ANDRONIKI N. TZIVANAKI

UNIVERSITY OF LEICESTER

Information Society services in Southeastern Europe as a means for money laundering.

ATHENS

JANUARY 2001

TABLE OF CONTENTS

1. INTRODUCTION....3

2. INFORMATION SOCIETY SERVICES AND CYBER CRIME 4

3. MONEY LAUNDERING AND CYBER LAUNDERING 5

3 a. Practices and relations....8

3 b. The problem of location....10

4. THE CURRENT LEGISLATIVE FRAMEWORK - PARTICIPATION OF SOUTH EASTERN EUROPEAN COUNTRIES TO COLLECTIVE ANTI-MONEY LAUNDERING EFFORTS 10

4 a. FATF Members....10

4 b. Council of Europe / PC-R-EV Committee Members 12

4 c. EU Members....13

4 d. Other bodies....15
4 d (i). The European State Lottery Association (ESTLA):.... 15
4 d (ii). The Federation of European Stock Exchanges (FESE):.... 16

5. SOUTH EASTERN EUROPE: AN ALTERNATIVE?....16

5 a. Current situation....17

5 b. An alternative for cyber launderers – possible infringements....19

6. CONCLUSION....21

ANNEX....23

BIBLIOGRAPHY....24

1. Introduction

Money laundering is a threat to the good functioning of a financial system; however, it can also be the weak point of criminal activity and an indicator for corruption. The existence of a framework with high legal, professional and ethical standards is essential for the integrity of a national financial services marketplace.[1] As the emerging information society services offer new dimensions to the money laundering practices, international co-operation is defined as crucial in order for measures to bring results. Southeastern Europe is a region where most of the countries are associated with the European Union, but only two of them, Greece and Turkey, are members of the Financial Action Task Force (FATF) on Money Laundering; although none of the rest is among the non-cooperative countries or territories listed in FATF's review.

Taking into account the fact that the region has suffered a long period of disorders and that developing economies are expected not to be able to afford being too selective about the sources of capital they attract, the paper will attempt to identify the possibilities and risks of infringements of the FATF recommendations as a result of new technologies activity.

Undoubtedly, the impact of recent legal developments in the European Union, should be also considered, as - apart from the membership of Greece - Bulgaria, Cyprus, Hungary, Romania, Slovenia and Turkey have already signed association agreements and have submitted accession applications. The European Union institutions have recently proceeded to a new E-commerce Directive, combined with five proposed directives intending to shape the regulatory framework for electronic communications networks and services, in the view of guaranteeing that free movement of information society services within the Single Market will be a reality the sooner possible.

To what extent do these legislative reforms cover money laundering issues, occurring from the electronic activities of international business companies, or offshore front companies of international firms? Would the Southeastern European countries jurisdictions offer an alternative to money laundering activities? Are the

[1] Financial Action Task Force (FATF/OECD), <http://www.oecd.org/fatf>.

latter ready to implement the international and EU requirements concerning the protection from new technology money laundering practices?

2. Information Society Services and Cyber crime

A lot of noise is being made about the new economy, the development of information society, about introducing the Internet to more households worldwide, to reach more hits, page views, user sessions, banner clicks, list members, registered users in on-line clubs, user accounts for web services. Most of the times, for an on-line service provider, whether this is the web site of a brand simply aiming at interactivity with the public or an electronic store, requirements for personal data are viewed as repulsive for prospective users or customers. From a different perspective, some users view the extensive personal data fields in an on-line registration form as a guarantee for the quality of the service they apply for. In any case, a large number of Internet users when applying for on-line services usually give false personal information, accompanied by an existing web-mail[2], which nevertheless has been acquired using false or insufficient for identification data. It would be wrong though, to assume that nine out of ten people in our society have underlying criminal intentions. The simplest explanation is that when one is given the possibility of keeping his or her anonymity, he or she will do it, because "anonymity is of incontestable value in protecting privacy" and "[a]lmost everyone has a reason to speak or act anonymously at some point".[3]

Cyber crime and consequently cyber laundering, certainly ignores the anxiety of making the information society a new channel for media and commercial services and focuses on what possibilities one is given by these new technologies. In reality there is a delicate balance between possibilities requiring special skills by the user who can take advantage of the inefficiencies of the systems – (hacking) - and possibilities of facilitation between experts that became far-fetched paid services and then free services in the name of marketing and publicity goals – (exploitation of new

[2] E-mail address provided by a web-site, maintaining a personal mailbox for each e-mail account in its web servers, managed remotely by the user, with certain limitations in space availability as opposed to an e-mail account opened by an Internet Service Provider giving to the user the possibility to manage and store the mailbox in his or her personal computer.

means for coverage or diffusion of evidence). To continue with, the quest for "more" in the Internet world results to the offering of services that used to be "tricks for freaks" for free.[4] This trend gives way to a new generation of criminals to be, fascinated by the anonymity and the capability of worldwide communication at these low costs and most importantly in an economy that in a large part of the world can be still controlled by the skills of a programmer as opposed to the money of a businessman.

Finally, it seems that as far as the use of internet technologies is concerned, the world is advancing at almost the same pace; while on the contrary the commercial, advertising and marketing side of the information society requires for conventional businesses to adjust to the new conditions and follows the rhythms of economic development, obviously varying from region to region. This is why South Eastern Europe may be a region under development, with major economic problems, but still makes no exception to the rule.

3. Money Laundering and Cyber Laundering

For the purposes of the anti-money laundering EC Directive[5] money laundering is defined as "the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action". The above conduct has to be committed intentionally, while the EC Directive is specifically detailed, making sure that every aspect of the issue is covered. Thus, according to the same article, money laundering is also the "acquisition, possession or use of property, knowing, at the time of receipt that such property is derived from criminal activity (…)". Considering a more generic

[3] Reitinger P.R., "Encryption, Anonymity and Markets", *Cybercrime, Law enforcement, security and surveillance in the information age*, Ed. Thomas, D. – Loader, B.D., Routledge 2000, p. 136.

[4] Example of redirecting user URLs to sub web URLs (more commercial names) for free. Until recently, in order to have a URL that the user could remember, meaning that it wouldn't need the entire address bar, one had to pay.

[5] Article 1, Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.

definition[6] "[m]oney laundering is a legal catch phrase that refers to the criminal practice of taking ill-gotten gains and moving them through a sequence of bank accounts so they ultimately look like legitimate profits from legal business. The money is then withdrawn and used for further criminal activity."

The last observation is incorrect though. Anti-money laundering regulations do not seek to examine the ultimate use of laundered money, most probably because it goes without saying that the property of a criminal is used back in criminal activities. The Bulgarian law gives a slightly different aspect; money laundering concerns illegally gained "cash or other property, and the yield thereof (…) [which] is being introduced into the economic cycle and the result of its use is recorded by bookkeeping and taxed".[7] What is more than certain is that, at the end of the day, laundered money is being taxed and governments will not find an incentive there for combating the phenomenon. The latter is not so certain with the Internet, because it is harder to "pinpoint the identity or location of people who are carrying out potentially taxable activities"[8]. From a different point of view, "[t]he war against money laundering is really a second front in the failed war against drugs."[9], merely started by the United States. Moreover, the preamble of the above mentioned EC Directive acknowledges: "combating money laundering is one of the most effective means of opposing [organized crime in general and drug trafficking in particular]".[10]

Money laundering is said to be "a process, often a highly complex one, rather than a single act"[11]. This process includes the "placement", "layering" and "integration" stages[12], the first being "probably the point of greatest vulnerability for the launderer"[13]. After the proceeds have been placed in a financial institution or used to purchase an asset, the "layering" stage comes to conceal or disguise the source of the ownership of the funds by making sure that the authorities will be confused in

[6] Definition found in New York Times by Rob Norton, September 1999, "In Defence of Money Laundering", Fortune.
[7] Republic of Bulgaria, Measures Against Money Laundering Act, [No. 85/24-07-1998].
[8] The Economist, 27-1-2000, Survey: Globalisation and Tax, "Net losses: Why the taxman fears the Internet".
[9] Norton, R., 1999, n 6 above.
[10] Directive 91/308/EEC, n 5 above. Further analysis of this discussion below, (5. South Eastern Europe: An alternative?).
[11] Gilmore W., 1995, "Dirty Money", Council of Europe Press, Strasbourg, p. 37.
[12] It has become common to utilise a three-part framework that seeks to encompass an ideal money laundering scheme. (Gilmore W., 1995, n 11 above, p. 37).
[13] Snaith I., 2000, "Money Laundering, Financial Services and the European Union: Ever Expanding Regulation?", unpublished, p.2.

case of trying to trace them. The third stage consists of the apparent legalization of the funds.

Relating the above considerations, particularly the second stage, to the role of information society services, one can easily imagine that the less launderers are physically seen in a financial institution, the better they manage to increase the complexity of the process and make it even more untraceable. Managing multiple bank accounts through on-line banking services[14], can be easily done from a single person from any location. In describing the impact of on-line banking on money laundering FATF experts make a similar observation. "[A]n individual desiring to conceal his or her true identity (…) would be able to have unrestricted on-line access to and control of his bank accounts in any location."[15] In any case, on-line fund transferring comes to add a medium, giving to launderers greater chances for diffusion.

On balance, one could support, new forms of communicating and transacting are just a means, which can be used appropriately by both sides. Accomplices need to trust each other. With electronic transactions one can never know who is "at the other end" of the telecommunications network. On the contrary, "[t]otal anonymity affords criminals the ability to launder money and engage in other illegal activity in ways that circumvent law enforcement." [16] Combined with encryption or steganography[17] and anonymous remailers[18], electronic cash[19] becomes a very powerful medium. Moreover, money laundering measures regulate corporations licensed by national authorities and since the Internet can be (easily and at low costs) used for unofficial corporate activity and service providing by solely web businesses the enforcement and monitoring part of an anti-money laundering policy, becomes extremely difficult if not impossible.

[14] On-line banking includes accessing financial services indirectly, that is by telephone, automatic teller machines (ATM) and the Internet (FATF-XI, 3-2-2000, *Report on Money Laundering Typologies 1999-2000*, FATF/OECD). Yet, the present paper will focus on banking and non-banking Internet services which appear to be the newest area of money laundering typologies.

[15] FATF-XI, 2000, n 14 above, p.2.

[16] Denning, D.E. – Baugh, W.E., Jr, 2000, "Hiding crimes in cyberspace", *Cybercrime, Law enforcement, security and surveillance in the information age*, Ed. Thomas, D. – Loader, B.D., Routledge, p. 126.

[17] Methods of hiding secret data in other data such that their existence is even concealed. Encoding the secret data in the low-order bit positions of image, sound or video files is one of the methods used (Denning, D.E. – Baugh, W.E., Jr,, 2000 n. 16 above, p. 122).

[18] "A service that allows someone to send an electronic mail message without the receiver knowing the sender's identity." (Denning, D.E. – Baugh, W.E., Jr,, 2000 n. 16 above, p. 125).

3 a. Practices and relations

Internet services can well be used as a cover or as a means for money laundering purposes. It depends on which side the launderer is found. Three main categories of criminal activity can therefore be described through commonly conceivable at the moment web practices.

The first case would be that of the web service provider not being aware of the money launderer's activities, who takes advantage of the new technologies and above all the anonymity or relative anonymity offered, in order to launder the proceeds. Relative anonymity can be defined as the advantage of losing anonymity only upon suspicion.[20] To be more specific, the personal data of a customer being known, the web service provider has no reason or sometimes possibility to distinguish him from the whole of its customers or specially observe his activities. Therefore, such a situation could be referring to the e-banking service of a well-known bank, whose account opening procedure and monitoring software are proven unable to detect the suspicious movements. There is no doubt that a bank or non-bank financial institution could very well belong to the second category analyzed below, letting the money launderers act under its tolerance. At this point, provided that relative legislation exists, the role of the state authorities is considered crucial in order to enforce an anti-money laundering policy, as legally registered corporations are the first to be regulated and monitored.[21]

In the second case, the web business is an accomplice in the money laundering procedure and as the persons involved possibly co-operate by other means, the conventional methods of tracing criminals may be useful for authorities. In this category the first to be blamed is the on-line gambling business. Opening an account and maintaining a "wallet" in an on-line casino or bookmaker is subject to less identification requirements than opening an account with a bank, but this does not necessarily imply that the web site is involved or aware of the criminal origin of the funds put in its member accounts. The obvious reason for the involvement of the

[19] Transactions using electronic currencies such as E-cash, <http://www.digicash.com> or E-gold, <http://www.e-gold.com>.

[20] As Mark Bortner mentions "[t]he trick was, and still is, to avoid attracting unwanted attention", 1996, "Cyberlaundering: Anonymous Digital Cash and Money Laundering", University of Miami, School of Law.

[21] Existing regulation primarily focuses on measures to be taken by financial institutions. (FATF Forty Recommendations, 1996, FATF/OECD and EC Directive 91/308/EEC, n 5 above)

operator of the apparently legal activity is that laundering of the funds is not guaranteed, unless the "customer" is "lucky enough" to win back the money minus the percentage agreed, that would be the profit for the front-end business. On the other hand, one would argue that suspicion by the authorities is most possible as an on-line business willing to take the risk of offering money laundering services might not even be legally established. The apparently "unsuspicious customer" who is the initial provider of the illegal funds can still avoid liability, based on the falsified or insufficient identification data he provided during his registration. Given the opportunity of using the particular example, we may add that according to a well-respected member of the Greek gaming industry, "the money is where consumption is" and "for an online lottery or wagering business money laundering, as an additional source of income, is not worth the risk". With no doubt this is the case of a business with a satisfying market share, operating in a highly regulated system.

Furthermore, taking into consideration the above possible scenarios, hacking is not found necessary or at least indispensable. In the former case the money launderer presents himself as a regular customer, while in the latter the parties have already connived. Consequently, hacking has place only where the money launderer and the apparently legal "laundry" are not collaborating, in the occasion that anonymity must be guaranteed by electronic counterfeiting; the goal being not to extract but to put money into legal accounts.

A third service, exclusively electronic, developed thanks to the differences in jurisdictions around the world and above all intending to "exploit variations in national laws"[22] without having any legal consequences, is that of web sites offering investment opportunities. This third scenario contains some of the indisputable legality of a financial institution, not breaking any legal provision and some of the tolerance of an accomplice. It would be too optimistic to deny that another service, digital currency, does not comply with the above characteristics[23], as most applications work under the concept that "it is impossible for anyone to link payment

[22] Taggart, St., "Dotcoms desperately seeking sovereignty", The Industry Standard – Europe, 23 Nov. 2000, p.74.

[23] Although, with most applications the customer has to "load" his wallet with electronic cash through an existing bank account, his transactions from that point further remain anonymous. For example E-cash <http://www.digicash.com>.

to payer, but users can prove unequivocally that they did or did not make a particular payment, without revealing anything more".[24]

3 b. The problem of location

National legislation on money laundering usually imposes obligations to the financial institutions and in some occasions to other professionals[25], under the concept that the customers are found and transactions are taking place in their territory. In the case of on-line banking the financial institutions open a world wide web - therefore transnational – branch, but normally offer their services provided that the customer supplies a local address and other identification data[26]. On the other hand, customers are not necessarily found within the territory where the financial institution is legally registered and/or provides conventional services. The transaction could be taking place in the server, in the institution's site of incorporation or head office location or in the client's personal computer, depending the legislation, if any.[27]

To continue with, the parties of an information society transaction are the client and the service provider, while the web server where the on-line content is being hosted realizes the electronic contract, agreement, exchange, order. The web server could be physically in a different location than the business providing the service and the actual head office of the business could be in a different location than the place it has been incorporated.

4. The current legislative framework - Participation of South Eastern European countries to collective anti-money laundering efforts[28]

4 a. FATF Members

The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body under the auspices of OECD, which develops and promotes

[24] Bortner, M., 1996, n 20 above.
[25] View below: 4 a) FATF Members and 4 c) EU Members.
[26] An on-line registration is almost always required. The level of details required through compulsory fields depends on the legislative provisions imposed to each institution.
[27] Lloyd, I.J., 2000, *Information Technology Law*, Butterworths, p. 553 and 593.

policies, both nationally and internationally, to combat money laundering. Its primary goal is to generate the political will for national legislative and regulatory reforms, needed for combating economic crime of this type. From the countries under discussion, only Greece and Turkey are members of the FATF. [29]

The main obligations deriving from this membership is the ratification and full implementation of the 1998 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances as well as the implementation of the Forty FATF Recommendations.[30] More specifically, regarding the new technologies, participating countries are urged to "pay special attention to money laundering threats inherent in new or developing technologies that might favour anonymity" and if needed "take measures to prevent their use in money laundering schemes".[31]

In their latest Report on Money Laundering Typologies (1999-2000)[32], FATF experts consider on-line banking as one of the major money laundering issues. In reports of previous years new payment technologies are also analyzed.[33] The forty recommendations currently reserve a special role for the financial system in order to combat money laundering[34]. Concerning banks and non-bank financial institutions of all kinds[35], they set customer identification and record-keeping rules[36]; ensure the increased diligence[37] of financial institutions by exempting the institutions, their directors, officers and employees from any criminal or civil liability if they report their suspicions in good faith[38]; imply measures to avoid money laundering and especially for transactions with countries with no or insufficient anti-money laundering policies[39].

---

[28] ANNEX.
[29] The organization's membership includes twenty- nine countries in total covering Europe, North and South America and Asia as well as the European Commission and the Gulf Co-operation Council. FATF web site, "More on the FATF and the focus of its current work", <http://www.oecd.org/fatf>.
[30] Recommendations 1 and 2, n 21 above.
[31] Recommendation 13, n 21 above.
[32] FATF-XI, 2000, n 14 above, as a result of the FATF-XI meeting of experts, Washington, DC, 18-19 November 1999.
[33] FATF-X, 11-2-1999, *Report on Money Laundering Typologies 1998-1999*, FATF/OECD, after the group of experts meeting in London, 17-18 November 1998 and FATF-IX 12-2-1998, *Report on Money Laundering Typologies 1997-1998*, FATF/OECD after the Paris meeting on 19-20 November 1997.
[34] Recommendations 8-29, n 21 above.
[35] Recommendation 8, n 21 above.
[36] Recommendations 10-13, n 21 above.
[37] Recommendations 14-19, n 21 above.
[38] Recommendation 16, n 21 above.
[39] Recommendations 20-25, n 21 above.

FATF recommendations focus on the criminal and not the financial institution through which the money is laundered; but contradiction remains: "would you feel comfortable if you could be prosecuted for failing to immediately inform the police of your suspicions?"[40] One could claim that if a financial institution can prove that nothing came under its suspicion, then it is not liable. Still, legal departments of banks usually have other obligations to fulfill. In the case where it is proved that the illegal funds pass through a financial institution there is actual liability of either the enterprise or its employees or both. In the interpretative notes for Recommendations 8 and 9, where the details for "bureaux de change" are presented, as differing from banks, the main consequence in case of non-compliance with anti- money laundering national law, is fail to obtain a license of operation.[41] Of course constant and effective control is difficult in such small units as "bureaux the change" are and especially in case they provide on-line services, let alone that this kind of national law enforcement has chances of happening only in Greece and Turkey.

4 b. Council of Europe / PC-R-EV Committee Members

The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (PC-R-EV Committee) is a sub-committee of the European Committee on Crime Problems (CDPC) and its main task is the mutual evaluation reporting of its member states, carried through by the national experts appointed to it.

Albania, Bulgaria, Croatia, Cyprus, Hungary, F.Y.R. of Macedonia, Moldova, Romania, Slovenia are members of the PC-R-EV Committee, while Greece and Turkey participate as observers, due to their FATF membership. Additionally, a number of international and regional organizations, amongst which the European Commission, the European Bank for Reconstruction and Development (EBRD), the

[40] Norton R. , 1999, n 6 above.
[41] "(…) Bureaux de change would have to notify their existence to a designated authority but would not need to be authorised before they could start business. It would be open to the authority to apply a "fit and proper" test to the management of bureaux de change after the bureau had commenced activity, and to prohibit the bureau de change from continuing its business, if appropriate. (…)", *Necessary Counter-Measures Applicable to Bureaux de Change*, Recommendations 8 and 9, Interpretative Notes, n 21 above.

International Monetary Fund (IMF) and the Secretary General of the Council of the EU, are observers to the Committee.[42]

The work of the PC-R-EV Committee is thus a way of evaluating the existing money laundering conditions in European countries that are not FATF members, based on the compliance with the FATF forty recommendations, the Vienna Convention[43], the 91/308/EEC Directive and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime[44]. As it will be further analyzed below, although the majority of the countries of South-Eastern Europe have signed the Vienna and Council of Europe conventions, national legislations have very recently proceeded to anti-money laundering measures, a fact that makes effectiveness quite impossible at the present time.

4 c. EU Members

The "Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering"[45] mainly sets the European Union's legal framework against money laundering. The 1999 Commission proposal for amendment of the above directive aims to "continue to strengthen the Single Market's defenses against organized crime"[46], by introducing regulative answers to new trends and extending the scope of the provisions to non financial sectors. "[A]s the money laundering defenses of the banking sector have become stronger money launderers have sought alternative ways"[47] and this is "the most noticeable trend" in money laundering techniques, according to FATF's 1996-97 Typologies Report. It goes without saying, that the on-line versions of these alternative professional businesses, such as "estate agents, arte dealers, auctioneers,

[42] "Council of Europe PC-R-EV Committee", FATF web site, <http://www.oecd.org/fatf/ctry-orgpages/org-pcrev_en.htm>.
[43] United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Vienna, 20 December 1988.
[44] Adopted in Strasbourg on 8 November 1990.
[45] Doc. 391L0308, n 5 above.
[46] Declaration by Financial Services Commissioner Mario Monti, referring to the Commission proposal to extend the scope of the 91/308/EEC Directive (n. 4 above), Europa web site, <http://europa.eu.int/ comm/ internal_market/en/finances/general/99-498.htm>.
[47] European Commission, Proposal for a European Parliament and Council Directive amending Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering. [Doc. 599PC0352].

casinos, bureaux de change, transporters of funds, notaries, advocates, tax advisors and auditors"[48] might be already used for money laundering purposes.

Measures that would directly interest the money laundering via electronic means discussion are remarkably comprised in an annex that will be added to the amended Directive. The proposed annex[49] specifies appropriate methods for credit and financial institutions to identify their customers in non face-to-face financial operations. To be more specific, concerning the opening of a new account, special attention is intended to be paid to the verification of the customer's address, while the contracting institution will be using its nearest to the customer branch in order to carry out a face-to-face identification.

Additionally, according to Article 3(2) of the EC Directive, identification is required "for any transaction (…) involving a sum amounting to 15.000 Euro or more, whether the transaction is carried out in a single operation or in several operations which seem to be linked". For the case of on-line transactions this could be partly supported by appropriate software, which would monitor the amounts and frequency of transactions and then produce a suspicions report. But, no regulation imposes such application yet.

Greece is at the moment the only EU member in the region and has fully[50] implemented the Directive. Furthermore, Bulgaria, Cyprus, Hungary, Romania, Slovenia and Turkey are associated members and lately Albania, Bosnia-Herzegovina, Croatia, F.Y.R. of Macedonia and Yugoslavia have participated to one more meeting preparing the ground for their EU candidature.[51] It is then, important to realize that the high degree of regulation in the EU context, makes more imperative the need for compliance of all South East European jurisdictions with the FATF recommendations.

Article 9.3 of the EC Directive on electronic commerce, relating to the treatment of electronic contracts, issues an alternative way for Member States to amend their money laundering policy as far as information society services are

[48] Concerning the extension of Article 6 (of 91/308/EEC Directive, n 5 above) to persons and professions other than the financial institutions currently mentioned in the Directive, which are at risk of being involved in money laundering or abused by money launderers, European Commission, [Doc. 599PC0352], n 47 above.
[49] European Commission, [Doc. 599PC0352], n 47 above, Annex.
[50] DG Internal Market, "Money laundering: How to improve EU rules for prevention", Europa web site, <http://www.europa.eu.int/comm/internal_market/en/index.htm>.
[51] Referring to a meeting of November 2000, Kerin H. (Ed.), January 2001, Business File Newsletter – Greek Special Survey Series, *Economic and Industrial Review*, No 8.

concerned. "Member States shall indicate to the Commission the categories [of electronic contracts] to which they do not apply [Art. 9] Paragraph 1"[52]. The first paragraph of the article sets that the Member States "shall ensure that their legal system allows contracts to be concluded by electronic means". Most importantly, EU Member States shall submit to the Commission every five years a relative report.[53]

Moreover, it is interesting to consider the consequences of gambling (including lotteries and betting transactions) being excluded[54] from the scope of the e-commerce Directive.[55]

4 d. Other bodies

4 d (i). The European State Lottery Association (ESTLA):

Although a union movement cannot be of the same importance as supranational or intergovernmental efforts against fraud, the role of ESTLA can acquire particular significance for the purposes of the subject under analysis. Firstly, the State Lotteries of all thirteen countries[56] of South Eastern Europe are members of the ESTLA, even the State Lotteries of Bosnia-Herzegovina and F.R. of Yugoslavia that do not participate to any other of the bodies presented above.

State lotteries, being monopolies in most of the states involved, are trying to prevent cross border providing of lottery and wagering services, which is the main advantage for on-line gaming businesses to count on. The threat is described as "free lottery sites, which are developing into a thriving commerce"[57], the means could be among others the under development EC legislation, and the reason to combat such economic activity is "the danger of lost tax revenue [for states] and the problem of money laundering" [58].

[52] The report can only specify categories within the framework of paragraph 2 of the same article.
[53] Article 9, 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) [17-7-2000, L 178/1].
[54] Since in most of the EU countries state lotteries are monopolies ensuring big percentages of state revenues, if the gambling industry was to be included, it is more than certain that the e-commerce Directive would still be under discussion.
[55] Article 1.5 (d), Directive 2000/31/EC, n 53 above.
[56] Albania, Bosnia-Herzegovina, Bulgaria, Croatia, Cyprus, Greece, Hungary, F.Y.R. of Macedonia, Moldavia, Romania, Slovenia, Turkey, F.R. of Yugoslavia.
[57] ESTLA, New Media and Internet working group, Meeting on 25-9-2000, Paris, France.
[58] ESTLA, 2000, n 57 above.

4 d (ii). The Federation of European Stock Exchanges (FESE):

Additionally, the FESE membership covers 21 stock exchanges[59], within which are the Athens Stock Exchange as a full member and the Budapest Stock Exchange, Ljubljana Stock Exchange, Cyprus Stock Exchange as associate members. The FESE exchanges have already concluded a Memorandum of Understanding, which specifically applies for the cross-border exchange of information, while the FESCO (Forum of European Securities Commissions) has also set up similar exchange of information mechanisms. The Secretary-General of the FESE, invited for the first time to a FATF Forum, refering "to the section of the FATF typologies report on on-line banking, (…) stressed the fact that all the European markets are fully electronic and the impact of this on the audit trail"[60].

5. South Eastern Europe: An alternative?

"Money has to circulate. Money has no origin. Money might be dirty but it doesn't stink."[61] To be more descriptive, transactions cannot be a crime by themselves and even when the criminal activity behind them is proved, funds of the size of criminal proceeds can be useful for an economy. Beyond any doubt and also recognized by the FATF, it is true that weak economies cannot afford to be too selective about the funds they attract, without being legalized for doing so. Yet "laundered money flows into global financial systems where it can undermine national economies and currencies [, turning money laundering] not only [to] a law enforcement problem but [to] a serious national and international security threat as well"[62]. Consequently, lack of political will to fight against money laundering can be viewed as a solution or a danger. To repeat the words of the owner of a company that provides regulatory arbitrage[63] by taking advantage of the Internet technology "(…) in any case, OECD member nations have limited incentive to financially isolate tax

[59] FESE, January 2001, "Second Report and Recommendations on European Regulatory Structures", < http://www.fese.be>.
[60] FATF/OECD, 2-6-2000, *Annual Report 1999-2000*.
[61] Comment expressed by an expert of the Greek banking system to the author.
[62] Bureau for International Narcotics and Law Enforcement Affairs, U.S. Department of State, "INCSR - Money Laundering and Financial Crimes", March 1999, p.2.
[63] Regulatory arbitrage refers to "[a] financial contract or a series of transactions undertaken, entirely or in part, because the transaction(s) enable(s) one or both of the counter parties to accomplish a financial

havens. Big countries may need these small nations' cooperation in fighting global threats such as terrorism bio-warfare or computer viruses. The price of cooperation may well be a willingness to look the other way regarding a few margarita-drinking tax cheats."[64]

5 a. Current situation

This paper aims to analyze the impact of new technologies on money laundering activities, deriving from, passing through or using the regimes of SE European countries. As the majority of the countries concerned are experiencing a transitional period facing major economic problems, it seems strange or rather impossible that new technologies can be sufficiently supported for money launderers to act. We thus have to accept an uncontestable truth: crime always has access to latest technology first, way before governments or even private sector have.

Another acknowledgement needing to be made is that on-line services not more than money-laundering activity is a global phenomenon. Cyber laundering is, therefore, a highly transnational activity, giving to FATF's Recommendation 3 exhortation for "increased multilateral co-operation and mutual legal assistance"[65], a more and more imperative character. After all, according to an expert of the Greek banking system, there is no need for a whole country to be familiarized with information and communication technologies; "ten persons are absolutely sufficient" for money laundering market to flourish; and it would be a mistake to suppose that each of the Balkan states does not host "ten experts". Taking into account the presence of languages in the online community from the countries under consideration Cyprus, Greece, Hungary, Romania, Slovenia and Turkey are the more Internet active [66].

---

or operating objective which is unavailable to them directly because of regulatory obstacles.", International Financial Risk Institute (IFCI) <http://risk.ifci.ch>

[64] Taggart, St., n 22 above, p.76-77.

[65] "An effective money laundering enforcement program should include increased multilateral co-operation and mutual legal assistance in money laundering investigations and prosecutions and extradition in money laundering cases, where possible", Recommendation 3, n 21 above.

[66] Greek speaking online population is 1.5 million, Hungarian is 0.8 m., Romanian 0.6 m., Slovenian 0.46 m., Turkish 2.2 m. Indicatively, and taking as a fact that the populations' presence indicates the majority of web sites in the same language, the Russian speaking community is 9.3 m. and the English 192.1 consisting with no doubt of users throughout the world. Global Internet Statistics / by Language, December 2000, <http://www.glreach.com>.

Furthermore, a useful observation would be the following: Greece is apparently the most regulated jurisdiction in the region (meeting most of the FATF forty recommendations and having implemented the EC Directive) and "[t]he Greek anti-money laundering system (…) appears to be working reasonably well in several areas" and still "the results achieved so far, though moving in the right direction, are modest"[67]. Additionally, Turkey "[s]ince the first evaluation has taken significant steps towards meeting the forty Recommendations and working to implement an effective anti-money laundering system. (…) [but] the results in the first year have been moderate"[68]. It is significant to notice that Turkey does not currently meet FATF Recommendations 19 and 20, concerning anti-money laundering programs that should be developed by financial institutions[69] and application of principles governing financial institutions to their branches located abroad[70]. On the contrary, membership to international bodies does not ensure legal action. "The prevention and Suppression of Money Laundering Activities Law 1996" of Cyprus "(…) provides a very comprehensive legal framework which compares favourably with others in place in larger countries which are members of the FATF"; the PC-R-EV Committee continues mentioning that "[i]ts impressive legal structure, based on existing international anti-money laundering standards, is significantly in advance of any other country in its geographic sub-region".[71]

The rest countries of the region being non-FATF members, as well, are not typically obliged to impose such policies. Despite the many differences existing in the financial systems' structures of the countries concerned, according to the PC-R-EV Committee reports, the economies of Croatia, Hungary, F.Y.R. of Macedonia and Slovenia are still heavily cash based[72], a factor indicating money laundering possibilities.[73] To be more specific, "[w]hile [the Romanian law] provides for some sanctions to be taken by the office for non-compliance, no authority or institution is

[67] FATF/OECD, 2000, Report for Greece.
[68] FATF/OECD, 2000, Report for Turkey.
[69] Recommendation 19, n 21 above.
[70] Recommendation 20, n 21 above.
[71] PC-R-EV Committee, Report for Cyprus to be included in the 1999-2000 Annual Report, Council of Europe.
[72] PC-R-EV Committee, Reports for Croatia, Hungary, F.Y.R. of Macedonia and Slovenia to be included in the 1999-2000 Annual Report, Council of Europe.
[73] For the purposes of the subject under analysis a cash based economy implies the existence of launderers and criminal activity rather than the facilitation of cyber laundering.

tasked explicitly with checking compliance with [the law]"[74]. With no doubt the international community invites all countries to continuously monitor their anti-money laundering system as well as to implement the necessary changes to make their system more effective. Still, it is obvious that launderers using new on-line technologies cannot be effectively controlled, when not even conventional criminal activity is being traced; and cyber laundering has a brilliant opportunity to flourish as web services develop with unusually high speeds and low costs.

5 b. An alternative for cyber launderers – possible infringements

In relation with dealing cyber laundering problems, FATF experts offer to states suggestions[75] such as: customer identification reinforcement; development of new information technology capabilities for "detection of suspicious on-line transactions and verification of the customer"; prohibition of financial institutions not licensed in a jurisdiction from offering their services in that jurisdiction on-line, which is consistent with offering on-line services only to accounts that have been opened with face-to-face identification[76]. Yet, it has to be recognized that due to universal competition the web presence of a legally formed financial institution – or any other business - is subject to, it is unfair from the part of national authorities to impose measures restricting the types or quality of services permitted[77].

Finally, the most difficult part is that of the suggestion for "oversight of both"[78], the jurisdiction where an on-line banking service is offered from and the one where the clients are using the service. Southeastern Europe is characterized by this difficulty due to the different international obligations the countries of the region are subject to. To bring an example, supposing that Greek banks in the near future will comply with measures similar to those described above[79]; on the first hand they will

[74] Refering to Law No 21/99, PC-R-EV Committee, Report for Romania to be included in the 1999-2000 Annual Report, Council of Europe.
[75] FATF-XI, 2000, n 14 above, p.4.
[76] The above measure is also considered in the framework of an ANNEX to be included to the EC anti-money laundering Directive, which is currently under amendment [Directive 91/308/EEC, n 5 above]. View below, *4 c. EU members*.
[77] One of the suggestions refers to limiting "the types of permitted on-line services ore the amount of such transactions", while avoidance of creating anonymous accounts, is with no doubt a disincentive for the Internet customer, who may well prefer other on-line services. (FATF-XI, 2000, n 14 above, p.4.)
[78] FATF-XI, 2000, n 14 above, p.4.
[79] As a consequence of legislative changes deriving from both its FATF and EU memberships.

possibly be unable to identify their Bulgarian client who manages his on-line account from Bulgaria and who has given the identification information of a relative legally residing in Greece; and on the second they cannot expect from Bulgarian authorities - trying to conform their current anti-money laundering policy to international standards - to monitor through ISPs every Internet connection in order to trace such activity. Therefore, it is not the use of information society services, the act of transmitting electronically content, that will lead to the criminal.

A similar situation and absolutely unregulated is the case of an on-line casino[80] managed remotely through Romania, physically being hosted in Turkey, typically owned by an offshore company incorporated in Cyprus, where the Greek players residing in Greece and having given false personal data but an existing address possibly in Greece - since the casino's registration form does not impose such restrictions - cannot be traced separately by Greek authorities and certainly not by Cypriot[81] or Romanian or Turkish.

Supposing that criminal activity has been found with the collaboration of the involved states' authorities and that Turkey and Cyprus are EU members and have implemented the *acquis communautaire*, the Turkish hosting provider would be liable in case it was provable that there was "actual knowledge of illegal activity"[82] being offered through its servers, while the company incorporated in Cyprus, owned by a resident of Romania would probably face sanctions set by EU and Cypriot legislation.[83] It is most possible though that none of the collaborating corporations will have evidence for the identity of the person(s) managing remotely the on-line service.

[80] This is not to imply that all on-line gaming services or all offshore incorporated web businesses are suspicious for money laundering activities, the main reason for using offshore locations being to offer free VAT services. The offshore jurisdiction not imposing any restrictions, the jurisdiction where the client accesses the service from is not able to monitor him or her.

[81] As long as the bookkeeping obligations of the company do not raise suspicions.

[82] Article 14, Directive 2000/31/EC, n 53 above.

[83] The example is totally hypothetical and the possible legal consequences presented aim only to demonstrate that although legislative measures can be such as to bring effect, their enforcement is subject to the collaboration between state authorities, the full implementation of obligations deriving from international agreements and the development of methods for tracing cyber crime. One would argue, if this would happen, cyber launderers would find alternative jurisdictions to host illegal electronic content or create offshore companies and maintain management or access services remotely.

6. Conclusion

Conclusively, the countries of South-Eastern Europe in general do consist an alternative for money laundering activities, as they currently do not have strict anti-money laundering policies. Provided that they comply with international efforts at some point, combined with their future accession to the European Union the problem would seem to have been resolved. Still, the means of information society imply that money laundering will become more uncontrollable than ever, not only in the region but also worldwide. Adoption in the first place and implementation in the second of legislative provisions is unable to follow the pace of technological advances[84]. Relatively, it is indicative that the FATF experts group mention in late 1999, when the Internet certainly wasn't new to the international community that "there [is still] a need within the law enforcement community to develop expertise in the detection and investigation of potential money laundering in the Internet environment"[85].

The states cannot reduce or abstain from offering technologically advanced services or benefits to their citizens. The opposite would mean to choose not to digitalize a respectable amount of information and services important for the operation of the state itself or the economy in order to avoid criminal activity. On the other hand, "with electronic cash, investigators will have to (…) look at the [encrypted] packets themselves to determine if a money transfer is taking place". Consequently, transnational coordination in such a level would represent "a whole new order of intrusive supervision of global communications".[86]

In any event, the Internet users are the ones to make the first step, for their own benefit and in order to make the scene clearer for authorities to act. On this regard, efforts are being made to warn consumers not to trust web service providers that do not clearly present information about their company. Article 5 of the EC e-commerce Directive requires that this kind of information is rendered by the service provider "easily, directly and permanently accessible to the recipients of the service and competent authorities"[87]. The ESTLA considers establishing a certificate to be used by the web sites of its members that would guarantee the quality of the service

[84] Snaith I., n 13 above, p. 12.
[85] FATF-XI, 2000, n 14 above, p.4.
[86] Taggart, St., n 22 above, p.76.
[87] Directive 2000/31/EC, n 53 above.

provided.[88] Furthermore, numerous web sites constitute "black lists" of gambling or commercial web sites that are to be avoided by users.[89]

[88] ESTLA, 8-2-2000, Draft Code of Conduct the use of Information Society services for the distribution of gambling services.
[89] Tovas, C-W, 31-01-2001, "History repeats itself", Gambler's Domain, <http://www.gamblers domain.com>.

ANNEX

Participation of South-East European Countries in collective anti- money laundering efforts

Country	OECD	FATF	PC-R-EV Committee (Member / Observer)	EU (Member)	EU (Candidate / Associated)	Other bodies (ESTLA)	Other bodies (FESE)
ALBANIA			✓			✓	
BOSNIA-HERZEGOVINA						✓	
BULGARIA			✓		✓	✓	
CROATIA			✓			✓	
CYPRUS			✓		✓	✓	✓
GREECE	✓	✓	✓	✓		✓	✓
HYNGARY	✓		✓		✓	✓	✓
F.Y.R. OF MACEDONIA			✓			✓	
MOLDOVA			✓			✓	
ROMANIA			✓		✓	✓	
SLOVENIA			✓		✓	✓	✓
TURKEY	✓	✓	✓		✓	✓	
F.R. OF YUGOSLAVIA						✓	

BIBLIOGRAPHY

- Bortner M., 1996, "Cyberlaundering: Anonymous Digital Cash and Money Laundering, University of Miami", School of Law.

- Bureau for International Narcotics and Law Enforcement Affairs, U.S. Department of State, "INCSR - Money Laundering and Financial Crimes", March 1999

- Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering [Doc. 391L0308].

- Denning, D.E. – Baugh, W.E., Jr, 2000, "Hiding crimes in cyberspace", *Cybercrime, Law enforcement, security and surveillance in the information age*, Ed. Thomas, D. – Loader, B.D., Routledge.

- 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) [17-7-2000, L 178/1]

- ESTLA, 8-2-2000, Draft Code of Conduct the use of Information Society services for the distribution of gambling services.

- ESTLA, 25-9-2000, New Media and Internet working group report, Meeting on Paris, France.

- European Commission, Proposal for a European Parliament and Council Directive amending Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering. [Doc. 599PC0352].

- FATF/OECD, 1996, *Forty Recommendations*

- FATF/OECD, 2-6-2000, *Annual Report 1999-2000*.

- FATF-XI, 3-2-2000, *Report on Money Laundering Typologies 1999-2000*, FATF/OECD.

- FATF-X, 11-2-1999, *Report on Money Laundering Typologies 1998-1999*, FATF/OECD.

- FATF-IX, 12-2-1998, *Report on Money Laundering Typologies 1997-1998*, FATF/OECD.

- FATF, 2000, Report for Greece.

- FATF, 2000, Report for Turkey.

- Gilmore W., 1995, *Dirty Money*, Council of Europe Press, Strasbourg.

- Kerin H. (Ed.), January 2001, Business File Newsletter – Greek Special Survey Series, *Economic and Industrial Review*, No 8.

- Lloyd, I.J., 2000, *Information Technology Law*, Butterworths

- Norton, R., September 1999, "In Defence of Money Laundering", Fortune.

- PC-R-EV Committee, Reports for Bulgaria, Croatia, Cyprus, Hungary, Romania, Slovenia, F.Y.R.of Macedonia to be included in the 1999-2000 Annual Report, Council of Europe.

- Republic of Bulgaria, Measures Against Money Laundering Act, [No. 85/24-07-1998].

- Reitinger P.R., "Encryption, Anonymity and Markets", *Cybercrime, Law enforcement, security and surveillance in the information age*, Ed. Thomas, D. – Loader, B.D., Routledge 2000.

- Snaith I., 2000, "Money Laundering, Financial Services and the European Union: Ever Expanding Regulation?", unpublished.

- Taggart, St., "Dotcoms desperately seeking sovereignty", The Industry Standard – Europe, 23 Nov. 2000

- The Economist, 27-1-2000, Survey: Globalisation and Tax, "Net losses: Why the taxman fears the Internet".

- United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Vienna, 20 December 1988.

On-line sources:

- Council of Europe, <http://www.coe.int>
- E-cash, <http://www.digicash.com>
- E-gold, <http://www.e-gold.com>
- ESTLA <http://www.european-lotteries.org>
- Europa web site, <http://www.europa.eu.int>
- FATF/OECD, <http://www.oecd.org/fatf>
- FESE, <http://www.fese.be>
- Global Internet Statistics <http://www.glreach.com>.
- International Financial Risk Institute (IFCI) <http://risk.ifci.ch>