

# Chapter 2

## Cyberlaundering: Concept & Practice

### 2.1 Deciphering Cyberlaundering

#### 2.1.1 *The Meaning of Cyberlaundering*

The definition of cyberlaundering should necessarily reflect both the money laundering and cyber crime elements of it.

Money laundering is something that occurs every time any transaction takes place or a relationship is formed that involves any form of property or benefit, whether it is tangible or intangible, which is derived from criminal activity.<sup>1</sup> It is a process crime which, invariably, is not aimed directly at a person or property but against the machinery of justice itself.<sup>2</sup> Much like the logic behind other process crimes, such as obstructing the course of justice, contempt of court, and perjury, money laundering is effected by masking or hiding the predicate (or underlying) offence through a web of deceitful and evasive processes.

Cyberlaundering, however, adds a technological perspective to this because it also traverses the much broader terrain of cyber crime. Cyber crime can be defined as an act, which is punishable by law, using an automatic electronic device that performs mathematical or logical functions,<sup>3</sup> for example, a computer. The interplay with cyberlaundering occurs when the relevant ‘act’ in question is that of money laundering.

Therefore, in light of this, the following definition of cyberlaundering is proffered:

---

<sup>1</sup> Hopton (2009, p. 2). See previous discussions in Chapter 1.

<sup>2</sup> Murphy (2009, p. 1).

<sup>3</sup> Cf Reyes et al. (2007, p. 33); Koops and Brenner (2006, p. 20) and Wall (2007, p. 12). See previous discussions in Chapter 1.

Cyberlaundering is the use of a computer<sup>4</sup> to form a transaction or a relationship involving property or benefit, whether tangible or intangible, which is derived from criminal activity.

Although the computer is the tool, the playing field remains the internet, hence the need now to explore the internet as a playing field for money launderers.

### ***2.1.2 Catalysts of the Cyberlaundering Dilemma***

In order to fully grasp the concept of cyberlaundering, one has to know how it evolved. The phenomenon of cyberlaundering was triggered with the advent of the internet, which criminals have come to use to ply their trade of money laundering. Some of the unique features and traits of the internet that form the blueprint upon which cyberlaundering thrives are further discussed.

Computers today are designed in such a way that they are able to process data at an extraordinary speed, thanks to the capabilities of the computer's central processing device ('CPU'). The CPU is measured in giga hertz ('GHz'), which determines the speed with which data is processed. What also determines speed is the computer's Random Access Memory ('RAM') and the graphics card.<sup>5</sup> The former refers to a depository where current files are being used or stored. Hence, with a very fast RAM, easy access to one's files can be guaranteed. The graphics card on the other hand is the hardware that processes graphics. With a very fast graphics card, more graphics, or displayed images or frames, can be processed per second, which is crucial for computer and online gaming.<sup>6</sup> The speed of computers is further complemented by an equally fast internet service. With the transition from dial-up internet access to broadband internet access—the latter averaging about four megabytes per second, as opposed to the former's 60 kilobytes per second—a high data rate connection is guaranteed.<sup>7</sup>

It is certainly not far-fetched to think that cyberlaundering is linked directly to all these basic features of technology, because without these features, the notion of cyberlaundering will be non-existent. This becomes clearer in the discussion on cyberlaundering methods and techniques.

Another catalyst of the cyberlaundering dilemma is access to the internet. The internet is the virtual playground for cyberlaundering. Evolving originally from

---

<sup>4</sup> See paragraph 4.4.1 below.

<sup>5</sup> Cf Shelly and Vermaat (2010, p. 9) and Molly and Parker (2010, p. 23).

<sup>6</sup> Molly and Parker (2010, p. 23). Online gaming refers to gaming activities that occur within the environment of the internet.

<sup>7</sup> Cf Shelly and Vermaat (2010, p. 44).

several military projects of the United States government in the late 1960s,<sup>8</sup> the internet today aids cyberlaundering because it has become a common luxury for all, given its ubiquitous nature and presence. In its early days, which is the 1990s,<sup>9</sup> the internet was popular only amongst businesses and households, mainly in the United States (US) and the United Kingdom (UK). This popularity was based on an increased awareness of the internet's functionalities and infinite capacity. This is why it can be said that cyberlaundering is borne out of the globalization of the internet. Gone are the days when only an elite class of people had sole access to such opulence. Today the world is a global village, thanks to the internet. But for certain human activities that cannot be done on the internet, such as eating and drinking (at least not yet), numerous things are doable on the internet.

Access to the internet continues to grow. Statistics show that over 2 billion people, of a world population of more than 6 billion people, have access to the internet.<sup>10</sup> In the previous decade, this number was a measly 360 million.<sup>11</sup> The number increased by a solid 480% between the years 2000 and 2011.<sup>12</sup>

The fact that one's everyday life basically revolves around the internet has caused it to be an indispensable resource for numerous human activities. Accessibility to the internet has become a hotly contested topic, and the debate has even shifted onto the legal sphere, giving rise to many deliberations over the years. In 2003, during the United Nations World Summit on the Information Society, it was proposed that access to the internet should be entrenched as a fundamental human right.<sup>13</sup> Since then, several countries such as Finland, France, Greece, Spain and Estonia have made access to the internet a part of the basic fundamental rights of an individual.<sup>14</sup> This shows the seriousness and importance of the issue of internet accessibility. In the aforementioned countries, and in others as well, it goes without saying that having access to the internet in modern times is crucial for all individuals. It is almost now on the same pedestal as the right to life. The International Telecommunications Union ('ITU') has also joined in the campaign to globalize access to the internet, and has spearheaded several projects across multiple continents in order to achieve this goal.<sup>15</sup> The European Union ('EU') is also hard at work ensuring that the right

<sup>8</sup> Living Internet (an undated internet article) 'History of the Internet' available at <<http://www.livinginternet.com>> [accessed on 10 February 2013]. Cf Ryan (2010, p. 3).

<sup>9</sup> Cf Ryan (2010, p. 3) and Living Internet (an undated internet article) 'History of the Internet' available at <<http://www.livinginternet.com>> [accessed on 10 February 2013].

<sup>10</sup> A breakdown of the figure shows the following: In Africa, there are about 118, 609, 620 people; in Asia 922, 329, 554; in Europe 476, 213, 935; in the Middle East, 68, 553, 666; in North America, 272, 066, 000; in Latin America, 215, 939, 400, and in Oceania/Australia, 21, 293, 830 people. See Internet World Stats <<http://www.internetworldstats.com/stats/htm>> [accessed on 15 July 2013].

<sup>11</sup> Internet World Stats <<http://www.internetworldstats.com/stats/htm>> [accessed on 15 July 2013].

<sup>12</sup> Internet World Stats <<http://www.internetworldstats.com/stats/htm>> [accessed on 15 July 2013].

<sup>13</sup> World Summit on the Information Society (2003, p. 1). Cf Lucchi (2011, p. 646).

<sup>14</sup> British Broadcasting Cooperation <<http://news.bbc.co.uk/2/hi/8548190.stm>> [accessed on 15 July 2013].

<sup>15</sup> For more information on the projects of the ITU see <[http://www.itu.int/africainternet2000/Documents/doc7\\_e.htm](http://www.itu.int/africainternet2000/Documents/doc7_e.htm)> [accessed on 15 July 2013].

to internet access is safeguarded. This is evidenced by the EU Amendment 138/46 of the Telecommunications Reform Package,<sup>16</sup> now article 1(3)(a) of the Framework Directive,<sup>17</sup> which is to be adopted into law in all EU countries that are states parties.

Other countries that share this notion, but that have yet to entrench it as a fundamental human right, are South Korea, Mexico, Brazil, Turkey and Nigeria.<sup>18</sup> In the same survey conducted, results show that these countries feel strongly against government regulation of the internet, although a majority of other countries in Asia and Europe have disagreed.<sup>19</sup>

Furthermore, access to the internet has not only become affordable, but also convenient, especially with the notion of cloud computing.<sup>20</sup> The latter means anything that involves delivering hosted services over the internet and it works in such a way that one can gain access to data/information contained in a hosted service on the internet, using different computers.<sup>21</sup> What is more, in this modern age, a computer need not be a desktop or laptop apparatus; it could also be a phone or any personal digital assistant ('PDA').

One very glaring fact is that easy accessibility to the internet on a global scale will spiral in growth over the next couple of years, as statistics have shown. As a downside, without efficient regulators in place to minimize its abuse, especially for purposes of money laundering, the phenomenon of is bound to grow concomitantly.

---

<sup>16</sup> COM (2007) 697 and COD/2007/0247.

<sup>17</sup> Council of Europe: Council Directive 2009/136/EC, on universal service and users' rights relating to electronic communications networks and services, adopted by the Parliamentary Assembly on 25 November 2009 and came into force on 18 December 2009. Cf Article 1 of the Council of Europe: Council Directive 2002/58/EC, on the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws adopted by the Parliamentary Assembly on 12 July 2002 and came into force on 31 July 2002.

<sup>18</sup> British Broadcasting Cooperation available at <<http://news.bbc.co.uk/2/hi/8548190.stm>> [accessed on 15 July 2013].

<sup>19</sup> Government interference or regulation of the internet has always been a sensitive issue. As this study shows, regulation of the internet is very expedient in order to prevent problems such as cyberlaundering that plague economies the world over. However, the main issue is not whether or not regulation should occur, but the extent of it. For instance, in the United Kingdom ('UK'), the controversial Digital Economy Act 2010 (Chapter 24) promises to deliver universal broadband in the United Kingdom (UK) by 2012. This law gives regulators new powers to disconnect or slow down the internet connections of illegal file-sharers and other cyber criminals. Countries such as France and Germany are also considering introducing similar laws. British Broadcasting Cooperation <<http://news.bbc.co.uk/2/hi/8548190.stm>> [accessed on 15 July 2013].

<sup>20</sup> Searching Cloud Computing (an undated website document) 'Cloud Computing' available at <<http://searchcloudcomputing.techtarget.com/definition/cloud-computing>> [accessed on 15 July 2013].

<sup>21</sup> Cloud computing differs significantly from a traditional hosting service, as it is sold on demand. The user can determine how much of the service it wants at a given time and the service is fully managed by the relevant provider. See Searching Cloud Computing (an undated website document) 'Cloud Computing' available at <<http://searchcloudcomputing.techtarget.com/definition/cloud-computing>> [accessed on 15 July 2013].

One other catalyst of the cyberlaundering dilemma is the notion of anonymity. The issue of anonymity has always been a subject of contention, even before the debate shifted to internet anonymity. Initially, the issue of anonymity was pitted against one's fundamental right to freedom of expression, free speech, privacy and so on.<sup>22</sup> This debate has been transposed onto the internet since the latter's advent. The internet has the feature of anonymity, as it allows individuals to conduct activities without disclosing their true identities or without any possible direct traceability. However, the notion of anonymity in this context differs from some of its variants, such as pseudonymity and allonymity.<sup>23</sup> The latter forms of anonymity, when used on the internet, could have good purposes.<sup>24</sup> Amongst some of the advantages that anonymity holds is its possible use by people under a repressive political regime to vent their opinion.<sup>25</sup> It could be used to disclose information that is extremely personal, such as sexual problems. It could serve as a platform to express opinions, thus promoting parity and rendering attributes of gender and race immaterial.<sup>26</sup>

Unfortunately, the few benefits associated with anonymity on the internet are overshadowed by the more glaring disadvantages. From the seemingly endless list of demerits of anonymity that are germane to the internet's framework, a criminal could spin a perfect web of transactions over the internet, thus obliterating all traces of the original act. This essentially, is what cyberlaundering is. Given the many dangers that are caused by the internet as a result of its anonymity feature, several authors have argued for a 'reconstruction' or 'restructuring' of the internet to ensure universal identification, thus completely burying the notion of anonymity.<sup>27</sup> Though logical, this argument implies, albeit generally, that one should wipe the slate clean on which the internet's framework is sketched because anonymity is part of the very fabric of the internet, and forms a core of its blueprint. The pros and cons of this argument are considered in an ensuing discussion.<sup>28</sup>

The last identifiable catalyst of the cyberlaundering dilemma is the boundless borders of the internet. For much of its life, the internet has witnessed sporadic changes in development, but a constant factor in its evolution is its incessant nature of shrinking the world into one small space. The manner in which information is accessible through the internet traverses physical borders and known boundaries. Indeed, the phenomenon of the internet defines modern times. However, such convenience has raised eye-brows and continues to spur curiosity. On the one hand, many wonder why governments of the day are overly cautious about censoring the

<sup>22</sup> See the elaborate discussion in Mandujano (2003, p. 4). Cf Reiter and Rubin (1998, p. 21).

<sup>23</sup> Pseudonymity refers to the case where one uses another's name or takes on another's persona in order to make an artistic or literary expression. Allonymity is a slight variant of the former, as it refers to a writer's assumption of an historic literary figure in a literary writing.

<sup>24</sup> Cf Joinson (2001, p. 177), Wallace (1999, p. 3) and Abelson (2001, p. 1).

<sup>25</sup> Joinson (2001, p. 177) and Abelson (2001, p. 1). Cf Palme and Berglund (2002, p. 3).

<sup>26</sup> Palme and Berglund (2002, p. 2).

<sup>27</sup> See Kiviat (2010, p. 2), Chawki (2010, p. 32) and Kirtley (2010, p. 1478). Cf for conflicting views: Moore (2009, p. 58) and Palme and Berglund (2002, p. 2).

<sup>28</sup> Cf Chapter 5, for detailed discussions.

internet, whereas, on the other hand, the fundamental right of access to information is asserted vigorously.<sup>29</sup> For the first argument, the current situation in Italy, involving the presence of the giant internet company, Google, serves as an example. The Italian government recognized YouTube<sup>30</sup> as a television station that is subject to television regulations.<sup>31</sup> This implies that Google pays taxes as a television broadcaster, and it would be liable for its contents. YouTube has been banned in several countries such as China and Morocco, as people often post videos that their governments have deemed offensive and having the capabilities of inciting anti-government protests.<sup>32</sup> Also, in January 2010, the Libyan government blocked access to the website for this reason.<sup>33</sup>

The instances cited above, however, are only isolated incidents. The fact still remains that information sharing over the internet continues to grow, and several governments, amongst them those of the United States and the United Kingdom, still promote anti-censorship and strongly uphold the rights of freedom of expression. It could therefore be said that, currently, the pendulum is swinging in favour of a borderless internet environment. The difficulty of this issue is expressed below:

The difficult area is that while countries understand the benefits of information sharing on the internet, they also see that practices such as digital terrorism, large-scale crime, fraud, spam, stalking and pornography are on the rise[...] The sensitive part of the debate, as with all debates about censorship, is not whether some of these areas need to be excluded from the internet but where the line is drawn between legitimate threat or security risk and governments taking on the role of our political, moral and ethical minders.<sup>34</sup>

The proliferation of information through the internet and the ease of gaining access to it have resulted in both good and evil, with the latter manifesting in the form of cyberlaundering, as further discussions will show.

### 2.1.3 *Categorizing Cyberlaundering*

Cyberlaundering traverses two distinct fields of crime—cyber crime on the one hand, and money laundering on the other. This makes it a hybrid discipline that poses the question: How should one see cyberlaundering, and under what category of crime does it fall? As part of the quest to understand the subject for purposes of establishing an appropriate legal framework for it, it is necessary to see it through the right lenses. From the outset, therefore, it must be fitted in the right frame. Without establishing the parameters of cyberlaundering, one may falter along the

---

<sup>29</sup> Baran (2011, p. 2).

<sup>30</sup> Youtube is owned by Google and is the world's largest video sharing website, boasting billions of users from around the world.

<sup>31</sup> Baran (2011, p. 2).

<sup>32</sup> Baran (2010, p. 1). Cf Schroeder (2007) 'Censored: List of Countries That Banned YouTube' available at <<http://mashable.com/2007/05/30/youtube-bans/>> [accessed on 10 July 2013].

<sup>33</sup> Human Rights Watch (2011, p. 65).

<sup>34</sup> Hughes (2010, p. 1).

way, as the notion itself could be ensconced in one big conceptual blur. The following discussion juxtaposes the varying possible categories into which the concept of cyberlaundering falls, or ‘lenses’ through which it should be seen.

### **Cyberlaundering as a Subset of Cyber crime**

Should cyberlaundering be couched just as a subset of cyber crime? If cyberlaundering is indeed seen as a subset of cyber crime, it would mean that it falls squarely within the area of cyber crime, without the element of money laundering. If this is the case, one may be forced to look solely to the field of informatics<sup>35</sup> to find regulatory measures for it.

However, this notion cannot be entirely acceptable. Although it is accepted that cyberlaundering has roots in cyber crime, one must not lose sight of the core element of money laundering. Hence, the crime at its core is money laundering, with a technological aspect.

### **Cyberlaundering as a Technique of Money Laundering**

Another popular school of thought on cyberlaundering considers not only the money laundering element, but sees cyberlaundering solely as a mere technique within the marquee of money laundering.<sup>36</sup> For this reason, when the method used by a criminal to launder funds is internet-based, then the conclusion is quickly drawn that money laundering has been committed through that technique. This notion might be plausible if one looks at the broad concept of money laundering, which entails several other aspects, for instance, trade-based money laundering.

It would nevertheless be entirely incorrect to accept that cyberlaundering is only a technique of money laundering. To think of something as a ‘technique’ of another would mean that the latter is a means to an end, and, impliedly, that it cannot stand on its own. As regards cyberlaundering, the fact that a criminal utilizes technological resources does not make such resources merely a tool for the money laundering enterprise; conversely, this makes the criminal’s activity the money laundering enterprise.

---

<sup>35</sup> Informatics is the science of information, the practice of information processing, and the engineering of information systems. Informatics studies the structure, algorithms, behaviour, and interactions of natural and artificial systems that store, process, access and communicate information, i.e. the computer. It also develops its own conceptual and theoretical foundations and utilizes foundations developed in other fields. Fourman (2002, p. 1).

<sup>36</sup> Some authors have described cyberlaundering in this light. See Hunt (2011, p. 133) and Filipkowski (2008, p. 4).

## Cyberlaundering: ‘Money Laundering 2.0’

So what then could be the correct conceptual phrasing of cyberlaundering? The answer lies at the heart of the crime itself, which is money laundering. A rather astute answer is that cyberlaundering is money laundering, which appears at a more advanced level, given its roots in technology. Although it overlaps with the concept of cyber crime, it should not be seen entirely in that light. Arguably, the gravity of the cyberlaundering problem, which already embodies the behemoth weight of money laundering, exceeds the severity of other kinds of cyber crimes combined.<sup>37</sup>

It is important to know the right category in which cyberlaundering falls, because understanding the right framework, would inadvertently determine the kind of liability it creates. Having accepted that cyberlaundering is money laundering, the primary liability it creates is the liability for money laundering. However, cyberlaundering is unique for the fact that it is likely to create subsidiary or ancillary liability for the criminal other than the liability for money laundering. It could incur liabilities under the broad notion of cyber crime, or other subsets of cyber crime, in jurisdictions where such crimes are recognized. Such ancillary liability differs from the traditional predicate offences that usually establish liability for the crime of money laundering. For instance, a cyberlaunderer is likely to be found liable for crimes such as hacking or cyber-vandalism, both of which might not necessarily be predicate offences for the main crime of money laundering. This comes to light in the ensuing discussion on the vulnerable industries for cyberlaundering.<sup>38</sup>

Another point that supports this conceptual phrasing of cyberlaundering is the aspect of prosecution.<sup>39</sup> When a prosecutor prosecutes individuals who have engaged in cyberlaundering activities, the name of the crime that should reflect on the charge sheet is the phrase ‘money laundering,’ not cyberlaundering.<sup>40</sup> In essence, cyberlaundering is not a separate crime from that of money laundering. It remains under the umbrella of the latter. The sad reality is that the gravity of the cyberlaundering dilemma gives rise to an escalation of the current money laundering problem. This hinges on the overall purpose of this study, which assesses the possibilities of forging a proper legal framework to counteract the problem. However, a foreseeable challenge to actualizing this goal lies in one underlying truth—cyberlaundering is a legal problem with very complex legal ramifications.

---

<sup>37</sup> This is highly debatable. One report shows that in the United Kingdom alone, banks lose up to £ 1 million per day in phishing and malware attacks. See Evron (2008, p. 1). Another report shows that, on an annual basis, an average of \$ 52 million is lost to organisations in the United States alone as a result of cyber crime attacks. See ArcSight (2010, p. 1). These statistics, however, present sector-based facts. There are not very detailed statistics showing the economic impact of cyberlaundering as yet. However, riding on the notion that over \$ 5 trillion is laundered on an annual basis (as far back as 2007), and that a substantial percentage is added through cyberlaundering, the statement would not be far-fetched. See Ehrenfeld and Lappen (2007, p. 1).

<sup>38</sup> See paragraph 2.4 below.

<sup>39</sup> See Chapter 5 for further discussion.

<sup>40</sup> This is so because of the question of legality, hence why cyberlaundering has to be conceptualized legally. See discussion in Chapter 4, paragraph 4.4.1.

## 2.2 Electronic Payment Systems: New Tools for Laundering

It was once said that money does not have to be a legal tender created by governments. Like law, language and morals, it can emerge spontaneously.<sup>41</sup> The exponential growth of electronic payment systems (e-payment systems) caused by the internet affirms this statement.

E-payment systems refer to the means through which payment can be made over the internet.<sup>42</sup> It entails a financial exchange, usually in the form of an encrypted financial instrument, such as an encrypted credit card number, digital cash or an electronic cheque, which is usually backed by a bank, an intermediary, or a legal tender.<sup>43</sup> The evolution of e-payment systems began with the concept of electronic funds transfer<sup>44</sup> (EFT) in the 1940s.<sup>45</sup> EFT gave rise to the notion of a transferable information-based data through computer and telecommunication components. The concept of EFT has now been largely replaced with electronic commerce payment systems which are online-based.

E-payment systems are becoming more institutionalised by the sheer propagation of its trust-based system,<sup>46</sup> even as established institutionalized financial infrastructures fail to fully comprehend the workings of this novelty. Similar to the terrestrial commerce systems which depend entirely on the notion of trust between strangers, the exacerbation of the e-payment system is fuelled by this rationale, because trust between its users is being forged increasingly.<sup>47</sup>

### 2.2.1 *The Concept of Illegal Electronic Money*

Cyberlaundering is based on the concept of e-payments. As a sickle is to a wheat farmer, so is electronic money, or e-money,<sup>48</sup> to a cyberlaunderer. E-money is particularly significant because of the notion of 'illegal e-money.' In the terrestrial world where the traditional notion of money laundering is the order of the day, the opposite concept exists in the form of illegal hardcash. Illegal e-money refers to

<sup>41</sup> Von Hayek (1978, p. 12). Cf Demetis (2010, p. 19).

<sup>42</sup> Business Dictionary (an undated website document) 'Electronic Payment System' available at <<http://www.businessdictionary.com/definition/electronic-payment-system.html>> [accessed on 25 July 2013].

<sup>43</sup> Manzoor (2008, p. 213). Cf IGNOU (an undated website document) 'Electronic Payment Systems' available at <<http://webservice.ignou.ac.in/virtualcampus/adit/course/cst304/ecom2.htm>> [accessed 2 August 2013].

<sup>44</sup> Electronic Funds transfer refers to the transfer of funds initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape in order to instruct or authorize a financial institution to debit or credit an account. Manzoor (2008, p. 214) and Lassila (2011, p. 54).

<sup>45</sup> Lassila (2011, p. 54) and Manzoor (2008, p. 214). Cf Geva (1992, p. 23).

<sup>46</sup> Demetis (2010, p. 19).

<sup>47</sup> Newman and Clarke (2003, p. 23). Cf Fukuyama (1995, p. 15).

<sup>48</sup> See paragraph 2.2.1 below

funds which are either derived from the cyberworld, which is the environment of the internet,<sup>49</sup> or funds that were originally illegal hardcash, but became converted into illegal e-money.<sup>50</sup> With respect to the second category, illegal hardcash can be converted into illegal e-money through the use of e-payment systems. This is why the ensuing discussion is of great relevance.

In this section, the notion of e-money is explored in further depth, in order to bring to light the practicalities surrounding it, and why it represents the perfect weapon being wielded for cyberlaundering purposes.

E-money can be described as monetary (or equivalent) value which is represented in an electronic format.<sup>51</sup> A more elaborate definition is as follows:

[Electronic money] is a system that allows a person to pay for goods or services by transmitting a number from one computer to another. Like the serial numbers on real dollar bills, the digital cash numbers are unique. Each one is issued by a bank and represents a specified sum of real money. One of the key features of digital cash is that, like real cash, it is anonymous and reusable.<sup>52</sup>

A key feature of e-money is that it is usually held in online banking systems, and not in physical form. In countries such as the United Kingdom and the United States, only a small fraction of money is held in cash, as most of it is in the digital form.<sup>53</sup> Despite the dip in the economies of these countries in recent times, domestic e-commerce climbed 10.8% from \$ 185 billion (£ 113 billion) in the year 2008

<sup>49</sup> An instance where illegal funds can be derived from the cyberworld is when one profits from running an unlicensed website on the internet. See elaborate discussion in Chapter 5, paragraph 6.5.2 below.

<sup>50</sup> An example of this can be seen in several cyberlaundering techniques, such as virtual worlds, online banking, online gambling and online barter trade to name a few. See discussion in paragraph 3.5 below.

<sup>51</sup> Cf an alternative definition by the European Union: “Electronic money means electronically, including magnetically, stored monetary, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions [...], and which is accepted by a natural or legal person other than the electronic money issuer.” See Article 2(2), Council of Europe: Council Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions, adopted by the Parliamentary Assembly on 16 September 2009, and which came into force on 30 October 2009.

<sup>52</sup> Webopedia (an undated website document) ‘Digital Cash’ available at <[http://www.webopedia.com/TERM/D/digital\\_cash.html](http://www.webopedia.com/TERM/D/digital_cash.html)> [accessed on 04 August 2013]. Several other definitions of e-money have been proposed as well. For example, the Electronic Money Institutions European Directive defines it as monetary value as represented by a claim on the issuer which is: (i) stored on an electronic device; (ii) issued on receipt of funds of an amount not less in value than the monetary value issued; (iii) accepted as means of payment by undertakings other than the issuer.’ See 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.E.C. L275/39, 27/10/2002). The latter definition is very elaborate. One very important criticism that can be levied against it is that it confines the notion of electronic cash to monetary value, thereby automatically excluding internet cash, such as DigiCash and store reward points.

<sup>53</sup> Investopedia (an undated website document) ‘Electronic Money’ available at <<http://www.investopedia.com/terms/e/electronic-money.asp>> [accessed on 4 August 2013].



<http://www.springer.com/978-3-319-06415-4>

Legal Principles for Combatting Cyberlaundering

Leslie, D.A.

2014, XV, 368 p. 1 illus., Hardcover

ISBN: 978-3-319-06415-4