to encourage the use of EDI in trade[140]. Directive 98/34/EC and Directive 98/48/ EC[141], both adopted in 1998, provided further procedures for the provision of information in the field of technical standards and rules on information society providers. Those Directives imposed on Member States the obligation to ensure that the standards of national bodies were compatible with the Commission's standards and that they did not create barriers to the functioning of the Internal Market.

Other Directives related to e-commerce – The Distance Selling Directive[142], when implemented in 1997, did not regulate any distance e-commerce issues. It was originally tailored to regulate distance transactions concluded via catalogues, fax machines, and telephones. Other legal aspects regarding electronic trade before implementation of the eCommerce Directive were regulated in the Data Protection Directive 95/46[143] and the Electronic Signatures Directive 99/93[144].

2.2. Electronic contracting under the eCommerce Directive

2.2.1. Basic requirements

Article 5, 10 and 11 impose several basic contracting requirements for online service providers. Following the implementation of this Directive at a national level, service providers quickly adapted their websites to comply with these requirements[145]. Thus, complying with the requirements of this Article did not originate major issues for website owners.

Information duty – In order to protect customers, article 10 holds that online service providers must provide information on the technical steps which customers have to follow in order to conclude a contract, how to correct input errors, and to provide information on codes of conduct, contract terms and

---

[140] Council decision introducing a communication network community programme on trade electronic data interchange system (OJ 1987 L 285/1) and following decision (OJ 1997 L208/1)

[141] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services and Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access

[142] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts

[143] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[144] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[145] First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Brussels, 21.11.2003, COM(2003) 702 final

general conditions, prior to entering into the contract. Most of these obligations can, however, be deviated from for non-consumers.

Article 10 is complemented by paragraph 1 of article 5, which holds that a set of general information (such as the name and geographic address of the service provider) must also be provided by the service provider, even when the service provider does not enter into a contract[146].

Harmonisation of contract rules – Article 11 introduces an innovative method for formation of e-contracts. Unless otherwise agreed by parties who are not consumers, the e-contract will be concluded through the placing of an "order" by the recipient of the service, followed by an acknowledgment of the receipt of the order by the service provider. Moreover, the service provider has to make available to the customer effective and accessible technical means allowing for the correction of errors. If, however, the contract is executed exclusively by exchange of electronic mail or equivalent individual communications, the service provider does not need to make available a means for correction of errors or to acknowledge receipt of the order.

2.2.2. *Characteristics of the electronic contracting regime*

The electronic contract regime is characterised by the following principles.

Equivalence – Pursuant to the general principle set forth in paragraph 1 of article 9, contracts made by electronic means shall be valid. In other words, save for the few exceptions (which are also set forth in article 9), anything which can be achieved through written documents must be in law achievable through electronic documents[147]. The provisions of this article are complemented by the Electronic Signatures Directive, which ensures the legal recognition of legal signatures[148].

The regime set out in paragraph 1 of article 9 does not apply to the contract types listed in paragraph 2 (such as real estate contracts, contracts requiring court involvement and family law contracts). It is not the purpose or intention of the Directive to have this list of exceptions remain unaltered for an unlimited period of time. According to paragraph 3, Member States must inform the Commission every five years of the reason why they would consider it necessary to maintain the category of *"contracts requiring by law the involvement of courts, public authorities or professions exercising public authority"* (article 9.2.b).

Removal of obstacles for the use of e-contracts – Article 9.1 establishes that Members States shall ensure that their legal system[149] allows for contracts to be concluded by electronic means. For this purpose, they must remove any legal requirements that could create obstacles for the use of electronic contracts or deprive them of legal effectiveness or value.

Pursuant to paragraph 34 of the recitals, the examination of the legislation must be made in a systematic way and should cover all the stages and acts of the "contractual process" (including publicity, negotiation, offer, acceptance, registration, amendments, invoicing and archiving[150]). This means that, by

---

[146] Proposal for a European Parliament …, p. 22

[147] A. MURRAY, *Ibid.*

[148] According to article 5.1 of the Electronic Signatures Directive, a "qualified electronic signature" attached to electronic data shall have the same status as a written signature on a paper document.

[149] The only change to the wording of this Article 9.1 from its first draft to the final draft was the elimination of the reference to “legislation". This change was intended to prevent common law Member States from using their common law principles of contract to achieve meet the equivalence principle without the need to enable legislation. Notwithstanding this change during the drafting process, according to Andrew D. Murray, the United Kingdom, a common law Member State, decided not to directly implement Article 9, thereby failing to fully implement this Article – See A. MURRAY, *Ibid.*

[150] *Ibid.*, p. 201

way of example, Member States would have to amend a provision in their civil code requiring that certain contracts must be handwritten[151]. However, according to paragraph 37 of the recitals, only *legal* obstacles have to be removed; *practical* obstacles do not have to be removed[152].

Information about the procedure of formation – "*In order to ensure a high standard of fair trading and consumer protection*" [153] article 10 paragraph 1 imposes "extensive requirements" [154] on the service provider (unless contractually agreed otherwise with customers that are not consumers). Service providers must also inform their customers of any codes of conduct the service provider has subscribed to, and how these codes of conduct can be consulted electronically. The purpose of this provision is to inform the customer of certain rules the service provider will comply with, particularly if those rules may have an impact on the customer' expectations[155].

The concluded contract – Prior to placing the order, service providers must inform customers on whether the contract will be filed by the service provide, and whether the concluded contract will be accessible by the service recipient.

Contractual terms and general conditions – Service providers must provide customers with the contractual conditions in a way that allows the customer to store and reproduce (print) them. The Directive does not establish any limit on the length of these conditions or on its content. Moreover, it does not provide for any difference between what should be included in the order and acknowledgement of receipt, *vis-à-vis* the contractual terms and general conditions.

The term "order" – Due to the "turbulent path" [156] of article 11 during the drafting process, the title of this article and its paragraph 1 make reference to the term "order". The use of this term was the result of the consensus that the parties involved in the legislative process were able to achieve. This concept of "order" is a neutral term that avoids any reference to the concepts of offer and acceptance[157]. According to GOBERT and MONTERO, the term "order" should be understood in a broad sense, irrespective of the online service it relates to, provided that from the "order" it is clear that the recipient wants to enter into an electronic contract with the service provider.

Acknowledgment of the receipt of the order – Without undue delay, the service provider must acknowledge the receipt of the order. The acknowledgment of the order has to be made by electronic means[158]. It is not clear from the wording of the Directive if the immediate display of the acknowledgment of the receipt on the service provider's website shall suffice to meet this requirement, or if it is required to send an e-mail[159].

---

[151] Example from D. GOBERT and É. MONTERO, "Les contrats conclus par voie électronique" in *Le Commerce Électronique sur les rails?,* Bruylant, Brussels, 2001, p. 200

[152] For instance, contracts that have to be executed before a third party, such as contracts before a public notary - D. GOBERT and É. MONTERO, "Les contrats conclus par voie électronique", p. 207

[153] Comments to Article 10, p. 6, Proposal for a European Parliament …,

[154] RAMBERG, CHRISTINA HULTMARK, "The E-commerce Directive and Formation of Contract in a Comparative Perspective", *Global Jurist Advances,* Volume 1, Issue 2, Article 3, 2001

[155] M. DEMOULIN, "Information et transparence sur les réseaux" in *Le Commerce Électronique sur les rails?*, Bruylant, Brussels, 2001, p. 124

[156] This process is explained in detail in A. MURRAY, *Ibid.*

[157] D. GOBERT and É. MONTERO, *Ibid.*, p. 258

[158] Article 11, paragraph 1, first bullet

[159] D. GOBERT and É. MONTERO, *Ibid.*, p. 258, consider that these are alternative means of acknowledgment, although most of the service provides use both e-mail and display on a webpage for each order.

Moment of the "order" and "acknowledgment of receipt" – The second bullet of paragraph 1 of article 11 establishes a sort of "delivery" rule to determine the exact moment in which the order and acknowledgement of receipt occur. The order and/or receipt shall be deemed to be received when the parties to whom they are addressed are able to access them. In other words, it is the moment when the message "enters the circle" [160] of the addressee that is relevant. In the case of an e-mail, the moment such message arrives at the mail server of the addressee's e-mail address, the message will be deemed as received at that moment. This rule is particularly significant, as it is also applicable to electronic contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

2.3. Issues linked to the electronic contracting regime

This section 2.3 highlights some of the issues related with and resulting from the electronic contracting regime deserving of further analysis.

2.3.1. Formalities in articles 10 and 11

The contracting requirements laid down in article 10.1 (transparency obligations), 10.3 (contract terms) and 11.2 (input errors) evidence the legislator's "cold feet": the legislator was afraid that consumer interests could be harmed during the online ordering procedure because customers were not familiar with online procedures, and therefore imposed basic requirements on the online service provider.

While these concerns may have been valid at the time the time the eCommerce Directive was adopted, they have now either become evident (tools to avoid input errors), have become a stumbling block for new technologies and business models (allowing to store terms and conditions), or merely lead to increased compliance costs (describing the technical steps of the contracting process).

Furthermore, it should be recognised that the consumer protection aspirations of articles 10 and 11 partially duplicate the existing rules of the *consumer acquis*. Abolishing article 10 and 11 would therefore not lead to less consumer protection.

> *For example, article 10.3 requires the service provider to make available the contractual terms and conditions. Articles 4 and 5 of the Distance Selling Directive have the same goal.*
>
> *Similarly, article 10.1.d) requires the service provider to specify in advance which languages are offered for the conclusion of the contract. The concern expressed by the eCommerce Directive (avoiding that a website would be offered in one language, while the accompanying contract would be offered in a different language) is also tackled by the Unfair Commercial Practices Directive (e.g., article 7).*

2.3.2. Article 5 of the eCommerce Directive

Article 5 holds that *"In addition to other information requirements established by Community law, Member States shall ensure that the service provider shall render easily, directly and permanently accessible to recipients of the service and competent authorities: (…) (c) the details of the service provider, including his electronic e-mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner"*

On 16 October 2008, the European Court of Justice ruled that the eCommerce Directive requires online service providers to offer a form of communication that permits the customer to contact the service provider rapidly and in a direct and effective manner. This form of communication must be offered before

---

[160] Sergio. M. ELVIRA, "Formación y validez del contrato electrónico: Estudio Comparad"o, *AR: Revista de Derecho Informático*, No. 51, October 2002, available at www.alfa-redi.org/rdi-articulo.shtml?x=1427

the contract is formed, and must be offered in addition to an e-mail address. This case[161], the only EU-level case regarding the electronic contracting provisions of the eCommerce Directive, highlights a fundamental flaw of the eCommerce Directive.

Background facts – The defendant, Deutsche Internet Versicherung ("DIV"), is an automobile insurance company operating exclusively online. Through its website, DIV provided its postal address and e-mail to its website visitor, but no telephone number. Instead, an online enquiry template was offered which had a response time of 30-60 minutes; a telephone number was only provided after a contract was concluded. The German Federation of Consumers' Associations[162] brought an action based on Article 5.1 of the eCommerce Directive, alleging that the Directive requires DIV to provide a telephone number even before the contract was concluded.

The ruling – The ECJ held that Article 5.1(c) of the Directive had to be interpreted as meaning that "*a service provider was required to supply to recipients of the service, before the conclusion of a contract with them, in addition to its electronic mail address, other information which allowed the service provider to be contacted rapidly and communicated with in a direct and effective manner. That information did not necessarily have to be a telephone number, it might be in the form of an electronic enquiry template through which the recipients of the service could contact the service provider via the Internet, to whom the service, provider replied by electronic mail except in situations where a recipient of the service, who, after contacting the service provider electronically, found himself without access to the electronic network, requested the latter to provide access to another, non-electronic, means of communication*"[163].

In addition, the European Court of Justice stated that "in exceptional circumstances" where a recipient of the service, after making contact by electronic means with the service provider, is deprived of access to the Internet (*e.g.,* due to a journey, holiday or a business trip), communication by an enquiry template can no longer be regarded as effective within the meaning of article 5.1.c of the Directive. The service provider must then provide *"access to a non-electronic means of communication"* [164], even if that client initially entered into contact with the provider through electronic means.

According to the ECJ, the requirements of the "*direct and permanent"* means of communication were not sufficiently met by an e-mail address and, as such, online vendors must also display either a telephone number or, alternatively, a web response form that is answered in 30-60 minutes – not by an automated responder, but by a human being.

Evaluation – Offering only an e-mail address does not comply with the E-Commerce Directive's disclosure requirements even when the service provider maintains very high levels of availability, both on its website and via the communication channels it offers to its customers through its website.

Instead of promoting digitalisation and use of electronic services, this ruling takes a step back, by assuming that the Internet is less available and less efficient than a telephone line or a mobile phone. The ECJ approach is to have more personal service, instead of electronic templates, and to guarantee to consumers an important level of service. But not all e-stores, particularly small web-shops, have those resources. Some e-stores are owned, managed and supplied by a single individual. They use the

---

[161] ECJ Case [C-298/07] Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Deutsche Internet Versicherung AG, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62007J0298:EN:HTML

[162] Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV

[163] see para [40] C-298/07 Bundesverband [2008]

[164] see para [39] C-298/07 Bundesverband [2008]

Internet because of its reach and availability. This means that they could be receiving a visit on their website at 2:00 a.m. from a client in New Zealand.

Essentially, online service providers are now forced to provide 24/7 call centres to deal with requirements of the ECJ ruling. The ECJ obviously focused on consumer protection, without taking into consideration the fact that requiring additional direct contact with a human being creates additional costs for any enterprise which provide services online – not to mention SMEs and individuals acting as service providers. Moreover, the ruling was not very clear and created additional uncertainty on how service providers should be organised in order to comply with the ruling.

2.3.3. Unclear structure

Both paragraphs 1 (basic information requirements) and 2 (conveying codes of conduct) of article 10 include an exception for B2B contracts whenever the parties have agreed otherwise. However, paragraph 3 (making available T&C) does not contain a similar exception: no specification is made as to whether the "recipient" to whom the contract terms are to be provided is a consumer (B2C) or a business (B2B). It is not clear why this is the case.

2.3.4. Language requirements

According to article 10.1(d), service providers are required to provide recipients with information on "*the languages offered for the conclusion of the contract*". The question arises whether this requirement is relevant (or even whether this requirement has ever been relevant), because it is very uncommon for a website to be in a particular language, while the contractual terms are in another language. Therefore, this provision seems to result in a redundancy. Only in the event that the language of the contents on the website viewed is different from the language offered for the conclusion contract should service providers provide this information.

2.3.5. Confirmation step

Although in most legal systems contracts are formed through the exchange of offers and acceptance, the eCommerce Directive introduces a third step in contract formation – confirmation. Accordingly, a contract is concluded only when the customer has received an electronic acknowledgement of his order from the service provider[165]. Pursuant to article 11, if a service provider fails to send a confirmation to the consumer issuing acknowledgment, no contract is formed.

The central principle behind the prior information requirements provided for in article 10 of the Directive is to establish the confidence of consumers and businesses in e-commerce, which is again a sign of the legislator's "cold feet" in the area of contracting. Consumers will only be willing to use electronic commerce if they are convinced that it is as safe and reliable as conducting transactions on the traditional market.

Hence, in the words of MURRAY, "*it quickly becomes clear that article 10 is not a formation of contract provision at all, but rather a consumer protection provision embedded into the contract formation rules.*"

2.3.6. Execution of contracts via new devices

Articles 10 and 11 establish a regime which is mandatory for all electronic contracts entered into with consumers, and that may be briefly explained as follows: information such as the technical steps for

[165] Article 11 of the eCommerce Directive

conclusion of the contract, technical means to identify and correcting input errors and the terms and conditions of the contract (in a way that allows the service recipient to store and reproduce) is made available to the recipient of the service. The recipient will then agree with the offer and place the order. The service provider must then acknowledge receipt.

Procedure with a typical pc – It is very easy to imagine an individual (recipient of the information society service) in front of a computer screen going through the steps for conclusion of the contract and the terms and conditions, then clicking "OK" to accept the terms and conditions and storing them in the computer hard drive and, finally, receiving an e-mail with the acknowledgment of receipt of the order placed. To have this process properly executed, it would be necessary to have a screen large enough to allow for the reading of the terms and conditions, a mouse to click on the "OK" button of the terms and conditions, a hard drive to store all of this information and an e-mail account to receive the acknowledgement of receipt.

New technologies – Today, several new online services are being made available to the public, including services targeted to companies, through the use of SMS or instant messaging.

> *For example, while waiting at a bus stop for a bus, it is possible to request a service from the bus company providing information on when the next bus is due to arrive at such bus stop (a fee is charged for this service). This service is delivered upon sending an SMS to a number provided by the bus company. Such service is also an information society service pursuant to Directive 98/34 amended by Directive 98/48*[166]*, and for this reason it must comply with the requirements of articles 10 and 11.*

Limitations of SMS – SMS services have certain technical limitations in opposition to the user experience of accessing information through a browser on a computer screen. For instance, an SMS only allows 160 characters per message. The length of the majority of the terms and conditions for any service would take up more than 160 characters, or even ten times more. Should the recipient have to receive 10 SMS messages on his/her mobile phone before accepting any service, he would most likely not enter into the contract.

In addition to the number of messages, it is also important to consider size and design limitations of the devices, proving to be too bothersome for the consumer to read long texts on such devices. Accordingly, it is not very likely that the consumer will read all of this information, at least while in the process of formalising the contract[167].

Ease of use – Like in most consumer-related services, consumer adoption and use shall only occur if the service is useful and easy to use. The bus stop example is a prime example of how important it is to have simple solutions. The same line of reasoning applies to the provision of information society services via PDAs or smart phones[168], instant messaging services, *"and in the future – who knows?"* [169].

Technology neutral? – With the increase in the number of mobile phones[170], more services will be launched at a global scale[171]. The question arises whether the current regime is still adequate for all online services, including those that exist and/or will exist in the future.

---

[166] Preamble, and paragraphs 34 of eCommerce Directive

[167] J.L. M. HERNÁNDEZ and M.J.I. PORTELA, *M-Commerce: contract law, electronic payment and consumer protection* (ECLIP Series)

[168] Website owners make available versions of their websites prepared to be viewed in PDAs or smartphones.

[169] *Ibid*. JOSÉ L. M. HERNÁNDEZ and MARÍA J. I. PORTELA, *M-Commerce: contract law, electronic payment and consumer protection* (ECLIP Series)

[170] "There are over 3 billion mobile phones worldwide. This means that over 40% of the world's population carries a mobile phone, far more than use a computer or have access to the internet. In many developed countries, mobile phone penetration

The eCommerce Directive claims to take a *technology neutral* approach. In fact, in several of its provisions, the Directive makes reference to "electronic means" [172] without ever specifying the device to be used by service recipient. This is indeed the correct approach in order to promote innovation.

However, the Directive is not as "technology neutral" when it comes to establishing the steps for concluding contracts by electronic means. The required contractual steps and the entire legal structure seems conceived as if all customers would sit in front of a computer screen. This "contractual process" is very difficult to implement for mobile services.

These constraints are far from being a surprise. In November 2000, GSM Europe, the European interest group of the GSM association, wrote a letter[173] to the Commission stressing the "*necessity to take into consideration the specificities of m-commerce enablers such as mobile handsets*" when implementing the Directive at national level. Moreover, the Commission, in a 2004 document[174], had already noted that the information requirements on the Distance Selling Directive were implicitly based on computers as the main technology to provide Internet access[175].

2.3.7. *Storage and reproduction of contract terms and general conditions*

Article 10.3 establishes that the online service provider must make available to the customer the terms and conditions, in order to allow him to store and reproduce them. The relevant web page will have to be prepared and configured in such a way that the recipient at "his place"(*chez lui*) may adequately print or store them[176].

Technological development and change in consumer behaviours have made this provision outdated. Websites play a much less central role in today's consumer web experience. Consumer behaviour was recorded in The Yearbook of Consumer Law (2008) and evidenced that, upon being questioned on whether they read the terms and conditions made available to them when contracting online, 43% of consumers said they "sometimes" read them, 29% "always" read them and 28% of consumers never do[177].

Such a provision clearly calls into question the form of click-wrap agreement, when the agreement is displayed in a separate window from which it cannot be downloaded, copied or printed. Furthermore, a significant number of service recipients use mobile phones to access online services, which make the storage of contract terms and conditions barely feasible. Some of these mobile equipments do not allow

---

is above 90% and developing countries are catching up fast" in Mobile Commerce: opportunities and challenges, a GS1 Mobile Com White Paper, 2008, p. 6

[171] "Businesses are looking for innovative ways to enter into a relationship with consumers. Technology is allowing a two-way dialogue between brand owners and consumers to be real." *Ibid.* "Mobile Commerce…."

[172] A few examples of the use of the expression "electronic means": Paragraphs (18), (34), (35), (37), (52), Articles 2, 9 and 11

[173] Available at www.gsmeurope.org/documents/positions/2000/implementation_ecommerce_091100.pdf

[174] Commission Staff Working Paper, "Legal Barriers in e-business: The results of an open consultation to enterprises", Brussels, 26.4.2004, SEC(2004) 498

[175] *Ibid.*, p. 18

[176] M. DEMOULIN, "Information et transparence sur les réseaux" in *Le Commerce Électronique sur les rails?*, Bruylant, Brussels, 2001, p. 125

[177] C. TWIGG-FLESNER, D. PARRY, G. HOWELLS and A. NORDHAUSEN, *The Yearbook of Consumer Law 2008,* Ashgate Publishing, Ltd.

– or have limited capabilities – to store information which is made available on a web-page (including when such webpage is prepared to meet the requirements of article 10.3). Moreover, most of the mobile devices are not prepared to interface with printers to carry out printing jobs.

2.3.8. *Length of terms and conditions*

As pointed out above, most consumers do not read a service provider's terms and conditions. Still, the terms and conditions often contain important and extensive exclusions of liability of which end-users are not aware.

This observation is likely at least partially linked to the length of the contractual terms and conditions[178].

> *For example, the terms and conditions of Apple iTunes[179] encompass about 23 pages when printed; those of Amazon[180] and Dell[181] each about 15 pages; those of Facebook[182] about 8 pages.*

The eCommerce Directive does not restrict the length of the contractual terms and conditions used by an online service provider. Although the issue of lengthy contractual terms and conditions is not limited to the online environment — they equally exist in the offline environment — it must be recognised that offline terms and conditions are typically limited to a single page (often in a small font, printed on the back of an invoice) as it would be burdensome to provide a separate bundle of paper with terms and conditions. Conversely, the unlimited space available on websites seems to incentivise lawyers to make the terms and conditions overly long. Also, many lawyers seem to suffer from "cold feet" in the online context, so that many unnecessary legal provisions are nevertheless included.

However, lengthy terms and conditions are difficult to reconcile with the fast-moving and multi-tasked online environment, and are also difficult to apply to minors. Expecting a customer (particularly a minor) to read twenty pages before a service can be used, is exaggerated. We therefore recommend the Commission to adopt sector-specific, concise templates of terms and conditions, and to incentive service providers to use these templates. An interesting idea would also be to create a set of "boiler plate" standard clauses, whereby the actual terms and conditions of a service provider would only need to list clauses that deviate from the boiler plate standard clauses. This would drastically reduce the length of terms and conditions.

Preferably, the use of such templates would also be integrated in trustmarks[183].

3. eSignatures

Directive 1999/93/EC on a Community framework for electronic signatures (eSignatures Directive)[184] aims to ensure a basic legal recognition of electronic signatures within the EU, and allow the free flow of electronic signature products and services cross border[185].

---

[178] The typical use of "legalese" expressions is another issue.

[179] See, for example, the Belgian version at www.apple.com/legal/itunes/befr/terms.html - SERVICE

[180] See, for example, the UK version at www.amazon.co.uk/gp/help/customer/display.html?ie=UTF8&nodeId=1040616

[181] See, for example, www.euro.dell.com/content/topics/topic.aspx/emea/topics/footer/terms?c=uk&l=en&s=gen

[182] See www.facebook.com/terms.php?ref=pf

[183] See our recommendation in Chapter 13 - self regulation

[184] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *OJ* L 13, 19.1.2000, p. 12–20

[185] Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, 15 March 2006, COM(2006) 120 final ("Report")

Legal recognition – As the Commission noted in its Report on the operation of the eSignatures Directive, the first objective has been achieved by the transposition of the Directive into the legislation of the Member States. By implementing the general principles of the Directive, all Member States legally recognise e-signatures. As such, the objectives of the Directive have already been largely fulfilled at this moment[186].

Cross-border use – However, a legal and technical analysis of the practical usage of electronic signatures shows that the objective of (cross-border) use of e-signatures has not yet been achieved[187]. Service providers have little incentive to develop a multi-application electronic signature and prefer to offer solutions for their own services. As a result, today's e-signature market consists of isolated islands of e-signature applications, where certificates can only be used for one single application[188]. This lack of technical interoperability has been the main obstacle for market acceptance of e-signatures. In turn, the lack of market acceptance further decreases the incentive for service providers to develop new and multi-application e-signatures. In other words, a classic "chicken-and-egg" situation.

Action Plan – The Commission has acknowledged the need for mutually recognised and technically interoperable e-signature solutions, and has therefore adopted an Action Plan on e-signatures, which aims to offer a comprehensive and pragmatic framework to achieve interoperable e-signatures[189].

- With respect to **qualified electronic signatures** and advanced electronic signatures based on a qualified certificate, the main obstacle for cross border use lies in the lack of trust in e-signatures originating from other Member States. At present, it is often difficult to obtain information regarding the status of the certification service provider, or to verify the quality of the signature (as regards its advanced or qualified nature).

  To facilitate this validation process, the Commission will compile a "Trusted List of Supervised Qualified Certification Service Providers" at a European level. In addition, it will further update the list of generally recognised standards for e-signature products[190].

- With respect to **advanced electronic signatures**, Member States have used very diverse technical solutions with different security levels[191]. Similar to qualified e-signatures and advanced e-signatures based on a qualified certificate, the main challenge lies in the fact that receiving parties must be able to easily validate advanced electronic signatures, and to trust their legal value or security level.

  To avoid multiple validation efforts in Member States, the Commission proposes to delegate these verification and validation tasks to a centralised or distributed validation service mechanism. The available options for establishing such a mechanism will be examined through a feasibility study[192].

We welcome this Action Plan: with such initiative, the Commission is taking the necessary steps to further encourage and facilitate the use of e-signatures. As the main obstacles for widespread use of e-signatures are of a practical and technological nature rather than a legal nature, it is indeed necessary to

---

[186] *Ibid.*, p. 9-10

[187] Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, 28 November 2008, COM(2008) 798 final ("Action Plan")

[188] Report, p. 7

[189] Action Plan, p. 4

[190] *Ibid.*, p. 7-8

[191] Article 2.2 of the eSignatures Directive defines advanced electronic signatures in a generic way. Member States had more discretion as to which advanced electronic signature solutions they would accept.

[192] Action Plan, p. 8-9

take measures which can simplify the technical validation and verification of e-signatures in practice. By doing so, the Commission has taken a first step to deal with the "chicken-and-egg" problem described above.

Long-term validation – A second reason for the reluctance to implement e-signature applications is that the archiving of electronically signed documents is often considered too complex and too uncertain[193]. This is caused by the fact that the validity of certificates is usually limited in time. Indeed, the rapidly evolving technologies for certificates do not allow certificates to have a long-term validity.

The expiry of such certificates also entails the expiry of e-signatures based on these certificates. This problem can be bypassed by resigning the document with a new certificate each time the previous certificate expires, which is, however, a laborious procedure. The expiry of certificates and e-signatures undermines the concept of e-archiving, as the advantages thereof do not seem to outweigh the disadvantages. The issue of long-term validation of e-signatures therefore currently remains unresolved, and also requires to be addressed on a technical level rather than from a legal perspective.

4. E-invoicing

4.1. Introduction

All companies would like to cut back costs by 80% and reduce the average cost of 30 EUR of processing a paper invoice. Needless to say, in pursuit of these results, businesses are now looking at e-invoicing[194].

It is estimated that more than 30 billion paper invoices are sent each year in Europe. The adoption of e-invoices would deliver potential savings of 243 billion EUR per annum in Europe, according to the Corporate Action on Standards (CAST) project from the European Association of Corporate Treasures[195]. In addition to the costs reduction, there are other significant benefits associated with the use of e-invoices. Such benefits include[196] better customer services, jobs with less routine and better environment[197]. These benefits also align with the goals set out in the Lisbon Agenda, to allow Europe to become the most competitive and dynamic knowledge-based economy in the world.

---

[193] Report, p. 8

[194] See K. FLINDERS, "E-invoicing could help firms through recession", 03 September 2008, available at www.computerweekly.com/Articles/2008/09/03/232120/e-invoicing-could-help-firms-through-recession.htm

[195] See *E-Invoicing 2008*, published by the Euro Banking Association and Innopay (available at www.abe-eba.eu; www.innopay.com), p. 55, section 5.2. In this section it is also mentioned that the University of Hannover has potential savings of nearly €135 billion per year

[196] B. HARALD, "Electronic Invoicing – 238 billion reasons – to begin with.." at i2010 Conference, Information Society at the Crossroads, available at www.i2010conf.si/P2-Harald.pps - 577, 2, e-invoicing – massive cost savings

[197] *Ibid.* It is estimated that the energy and raw material needed for producing of the relevant paper, printing, enveloping, distributing and recycling 20 billion invoices would correspond to the following savings per year in the event of replacement of e-Invoices: 400 000 tons of paper; 2700 tons of ink; 160 million liters fuel; 1432 GWH energy and 15 million trees - www.i2010conf.si/P2-Harald.pps - 588, 5, Slide 5

4.2. The Electronic Invoicing Directive

4.2.1. Electronic invoicing before the Directive

"The invoice is probably the most important document in commercial trade", according to a 1999 PWC Report[198]. With the Single Market as an ultimate goal, a simplification and a harmonisation of the national VAT legislation on invoice requirements was deemed to be necessary in those days. For instance, some Member States like Germany, Greece, Luxembourg and Portugal[199] did not recognise paperless electronic invoices as proper invoices for VAT purposes.

EDI – In relation to the technologies used, EDI[200] and e-invoice delivery over the Internet by means of e-mail attachments were the systems used. However, both EDI and the use of e-mails were not treated in the same way by the Member States. In some Members States (like Belgium, France, Italy and Spain) the use of the EDI standards was mandatory, while in others (Austria, Denmark, the Netherlands, Sweden and the UK) EDI appeared to be the a *de facto* standard.

The same type of inconsistency among Member States existed in relation to the possibility to attach e-invoices to e-mails: Austria, Denmark, Finland, Ireland, Italy, Sweden and the UK were the only Member States allowing this. This inconsistency between Member States – of which the above mentioned cases are only an example – represented a significant barrier for the Single Market goals and for the development of electronic commerce.

It was clear then, as it is today, that new technologies can provide more security and offer more information, in a form easier to utilise than paper invoices, all this with lower production and storing costs for businesses. The European Commission recognised these concerns in a proposal of Directive[201]: *"the development of electronic commerce has made it necessary to establish a legal framework for the use of electronic invoicing to enable tax administrations to continue to perform their controls"*. This proposal was later amended and approved by way of Directive 2001/115/EC[202] (hereinafter called the "eInvoicing Directive"). Directive 2001/115/EC was eventually replaced by Directive 2006/112/EC [203] (the "Invoicing Directive"), although no relevant changes were made to the provisions on electronic invoices.

4.2.2. Invoicing under the eInvoicing Directive

Under the eInvoicing Directive, traders in Europe have to comply with one set of VAT rules for all the invoices it issues, irrespective of the place of taxation of the goods or services being sold. This Directive establishes the following regime for Member States to implement:

---

[198] "Study on the requirements imposed by the Member States, for the purpose of charging taxes, for invoices produced by electronic or other means" by PriceWaterHouseCoopers, available at http://ec.europa.eu/taxation_customs/taxation/vat/key_documents/reports_published/index_en.htm

[199] Ibid. "Study on the requirements imposed…", Section 4.2, p. 33

[200] Additional information on EDI is available on p. 30 of "Study on the requirements imposed…"

[201] Proposal for a Council Directive amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax, COM(2000) 650 final

[202] Council Directive 2001/115/EC, of 20 December 2001, amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax. This Directive was later now incorporated into the VAT Directive (Council Directive 2006/112/EC, of 28 November 2006, on the common system of value added tax)

[203] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax

- **A list of mandatory items** that must be mentioned on each invoice (such as name and address of the seller, date of issuance, number of the invoice, applicable VAT rate, etc.).
- **Electronic Invoices** – Traders have the right to issue invoices valid for VAT purposes both in paper or electronic by trades. They may use electronic invoicing on the condition that the authenticity of the origin and integrity of the content of the invoice are guaranteed. Pursuant to the Directive, those guarantees can be ensured by way of advanced electronic signatures, Electronic Data Interchange (EDI), or by any other method accepted by a specific Member State.
- **Place of storage** – Traders have the freedom to choose the place and method of storage of invoices (they may store invoices on-line in a Member State other than the country where it is established for VAT purposes).
- **Outsourcing** – Traders have the freedom to outsource invoicing operations to a third party or to his customer (i.e. self-billing).

Notwithstanding all the efforts of the Commission in preparing a directive that would allow for a significant harmonization and the benefits of this Directive, the wording of several provisions allowed for an open interpretation by Member States while implementing it. This has led to a lack of harmonization[204]:

- **Content of the invoice** – Several Member States' national VAT legislation contained provisions establishing requirements which go beyond the mandatory contents of an invoice set out in the Directive. For instance, in Hungary it was required to include an invoice page number as well as the total number of pages.
- **Summary statement on paper for EDI** – In certain national legislations, entities using EDI have to issue a paper summary document (for instance, Portugal, Greece or Hungary), while in other legislations there was no such requirement.
- **Electronic signatures** – Among other Member States, Greece and Germany required the electronic signature to be based on a qualified certificate, through means of a secure-signature creation device. For other countries, like Sweden and the United Kingdom, an advanced electronic signature would suffice.
- **Signature by legal entities?** – While electronic invoices do not need to be signed in order to be valid[205], electronic signatures can be used in the context of electronic invoices, as a means to secure the authenticity and integrity of an electronic invoice. Both functions of an electronic signature (*signing* and *ascertaining security*) should be clearly distinguished, although they both use the same technologies. It should not come as a surprise, however, that the dual role of electronic signatures has led to confusion regarding the question of whether a natural person should necessarily be involved in creating an electronic invoice. In those Member States that require an invoice to be secured by a qualified electronic signature for security reasons, it is often (wrongly[206]) assumed that these qualified electronic signatures can only be placed by natural persons. This interpretation

---

[204] See, particularly, the conclusions from "CompTIA EU Electronic Invoicing and VAT compliance requirements Publication", 2005, from CompTIA – The computer Technology Industry Association – www.comptia.org

[205] See article 229 of the eInvoicing Directive

[206] Even though it is acceptable to argue that only a natural person can place a qualified electronic signature to *sign* an electronic document (because only natural persons can place a traditional handwritten signature on a paper document), nothing prevents a legal person from placing a qualified electronic signature to *secure* an electronic document such as an invoice. The latter use of a qualified electronic signature is *merely* for security reasons, and — despite its name — does not fulfil the function of a traditional handwritten signature. As mentioned, this opinion is not shared by all commentators.

completely defeats one of the most essential purposes of electronic invoices, *i.e.* to allow invoices to be generated more efficiently by avoiding unnecessary human interactions.

- **Place of storage** – Not all Members States have established the same storage requirements. By way of example, in Belgium storage must be in electronic form and guarantee full on-line access, while the same is not applicable in Hungary.

This situation has led to a scenario of lack of harmonization with legal uncertainty. Any company involved in cross-border electronic invoicing has to comply with a (slightly or significantly) different regime for each of the Member States with which it was doing business, which increases the invoicing costs substantially, due to the increase in complexity of the relevant IT system. The increase in direct and indirect costs not only applies to companies doing cross-border trade, but also to companies offering electronic invoicing services, software solutions or auditing e-invoicing services.

It should be note that the aforementioned discrepancies only concern issues that are addressed by the eInvoicing Directive. Other issues (such as the time of storage of data and verification of certificates) are also not harmonized, thereby contributing to the legal uncertainty and increase of costs, and creating additional barriers to cross-border trade.

> ***Practical example: delegated signing of e-invoices.*** *A leading European e-invoicing service provider developed a new e-invoicing system that would allow customers to send raw invoice data from its enterprise systems to the service provider's central e-invoicing platform. The service provider's platform would then convert the raw data into a PDF file that was signed with the service provider's qualified signature. This PDF file – which constitutes the invoice for legal purposes – would then be sent to the recipient selected by the customer.*
>
> *When the service provider performed a legal compliance audit of this system, it was revealed that assessing the legal compliance of this system with the rules of the eInvoicing Directive was difficult, because the authenticity of the origin of the invoice did not result directly from the advanced (or even qualified) electronic signature that was applied to the PDF file (which referred to a certificate of the service provider). In addition, although the service provider's end-to-end workflow was very secure, the integrity of the content of the invoice did not only result from the use of an advanced or qualified electronic signature, but also from secure communications between the service provider and the customer, as well as extensive audit trails. For these reasons, it was difficult to asses that "the authenticity of the origin and the integrity of their content are guaranteed "by means of" an advanced electronic signature, even though the service provider's platform was innovative and at least as secure as platforms that rely on EDI methods to secure invoices.*

4.3. A moving target

4.3.1. The EEI Report

As previously noted, the current electronic invoicing framework is *on the move*.

In July 2007, the European Commission Informal Task Force on E-invoicing completed its report on Electronic Invoicing (hereinafter the "EEI Report") [207]. This report highlighted the fact that Electronic

[207] European Electronic Invoicing (EEI), Final Report, Document Reference EEI-3.2, available at http://ec.europa.eu/information_society/eeurope/i2010/docs/studies/eei-3.2-e-invoicing_final_report.pdf

Invoicing "penetration and adoption" [208] in Europe to be limited, irrespective of the fact that several cases have evidenced that the use of electronic invoices may lead to significant savings.

The EEI Report identified three levels of barriers for electronic invoicing:

- **Standardisation** – A significant number of technical specifications for electronic invoicing are currently in use. Unfortunately, none of these specifications are a perfect fit for the mass-market. According to the report, further standardisation work is necessary to decrease the need for costly integration and improve interoperability between existing European standards and solutions. An international e-invoice standard should also be developed. A common international (ISO) European Electronic Invoice standard would also avoid the need for interim European standards, which will be costly to amend or replace in the longer term.

- **Trust and Operational** – Risks associated with the electronic exchange, automated processing and storage of invoices will have to be reduced. Whether an invoice is sent in paper form or via electronic means has no bearing upon the level of trust between the trading partners involved. It is to be expected that business and financial controls will be applied for an e-invoice, as they would for its paper equivalent.

- **Legal** – E-invoicing lies at the crossroads of several areas of legislation (mainly VAT, accounting, payment, authentication, company transparency and data retention). This adds complexity and uncertainty to the implementation of any e-invoicing solution for both the supplier and buyer, as well as for the vendor or the service provider. Moreover, there is currently no certification of e-invoicing solutions in place, or indeed harmonised legal or administrative practices between Member States.

The EEI Report therefore endorsed the creation of an EEI Steering Committee with the purpose of harmonizing approaches in order to establish an "umbrella EEI Framework"[209].

Following publication of the EEI Report, and as per the recommendations set out therein, the Commission has appointed a group of experts with a mandate to prepare a European e-invoicing Framework by the end of 2009. One of the tasks of the Expert Group is to identify those shortcomings in the regulatory framework for e-invoicing at Community and Member State level that prevent the Community economy exploiting its full potential[210].

4.3.2. *The Mid-Term Report*

On 27 January 2009, the Expert Group released its Mid-Term Report[211].

In order to help remove the barriers to massive adoption of electronic invoices, the Mid-Term Report sets several initial recommendations and identifies priorities.

This Report calls for the *"principle of equal treatment of paper and electronic invoices with no distinction between invoicing carried out on a domestic or on a cross-border basis within the EU."* [212] The Report suggests that it is not advisable to place additional demands on *"electronic invoices as they generally are*

---

[208] *Ibid.*, p. 4

[209] EEI Report, p. 4

[210] *Ibid.*, Article 2, paragraph 3.,(a)

[211] Mid-Term Report of the European Commission Expert Group on e-Invoicing, available at http://ec.europa.eu/internal_market/payments/docs/einvoicing/report-2009_01_27_en.pdf

[212] Mid-Term Report – section 1.3, p. 5

more secure and less prone to fraud than paper invoices"[213]. In the same paragraph, it is also mentioned that "*the threshold to electronic invoicing must be lowered and be unified especially in the VAT auditing dimension*". This is indeed a sound position, which aligns with the increased convergence of the online and offline environment, and constitutes a message to all stakeholders towards the massive adoption of electronic invoice.

4.3.3. The new proposal

Following the recommendations of the Expert Group and an open consultation, the Commission published its "Proposal for a Directive amending Directive 2006/112/EC on the common system of value added tax as regards the rules on invoicing" [214]. In the proposal, the Commission notes that in order to promote e-invoicing, the proposal aims to eliminate the barriers to e-invoicing by removing the differences between electronic invoices and traditional paper invoices. Accordingly, a new article 218a holds that *"Member States may not impose on taxable persons any obligations or formalities, other than those laid down in this Chapter and Chapter 4, in relation to the issue or storage of invoices, irrespective of whether the invoices are sent or made available by electronic means or sent on paper."*

Taking into account the many issues that plague the current e-invoicing legal framework, we fully endorse this proposal and strongly recommend its adoption.

5. E-archiving

5.1. Introduction

Electronic document management and electronic information transmission constitutes an extensive part of commercial and administrative activities. However, paper documents are not likely to completely disappear as electronic documents take the front seat: individuals still often fall back on the use of paper when dealing with crucial information, such as important contracts.

One of the reasons leading to the distrust in electronic documents has been identified as the **lack of security** on the possibilities for storing electronic documents on a longer term[215]. Although the lack of trust in electronic documents has been pointed out as an issue when it comes to regularly using such documents as complete replacements of paper documents, one of the most difficult issues faced with regard to e-archiving refers to the **cross-border context** within an electronic environment.

5.2. E-archiving and EU legislation

On 27 January 2009, the Expert Group on E-Invoicing adopted its mid-term report[216] providing for an outline of the overall progress made during the first year of the group's mandate and represents an important step towards the final proposal of the EEI Framework[217]. Upon publishing this report, stakeholders were invited to provide their comments and a summary was drawn[218]. According to the

---

[213] Mid-Term Report – Section 1.4.2, p. 7

[214] COM(2009) 21 final, 28 January 2009

[215] J. DUMORTIER, "E-Government and Digital Preservation, E-Government: Legal, Technical and Pedagogical Aspects", *Publicaciones del Seminario de Informatica y Derecho, Universidad de Zaragoza*, 2003

[216] Mid-Term Report of the European Commission Expert Group on Invoicing, 27 January 2009

[217] Feedback on Comments Received on the Mid-Term Report of the Expert Group on E-Invoicing, 6 April 2009

[218] *Ibid.*

summary of the comments received, some respondents[219] specifically called for more clarity and harmonisation of archiving requirements.[220]

Diverging implementation of the rules governing e-archiving hinder the use of electronic invoices. Although the issuer was given the prerogative to choose the place of storage of electronic invoices[221], for example, some Member States have imposed additional conditions concerning notification requirements to tax authorities and periods and terms of storage.

> *For example, France allows storage outside of its national borders, but only in countries that have signed mutual assistance agreements. Conversely, Germany only allows storage in other Member States[222].*

Reference to e-archiving within E-Commerce at the EU level is found in the eInvoice Directive, as well as in the eCommerce Directive itself:

- In the absence of a set of rules and requirements specifically governing archiving in the EU, a reference to transmission and storage of invoices "'by electronic means'" is found in the eInvoice Directive. This Directive has provided that *"transmission and storage of invoices 'by electronic means' means transmission or making available to the recipient and storage using electronic equipment for processing (including digital compression) and storage of data, and employing wires, radio transmission, optical technologies or other electromagnetic means"*.[223]
- In addition to e-invoices, e-archiving also applies to other elements of e-contracting. The eCommerce Directive sets forth that contract terms and general conditions provided to a recipient must be made available in a way that allows him to store and reproduce them[224]. Furthermore, an additional reference to archiving is found in article 10.1.b of this Directive, requiring service providers to provide service recipients with information on whether *"the concluded contract will be filed by the service provider and whether it will be accessible"*.

5.2.1. The eInvoice Directive

The invoice, in terms of legal reality, is one of the most important documents in business processes. It holds references relating to the customer, products delivered and services rendered. Invoices must be archived and presented to auditors to support balance sheet entries and provide internal records of transactions[225].

Audit efficiency – Electronic document archives enable quick access to information; therefore, they allow a significant increase in audit efficiency of benefit to both tax authorities and businesses. However, although there remains a lack of standardization in e-invoicing practice, and irrespective of the significant efforts currently being employed, it is important that businesses in Europe can choose the e-invoicing technologies, business control framework and processes that better suit their particular circumstances.

---

[219] Contributions to the consultation came from six different Member States, with an additional five replies from representing bodies at the EU or global level.

[220] Feedback on Comments Received on the Mid-Term Report of the Expert Group on E-Invoicing, 6 April 2009

[221] Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernizing and harmonizing the conditions laid down for invoicing in respect of value added tax

[222] European Invoicing Final Report 2007

[223] *Ibid.,* article 2(2) paragraph 3(e)

[224] Article 10(3) of Directive 2000/31/EC

[225] Mid-Term Report of the European Commission Expert Group on Invoicing, 27 January 2009

Imposing limited options for e-invoice implementation is not only counterproductive for businesses, but also for the European economy[226].

Authenticity of the archiving – According to article 2.2.d of the eInvoice Directive, every taxable person shall ensure that copies of invoices issued by himself, by his customer, or in his name and on his behalf, by a third party, and all invoices which he has received are stored. The authenticity of the original and integrity of the content of the invoices as well as their readability must be guaranteed throughout the storage period.

Place of storage – The electronic data may be stored in any EU member State under the condition that there is online access to the electronic data. Moreover, the data can be stored outside the EU territory, but only under the additional condition that the third country guarantees the storage of invoices according to the European data protection rules. Each Member State has the possibility to opt out if there is no mutual assistance agreement with the third country. Several Member States (such as Germany) do not agree on storage outside the European Union territory. In contrast, Estonia allows storage outside the EU. Some Member States demand prior notification to the national tax authorities[227]. Nevertheless, as mentioned above, the electronic invoices can be stored on any medium provided that it guarantees the integrity, authenticity and readability of the invoices.

5.2.2. *The eCommerce Directive*

The invoice it is not the only important document in the audit trail. Other relevant documents include purchase orders, transport documents, delivery notifications and remittance advices[228]. Therefore, these other elements of e-contracting also need to be duly archived.

Article 10.1.b of the eCommerce Directive holds that information on whether *"the concluded contract will be filed by the service provider and whether it will be accessible"* must be provided to service recipients. Additionally, article 10.3 of this Directive holds that *"contract terms and general conditions provided to a recipient must be made available in a way that allows him to store and reproduce them"* [229]. All of these documents need to be auditable and accessible. In order to ensure this, they must be properly archived.

Article 10 of the eCommerce Directive aims to provide transparency as well as consumer protection in on-line transactions[230]. For purposes of this section on e-archiving under the electronic contracting regime, article 10.1.b and 10.3 are of particular importance whereby the service provider must inform the recipient of whether the *"concluded contract will be filed by the service provider"* and additionally that *"contract terms and general conditions provided to the recipient [of the service][231] must be made available in a way that allows him to store and reproduce them"*.

---

[226] Code of Practice on Electronic Invoicing in Europe, 24 March 2009

[227] EEI final report

[228] *Ibid.,* at p. 5

[229] Article 10(3) of Directive 2000/31/EC

[230] See A. MURRAY, "Contracting Electronically in the Shadow of the E-commerce Directive, in The New Legal Framework for E-Commerce" in L. EDWARDS, *Europe*, 2005

[231] With reference to Article 10(1) of the eCommerce Directive where information requirements are between the "service provider" and the "recipient of the service"

Service providers tend to keep copies of their concluded electronic transactions[232] for their record keeping and in the event of any future dispute. Accordingly, in view of this practice, service providers are better poised than consumers to maintain adequate archiving IT systems.

5.3. Requirements

Readability – The eInvoice Directive requires a guarantee of the readability of the electronic invoices during the storage period. An invoice is considered readable if all components of the corresponding record and optional electronic signatures may be retrieved and viewed on screen or printed in a way to be understood by a person.

Format and duration of storage – Member States can impose conditions on storage. They can opt for storage of the original format as well as storage of data guaranteeing the authenticity of the original and the integrity of the content. Member States like Belgium, Cyprus, France, Denmark, Hungary, Ireland, Latvia, Lithuania, Malta, Portugal, Slovakia, Slovenia, Spain and Sweden have imposed the requirement that invoices must be received in original format. Some, however, do not impose this requirement for issued electronic invoices, such as Cyprus, France, Ireland and Portugal[233].

Period of storage – The duration of storage is not harmonised at the European level. Member States are to determine the period for which invoices must be stored by taxable persons relating to goods or services supplied in their territory and invoices received by taxable persons established in their territory[234]. Electronic archive records need to be stored for five years in Denmark, seven years in the UK and ten years in Germany[235]. The average period is ten years. The Code of Practice on Electronic Invoicing has provided a guideline for storage whereby the audit trail maintained by businesses must be accessible for six years[236].

6. Digital evidence

6.1. Introduction

New technologies have exponentially increased the creation of electronic documents within organisations. More than 3 trillion of e-mails are sent in the world every year. More than 90% of the documents in an organisation are electronic and less than 30% are finally printed.

The use of the digital means and the virtual environment is not exempt from dishonest use and traditional evidence is moving from paper support to a virtual environment. As more and more transactions from the commercial world, government and private individuals exist only in digital form, the only way in which someone can prove that something has happened – or has failed to happen – is via digital evidence[237].

---

[232] M. DEMOULIN, "Information et transparence sur les réseaux" in *Le Commerce Électronique sur les rails?*, Bruylant, Brussels, 2001, p. 121

[233] Electronic Invoicing challenges In Europe, the Computer Technology Industry Association

[234] eInvoice Directive

[235] See www.efstechnology.com/pdfs_whitepapers/e-invoicing_whitepaper.pdf

[236] See Code of Practice on Electronic Invoicing in Europe, 24 March 2009. One of the core principles includes "Auditability: Businesses must be able to demonstrate and explain their administrative and control capability. Businesses must maintain an audit trail, including the underlying transaction data and any relevant supporting documentation and data, which must accessible towards external auditors, both statutory and tax. Accessibility must be ensured for six years."

[237] Information Assurance Advisory Council "Directors' and Corporate Advisors' Guide to Digital Investigations and Evidence", Second Edition, January 2009

In this context, management procedures and admissibility criteria are undergoing changes with regard to traditional evidence[238].

The importance of digital evidence grows proportionally to the growth of e-commerce in the European Union. The gap between domestic and cross-border e-commerce is widening, however. 71 % of consumers have indicated that a major inhibiting factor to their cross-border purchases are cross-border enforcement and redress while 39% of consumers think that it is harder to resolve problems such as complaints, returns, price reductions, or guarantees when purchasing from providers located in other EU countries[239]. Therefore, having to present electronic data in possible disputes is a very common scenario.

Between September and November of 2003, the open consultation on legal barriers in e-business took place. Among the reported cases was the question of legal validity of various types of electronic documents used in commercial transactions[240]. It was noted that the legal recognition of the various types of electronic documents used in business processes is not always ensured. This is, inevitably, a matter of great concern for companies – trade documents and receipts are not always legally recognised in electronic format by competent authorities[241].

Companies, as well as individuals, need to know how to precisely turn electronic data into evidence that is unimpeachable in terms of reliability. Transaction records, business records, e-mails, and any and all other records must be turned into evidence. Among other things, digital evidence may include e-mails, webpages, word processing files, data bases stored in memories of computers and servers (located in the users' facilities or some other place that user is not aware of and can only be accessed via a URL[242]), magnetic disks, optical disks and flash memory[243].

Computer systems have back-up procedures, even if only to enable rapid recovery after a disaster. Back-up archives prove to be extremely important sources of evidence as they can show if "live" files have been tampered with and can provide data which has been deleted from the "live" system[244]. However, this does not solve the problem of customers wishing to present evidence in case of a dispute; servers and server software are provided by the service provider, leaving the customer in a more vulnerable position.

6.2. (Non-)existing legal framework

The legal framework in the European Union does not provide any specific regulation on digital evidence. Across the European Union, legislation by Member States varies. Each Member State regulates e-evidence basically by analogical interpretation of existing rules of traditional evidence. Currently, the legal domestic rules of Member States differ as well as the case law on this matter.

---

[238] I. FREDESVINDA, "The Admissibility of Digital evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study"

[239] Commission Staff Working Document: "Report on cross-border e-commerce in the EU", February 2009 available at http://ec.europa.eu/consumers/strategy/docs/com_staff_wp2009_en.pdf

[240] Commission Staff Working Paper, Legal barriers in e-business: The results of an open consultation of enterprises

[241] *Ibid.*, at p. 17

[242] Uniform Resource Locator: an address of a web page, ftp site, audio stream or other Internet resource

[243] B.J. ROTHSTEIN, R.J. HEDGES and E.C. Wiggins, "Managing Discovery of Electronic Information: A Pocket Guide for Judges", Federal Judicial Center 2007 available at www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf

[244] *Ibid.,* p. 23-24

Hurdles created – The lack of a relevant legal framework for digital evidence in the European Union is a major impediment for efficient cross-border use of digital evidence. The lack of uniformity and legal criteria causes domestic regulations to very often be burdensome and poorly regulated (for instance, a lack of measures related to the authenticity of evidence or the right to data protection). Additionally, unsatisfactory and diverging jurisprudence along with the lack of relevant technical infrastructure creates further obstacles. As a result, this creates difficulties in proving the authenticity, readability, integrity and origin of electronic data, as well as the legal validity of digital evidence[245].

AEEC project – In November 2005, a group of European multidisciplinary experts started to set out the different methods by which digital evidence is adduced in the courts of sixteen member states under the Admissibility of the Digital evidence (A.E.E.C.) project. European judges, lawyers, prosecutors, law enforcement bodies which were interviewed consider that a European legal framework on e-evidence is necessary because it will help with the legal national development of the issue and further help to develop legislations concerning e-evidence in a uniform way, especially when considering the trans-national character that this type of evidence has. Moreover, it would facilitate the international cooperation between judges since, within the same country and under very similar cases there is diverging case law and a lack of homogeneity of criteria[246].

As a result of the findings of the A.E.E.C. project, procedural standards were not found to include any specific procedure regulating the collection, preservation, and presentation of digital evidence in court. Nonetheless, investigators have observed how countries usually apply by analogy the general rules and procedures for the traditional evidence: 48 percent of the rules analysed contemplate procedural processes that can also be applied for digital evidence[247].

Interestingly, the deep legislative review conducted under the A.E.E.C. project in sixteen Member States[248] showed that there is not even an accepted definition "digital evidence". However, there are some precepts referring to "digital evidence" in some way.

> *For example, the Finnish legal Proceedings Code refers to "deeds that support action" [249] meaning both the digital support and the paper support. A more direct reference was found in the Police & Criminal Evidence Code of the United Kingdom: "evidence is all information contained in a computer" [250].*

In the majority of European countries there are several definitions of e-evidence, separate for civil and criminal law, etc[251]. The different legislation of the European countries[252] does not establish any specific definition on e-evidence, nor does it specifically regulate digital evidence. Instead, digital evidence is regulated through the analogical interpretation of traditional evidence.

---

[245] I. FREDESVINDA, "The Admissibility of Digital evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study"

[246] The need of a European legal framework concerning Digital evidence (I. FREDESVINDA, Strategic Development Manager, CYBEX)

[247] I. FREDESVINDA, *o.c.*

[248] Austria, Belgium, Denmark, Finland, France, Germany, Greece, Holland, Ireland, Italy, Luxembourg, Portugal, Romania, Spain, Sweden, and the United Kingdom.

[249] Legal Proceedings Code of Finland. Chapter 17, Section 11b

[250] Police and Criminal Evidence Act, PACE

[251] The admissibility of digital evidence in the Courts, CYBEX initiative

[252] Study was undergone of the legislation currently in force in each of the following countries: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Holland, Ireland, Italy, Luxembourg, Portugal, Romania, Spain, Sweden, and the United Kingdom

7. Conclusions

1. The eCommerce Directive has **fulfilled its role of initiating cross-border electronic contracting**, by imposing the principle of equal treatment of electronic contracts, by removing the legal obstacles for the use of electronic contracts, and by harmonising important aspects of electronic contracting. Nevertheless, some issues have surfaced.
2. **Articles 10 and 11** impose several basic contracting requirements for online service providers. While article 10 describes the requirements to be met before the conclusion of the contract (which concern primarily information duties), article 11 describes the ordering procedure.

   While these requirements were answers to valid concerns at the time the eCommerce Directive was drafted, they have now either become **too evident**, have become a **stumbling block** for new technologies and business models, mainly lead to **increased compliance costs** and/or **overly protect consumers**. Furthermore, they discriminate against the offline contracting process, which is free from formalities in most cases and in most Member States. Moreover, the eCommerce Directive does not deal with real issues nowadays, such as unreadable and lengthy terms and conditions.
3. The **eSignatures Directive** has reached its first objective of requiring all Member States to legally recognise e-signatures. However, it has not succeeded in getting companies and consumers to actually use electronic signatures on a large scale in a day-to-day context[253]. Major hurdles include a lack of technical interoperability and market acceptance. We therefore welcome the Commission's Action Plan on e-signatures, which aims to offer a comprehensive and pragmatic framework to achieve interoperable e-signatures.

   An unresolved issue remains the long-term validation of e-signatures. This issue also requires to be addressed on a mainly technical level rather than from a legal perspective.
4. **Electronic invoicing** also suffers from insufficient market adoption. Contrary to the eSignatures Directive, however, the current legal framework is at least partially responsible. The current eInvoice Directive is plagued by a lack of harmonisation, legal clarity (*e.g.,* whether legal entities can sign invoices), diverging Member State implementations (*e.g.,* whether qualified or advanced electronic signatures are required) and unnecessary discrimination against electronic invoices. However, the proposal for a new eInvoice Directive seems to resolve these issues.
5. The legal framework in the European Union does not provide any specific regulation on **digital evidence**. Across the European Union, legislation and case law by Member States in this area varies. Each Member State basically regulates e-evidence by analogical interpretation of existing rules of traditional evidence.

8. Recommendations

8.1. Article 5 of the eCommerce Directive

The European Court of Justice ruled that when a recipient of a service, after contacting the service provider by electronic means, is either on a journey, holiday or a business trip, and therefore deprived of access to the Internet, communication by an enquiry template can no longer be regarded as "effective" within the meaning of article 5.1.c of the Directive. The service provider would have to provide "access to a non-electronic means of communication". Ultimately, the ECJ ruled that the requirements of the *"direct and permanent"* means of communication were not sufficiently met by an e-mail address and, as such,

[253] Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, 28 November 2008, COM(2008) 798 final ("Action Plan")

online service providers must also display either a telephone number or, alternatively, a web response form that is answered in thirty to sixty minutes.

The focus of the ECJ was on consumer protection and failed to take into account that not all service providers have large business models that would allow for a permanently accessible telephone line at any time of day. Moreover, the ruling was not very clear and created additional uncertainty on how service providers should be organised in order to comply with the ruling.

In order to avoid any further (mis)interpretations of the wording in this provision, and to make this provision technology-neutral, we recommend to change article 5.c to *"those electronic contact details of the service provider that are appropriate considering the nature of the information society service considered"*.

8.2. Article 9.2 of the eCommerce Directive

The purpose of article 9 of the eCommerce Directive is to require Member States provide equivalence for e-documents in all contractual matters, except those listed as exceptional in section 9.2. The exceptions in article 9.2 should be further analysed and reconsidered in the short term, as the Directive was drafted at a time where technologies were not in place that could offer the same level of security as the "traditional" offline solutions. If the exceptions in this provision are not removed, the message conveyed is that electronic contracting is only adequate for minor transactions. In the medium and long term, these exceptions should be removed as Member States become increasingly digitalised and trust grows in the use of technology.

Real estate – The "badge of formality" [254] already referred to and associated to written documents may subsist with adequate implementation of technology. Real estate transactions often require that a notary be present. This third party adds to the "badge of formality" required by those involved in such transactions. However, the continued development of technology for online notarisation will likely mitigate this (*e.g.,* the use of e-Notary applications in Estonia[255]).

Involvement of the courts – As technology develops, and assuming that Member States will follow the current tendencies of digitising their public services, courts will likely go digital as well. As in the case of Portugal's e-Government project[256], the submission of documents to the court may be done through electronic means. Therefore, in the long term we recommend this exception be removed.

Contracts of suretyship – This consumer protection provision was the result of considerable lobbying as there was a concern that if security agreements were digitised, the degree of formality which is necessary to communicate to consumers the gravity of the agreement they are entering into would be removed. Given the nature of this exception, it is recommended for the medium term that this exception be removed. A short term recommendation is not considered necessary as the inclusion of this exception in article 9.2.c.

Family and succession – Although this exception may just have been included as an act of respect for family, as technology develops and Member States digitise, family and succession services will be available electronically (divorce certificates, wills, etc.). It is recommended for the medium term that this exception be removed.

---

[254] A. MURRAY, D. VICK & S. WORTLEY (1999) "Regulating E-Commerce: Formal Transactions in the Digital Age", *International Review of Law, Computers & Technology* (Vol. 13(2)), p. 131-133

[255] EULIS – European Land Information System at www.eulis.eu/countries/profile/estonia

[256] www.epractice.eu/en/document/288346

8.3. Article 10 of the eCommerce Directive

The eCommerce Directive lays down minimum information standards required for electronic contracts in article 10. This provision aims to provide transparency, as well as consumer protection in on-line transactions, by requiring service providers to provide service recipients with the information therein. However, the wording and structure of this provision calls for further analysis and must undergo some adjustments in order to ensure it is coherent and in line with today's reality.

Removing article 10 – Preferably, we recommend to simply delete article 10, as its requirements have become either too evident, have become a stumbling block for new technologies and business models, mainly lead to increased compliance costs, and partially duplicate the protection measures found in other consumer directives.

When this drastic solution is not viable, we recommend to at least incorporate the following changes.

Article 10.1.b – The service provider must inform the recipient of *"whether or not the concluded contract will be filed by the service provider".* According to the wording in this information requirement, it is clear that the service provider is not required to file a copy of the concluded contract. In other words, *"whether or not"* indicates that it is the service provider's prerogative to either file or not store the contract. It is common practice for service providers to keep copies of their concluded electronic transactions for their record keeping; there may be a future dispute.

In light of this common practice, service providers are better poised than consumers to maintain adequate archiving IT systems. In order to align this information requirement with the consumer protection nature of the provision, it is recommended that in the short term the wording of this provision be changed so as to require the service provider to inform the recipient that the contract has been filed and additionally inform on where it can be accessed.

Article 10.1.d – This provision requires service providers to provide recipients with information on "*the languages offered for the conclusion of the contract"*. This provision, clearly drafted to ensure consumer protection, results in a redundancy. That is, when a consumer visits a website, the language of the website is most likely to be the language of the contract. This is the result of common practice for on-line activities. Only in the event this is not the case should service providers be required to inform recipients that the language offered in their website is not the language the contract is available in. Therefore, it is our recommendation that this provision be amended so as to require service providers to inform recipients on the languages offered, only in the event that the contract is offered in a different language.

Article 10.2 – Paragraph 1 of this provision sets forth that the information requirements therein shall be given by the service provider to service recipients *"clearly, comprehensibly and unambiguously… except when otherwise agreed by the parties who are not consumers"*. Paragraph 2, however, also sets forth an information requirement to provide information on *"any relevant codes of conduct"* to which the service provider has subscribed. In fact, both paragraphs 1 and 2 include exception on *"when otherwise agreed by the parties who are not consumers".* It is therefore not clear why the information requirement on codes of conduct was not included in the list of information to be provided in paragraph 1. In fact, codes of conduct, when followed by the service provider, proves to be an important piece of information that enlightens the (potential) service recipient on the rules the service provider follows.

It is therefore recommended that the information requirement in article 10.2 on codes of conduct be included in the list of information in paragraph 1 of this provision so that this information is also provided *"clearly, comprehensibly and unambiguously".*

Article 10.3 – As noted in the preceding paragraph, both paragraphs 1 and 2 of article 10 include an exception to B2B contracts whereby the information requirements therein will not be applicable *"when*

otherwise agreed by the parties who are not consumers". Although article 10 is an evident consumer protection provision, the choice was made to expressly make reference to this exception. This was not done, however, in paragraph 3 of this provision. As it is not clear, when compared to the preceding paragraphs in the provision, whether the requirement on *"contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them"* is applicable to consumers (B2C) or businesses (B2B), or whether this is a general requirement applicable to both, it is recommended that this paragraph be amended so as to clarify this.

Length of terms and conditions – We recommend the Commission to adopt sector-specific, concise templates of terms and conditions, and to incentive service providers to use these templates. An interesting idea would also be to create a set of "boiler plate" standard clauses, whereby the actual terms and conditions of a service provider would only need to list clauses that deviate from the boiler plate standard clauses. This would drastically reduce the length of terms and conditions. Preferably, the use of such templates would also be integrated in trustmarks[257].

8.4. Article 11 of the eCommerce Directive

Removing article 11 – As is the case with article 10, we recommend to simply delete article 11. However, when this solution is not viable, we recommend to at least incorporate the following changes.

Technology dependence – As the "contractual process" in the eCommerce Directive is very difficult to implement for mobile services, and may not be suitable for future technologies, it is our recommendation for the long term that the specifics of these technologies and the services they offer be taken into consideration as they may need to be governed by a separate legal framework.

Removing the confirmation requirement – Pursuant to article 11, if a service provider fails to send a confirmation to the consumer issuing acknowledgment, no contract is formed. This formality discriminates against electronic contracts, and should be removed, or at least made compatible with business models and technologies other than traditional webshops.

8.5. E-invoicing and e-archiving

E-Invoices – Taking into account the many issues that plague the current e-invoicing legal framework, we fully endorse the Commission's new eInvoice Directive proposal. We strongly recommend its adoption.

E-archiving – As one of the most important documents in business transactions, invoices must be duly archived. Given the narrow relationship between e-archiving and e-invoicing, it is recommended for the short term that the pending Final Report of the Expert Group include harmonisation rules on e-archiving in addition to e-invoicing.

8.6. Digital evidence

Given the lack of certainty caused by the absence of a legal framework for digital evidence in the EU and the diverging rules applicable to e-discovery and e-evidence within the Member States, it is our recommendation for the short term that digital evidence be an issue of priority and the object of further study and analysis. These studies should identify the applicable rules governing digital evidence in the Member States as well as identify the necessary steps towards eliminating the current cross-border related issues.

---

[257] See our recommendation in Chapter 13 - self regulation

In the medium term, we recommend to harmonise the digital evidence rules within the EU, because such harmonised legislation on digital evidence currently constitutes the "missing link" in the spectrum of legal instruments relating to e-contracts. All other steps found in a typical contractual process are already covered by other Directives (from the ordering process to the signature of the order and the invoicing process).