Fausto Martin De Sanctis

Technology-Enhanced Methods of Money Laundering

Internet As Criminal Means

Springer

Technology-Enhanced Methods of Money Laundering

Fausto Martin De Sanctis

Technology-Enhanced Methods of Money Laundering

Internet As Criminal Means

Springer

Fausto Martin De Sanctis
3rd Region
Federal Court of Appeals
São Paulo, Brazil

ISBN 978-3-030-18329-5 ISBN 978-3-030-18330-1 (eBook)
https://doi.org/10.1007/978-3-030-18330-1

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Acknowledgments

I want to express my gratitude to the Federal Judicial Center (FJC), notably Mira Gur-Arie, and the Law Library of Congress (LLC), especially Eduardo Soares, both in DC, for having the opportunity to access documents, judicial decisions, courts, and authorities in the United States.

I thank all of the people at the FJC and LLC and the staff of my chambers for their invaluable help and support.

I would like to give special thanks to Viviane do Amaral for her support, affection, and friendship.

Finally, I would like to express my thankfulness to my sons, Thomaz and Theodoro, for their constant motivation for my work, as well as to the Creator for his love over the creation.

Contents

About the Author

Fausto Martin De Sanctis who has a PhD degree in Criminal Law from São Paulo University (USP), is a Member of the Community of Portuguese-speaking Jurists and of the Advisory Board of American University for Legal Studies Programs Brazil, USA, is a Specialist in Civil Procedure from Brasília University (UnB), is Federal Appeals Judge at the Federal Court of Appeals for the Third Region, and is a Writer.

He started the career of the federal judiciary in 1991. Previously, he was a São Paulo State Judge (1990–1991), Public Prosecutor of the Municipality of São Paulo, and Public Prosecutor of the State of São Paulo in the area of the Public Defender's Office. He was a Professor at São Judas Tadeu University for 15 years.

He is General Ombudsman of the Federal Court of Appeals for the 3rd Region and Supervisor of the Monitoring Group of the Federal Penitentiary System.

As the Head of the 6th Criminal Court in São Paulo, specializing in money laundering and financial crimes, for 20 years, he judged complex cases involving financial institutions, several clandestine exchange dealers ("doleiros"), and international drug traffickers, etc.

He is Pioneer in the early sale of goods (before the final decision); in the performance of award-winning or plea-bargaining donations, serving as a basis for regulation of the law; in the allocation of resources to philanthropic entities received in donations (as a form of indemnification to society and show of repentance), donation of works of art for cultural entities and destination to public squares; and in the procedure of telephone interception, adopted by the subsequent legislation.

He received an honorary distinction from the New York State Bar Association (NYSBA) for being considered the forerunner of decisions to prevent and combat corruption and money laundering in Brazil (2016), distinction in commemoration of the 60th anniversary of the departure of the First Contingent of the Suez Battalion toward the Middle East, by the Brazilian Association of UN International Peace Forces (2018); Commendation of the Order of Judicial Merit, in the rank of Grand Officer, by the Labor Court of Appeals for the 2nd Region (2015); Anchieta Medal and Gratitude Diploma of the City of São Paulo (2011); Tiradentes Medal/Rio State Congress—ALERJ (2010); distinctions by the Military Police of the State of São

Paulo (2009) and by the Council for Control of Financial Activities (COAF), Brazilian Financial Intelligence Unit (2008) etc.

He was indicated by his peers in the Association of Federal Judges of Brazil (AJUFE)'s list to occupy a seat in the Brazilian Supreme Court in 2010, 2014, and 2017. His name was included in a list subscribed by the jurists, among them, Miguel Reale Júnior, Modesto Carvalhosa, and Hélio Bicudo, and by 49 class entities and social movements organized for the same purpose on January 25, 2017. He has lectured in Brazil (public and private entities) and abroad, among them the United States (UN/DC, American Congress/DC, Federal Judicial Center -FJC/DC, World Bank/DC, Massachusetts Division of Banks/Boston, Money Transmitter Regulators Association - MTRA/Kansas City, Inter-American Development Bank -IADB/DC, Harvard University/Cambridge, Columbia University/NY, Syracuse University/Syracuse, American University/DC, George Washington University/DC, Georgetown University/DC, Yale University/New Haven, Marquette University/Milwakee); China (Hong Kong University), Russia (Moscow State University), Turkey (Istanbul University), France (The Organization for Economic Cooperation and Development -OECD and Cour de Cassation/Paris), Germany (Heidelberg University/Hannover), Austria (International Anti-Corruption Academy (IACA)/Vienna), Angola (European Union/Luanda), Mozambique (UN/Maputo), Canada (York University – Terrorism, Transnational Crime and Corruption Center -TraCCC/Toronto), Qatar (ONU/Doha), India (Jindal University/Nova Delhi), Malaysia (International Anti-Corruption Conference (IACC)/Kuala Lumpur), Argentina (Grupo de Ação Financeira da América Latina (GAFILAT)/Buenos Aires), Peru (Ministerio de Justicia y Derechos Humanos/Lima), and Mexico (Fiscalía Anticorrupción/Hermosillo).

De Sanctis has written a number of articles published in newspapers and magazines specializing in law and economics, besides books.

His publications include, among others, the following:

Books

International Money Laundering Through Real Estate and Agribusiness: A Criminal Justice Perspective from the "Panama Papers." Cham, Heidelberg, New York, Dordrecht, London: Springer, 2017

Churches, Temples, and Financial Crimes: A Judicial Perspective of the Abuse of Faith. Cham, Heidelberg, New York, Dordrecht, London: Springer, 2015

Economic and Dinancial Delinquency (Delinquência Econômica e Financeira). Rio de Janeiro: GEN/Forense, 2015

Football, Gambling, and Money Laundering: A Global Criminal Justice Perspective. Cham, Heidelberg, New York, Dordrecht, London: Springer, 2014

Criminal Law – General Rules (*Direito Penal – Parte Geral*). São Paulo, Método, Rio de Janeiro: Forense, 2014

Money Laundering Through Art: A Criminal Justice Perspective. Cham, Heidelberg, New York, Dordrecht, London: Springer, 2013

Money Laundering Through Gambling and Soccer: Analysis and Proposals (*Lavagem de Dinheiro. Jogos de Azar e Futebol. Análise e Proposições*). Curitiba: Editora Juruá, 2010

Criminal Liability of Corporations and Modern Criminal Methods (*Responsabilidade Penal das Corporações e Criminalidade Moderna*). São Paulo: Saraiva, 2009

Organized Crime and the Disposal of Seized Assets: Money Laundering, Plea Bargains, and Social Responsibility (*Crime Organizado e Destinação de Bens Apreendidos. Lavagem de Dinheiro, Delação Premiada e Responsabilidade Social*). São Paulo: Saraiva, 2009

The Fight Against Money Laundering: Theory and Practice (*Combate à Lavagem de Dinheiro, Teoria e Prática*). Campinas: Millennium, 2008

Criminal Tax Law: Highlights (*Direito Penal Tributário: Aspectos Relevantes*). Campinas: Bookseller, 2006

Criminality in the National Financial System: Criminal Law and Protection of Brazil's National Financial System (*Punibilidade no Sistema Financeiro Nacional: Tipos Penais que Tutelam o Sistema Financeiro Nacional*). Campinas: Millennium, 2003

Criminal Liability of Corporations (*Responsabilidade Penal da Pessoa Jurídica*), São Paulo: Saraiva, 1999

Articles and Book Chapters

"Football: A Call for Transparency to Curb Corruption." Sociology and Criminology 4:133, OMICS International: Publications, Benefits & Features, 2016.

"Improving Delivery in Development: The Role of Voice, Social Contract, and Accountability." Chapter: "Voice and Accountability: Improving the Delivery of Anticorruption and Anti-Money Laundering Strategies in Brazil." The World Bank Legal Review, vol. 6. Washington, DC: World Bank Group, 2015

"Southwestern Journal of International Law." Chapter: "Requirements for the 2014 FIFA World Cup in Brazil and Requirements of Governmental Bodies to Deter Financial Crimes in the Football Sector." California: Southwestern Law School, 2015.

"Criminal Liability of Corporations" ("Responsabilidade Penal das Corporações"). In *A Book in Honor of Miguel Reale Junior* (*Livro Homenagem a Miguel Reale Junior*). Rio de Janeiro: GZ, 2014

"Popular Action: Using Habeas Corpus in the Context of Financial Crimes" ("Ação Popular: A Utilização do Habeas Corpus na Dinâmica dos Crimes Financeiros"). In *Popular Action* (*Ação Popular*). São Paulo: Saraiva, 2013

"Coherent and Functional Criminal Law" ("Direito Penal Coerente e Funcional"). São Paulo: Revista dos Tribunais, Vol. 919, 2012

"Telephone Tapping and Fundamental Rights" ("Interceptações Telefônicas e Direitos Fundamentais"). In *A Tribute to Afrânio Silva Jardim: Writings and Studies* (*Tributo a Afrânio Silva Jardim: Escritos e Estudos*). Rio de Janeiro: Lúmen Júris, 2011

"The Constitution and Freedoms" ("Constituição e Regime das Liberdades"). São Paulo: Revista dos Tribunais, 2009

"Human Trafficking: The Crime and Victim Consent" ("Tráfico Internacional de Pessoas: Tipo Penal e o Consentimento do Ofendido"). In *Women and Criminal Law* (*Mulher e Direito Penal*). Rio de Janeiro: Forense, 2007

"Crimes Against the National Financial System: A Precursor to Money Laundering" ("Crimes Contra o Sistema Financerio Nacional como Antecedentes de Lavagem de Valores"). In *Money Laundering - Commentary on the Law by Judges at Specialized Courts, In Honor of Gilson Dipp* (*Lavagem de Dinheiro – Comentários à Lei pelos Juízes das Varas Especializadas. Homenagem ao Ministro Gilson Dipp*). Porto Alegre: Livraria do Advogado, 2007

Chapter 1
Introduction

Modern criminals are focusing on the Internet.[1] Since they are increasingly using it to turn dirty money, criminals become more creative and opportunistic money launderers than before. Old methods like to convert, in a casino, their loot into a clean win on the roulette table or redeeming an insurance policy at a discount apparently has gone.

Internet is one of the main sectors attractive to criminals as a means of laundering the proceeds of all types of illegal activity. Most people are familiar with the spam when a high source asks help to transfer significant amounts of money, but first, it is required banking details which promptly will be used to empty accounts and then disappear.

For instance, two scams, in which criminals do actually transferring large amounts of money into an account and then ask the holder to forward it, or offering people jobs in which they can make a substantial income working from home; however, the "job" involves accepting money transfers into their accounts and then passing these funds on to an account set up by the employer.[2]

Also, tax misapplication on Sales, Use Tax, and Games must be a concern because with the rise of virtual worlds, those who cash out, that is, convert virtual wealth to real-world wealth, should be taxed on their gains, especially when there is an activity that occurs entirely within virtual words, what makes it an attraction field for many criminals.

It was not by accident that crime took such an unusual turn. Controls enacted pursuant to recommendations by the Financial Action Task Force—FATF made it necessary to seek out new mechanisms for the laundering of ill-gotten gains.

[1] The Internet began in 1969 as a network of four computers located at the University of California at Los Angeles, the University of California at Santa Barbara, the University of Utah, and the Stanford Research Institute. The U.S. Department of Defense funded the initial work through an entity known as the Advanced Research Projects Agency–ARPA. The ARPA Network (ARPANET) was designed to be a decentralized system. See American Bar Association [1, p. 1814].

[2] See MIT—Technology Review [2].

F. M. De Sanctis, *Technology-Enhanced Methods of Money Laundering*,
https://doi.org/10.1007/978-3-030-18330-1_1

Furthermore, the globalization of financial markets and the rapid development of information technology have gradually steered the underworld economy towards new possibilities for the commission of crimes.

Internet is an attractive sector for the practice of money laundering because of the large monetary transactions involved, the general unfamiliarity and confidentiality surrounding it, and the unlawful activity endemic to it due to fake identity or anonymity.

According to Cecily Raiborn, Chandra Schorg, and Christie Bubrig, "laundering money on the Internet entails transferring money electronically from one bank to another, using different names and different locations. The process is repeated until the money becomes clean or untraceable. Three advantages of laundering money on the Internet are that the transactions can be made as often as one wants, with anonymity, and from remote locations."[3] Anonymity is essential to money-laundering activity and becomes undesirable in attempting to control such a process.

The purpose here is to inquire into the scale of the problem and to look into legislative and institutional loopholes that might give power and mobility to organized crime, thereby making it a more deeply entrenched source of unprecedented illicit wealth. The carefree attitude which has been characterized by the industry must be confronted with a realistic understanding of the problem, and must go beyond the adoption of measures taken in isolation or in an uncoordinated manner, lest conflict and instability continue to undermine its credibility and possibly even jeopardize its continued existence.

No one predicted the reach of the World Wide Web, the rise of alternative payment systems, of the massive exploitation of the Dark Web. To Louise Shelley "The spread of the internet was originally interpreted almost entirely as a force for good. The assumption that greater connectivity and greater access to information would lead to more prosperity and greater intercultural understanding was rarely questioned and is still implicit in the way we continue to think about digital transformations. Not enough serious attention is given to dark sides of the globalized digital economy."[6] (see SHELLEY, Louise I. *Dark Commerce. How a New Illicit Economy is Threatening Our Future*. Princeton, New Jersey: Princeton University Press, 2018, p. 03) This analysis seeks to provide a basis for a number of important public decisions, to prompt specialists to speak up in order to keep Internet from being used or manipulated for illegal purposes, and to expound on situational vulnerabilities confronting this market which are not clearly understood by authorities or society at large.

Inasmuch as Internet, like art,[4] is a subject of universal interest, it must not be exempted from criminological scrutiny because of its great social, educational, and cultural importance.

We must constantly reflect on how authorities are defied on a daily basis in their efforts to take steps to prevent money laundering and the financing of terrorism and organized crime. Closer scrutiny is necessary if we are to understand the new global

[3] Raiborn et al. [3, p. 37].

[4] See the author De Sanctis [4].

situation that has encouraged the commission of serious crimes and the illegal enrichment of criminals. In other words, we seek solutions that will make effective criminal enforcement possible.

It is important to be mindful that one of the essential criminological features inherent in money laundering, as Pedro Caeiro, citing Jorge Fernandes Godinho and Luís Goes Pinheiro, reminds us,[5] is its necessary links to organized crime, which in turn add considerable diversity to the types of conduct that its prosecution and enforcement may prevent.

Therefore, strong criminal enforcement on the part of government is required from the outset, including investigations into assets of suspects, so that—by confirming their propriety and legitimate ownership—we may do away with the idea that crime pays, albeit despite occasional convictions and sentencing.

The author's purpose is to go beyond a mere introduction to this captivating subject. Considerations will be presented in an effort to further the study of methods likely to add transparency to business dealings and thereby inhibit or curtail unlawful activity. This work seeks to dispel the many mysteries surrounding the business of Internet.

The idea is to connect a number of important dots in the cyberspace, where its business practices are concerned, so as to bring about improvements in crime prevention systems. Our hope is to provide a useful foundation for conducting a critical analysis that is both realistic and practical, and to include an overview of studies already conducted worldwide which touch upon this important and current topic.

The aim here is to provide a reading on this sector, a snapshot of the Internet misunderstands which will provide the groundwork and guidance necessary to give it transparency and a backdrop sufficient for a particularized analysis. Some rigor in procedures for cataloging and investigation are in order, for we ought to remember that the resurgence of organized crime is often the result of a systemic atmosphere of inattention, mutual tolerance, and ethical codes which, however lofty, are in practice applied only selectively. Matters are worsened by the arrogance and permissiveness, if not covert complicity, of portions of civil society (the elite, the press, etc.) that insist on pointing out only the defects that do not suit their purposes.

As combatting crimes through Internet, especially money laundering, is a massive and complex activity, which requires a clear and holistic understanding of the various trends and techniques, criminals can adjust quickly to exploit new opportunities that often allow anonymous high value transactions with little or no paper trail or legal accountability.

An attempt to get a basis for detecting main evolving criminal schemes through Internet, this book is divided into ten chapters. Chapter 1 is the introduction. Chapter 2 deals with overarching topics of cyber-attacks or cybercrimes. Chapter 3 addresses the difficult task of catching online sales financing criminals. Chapter 4 is about social media, and the role of people in it. Chapter 5 seeks to organized online gaming. Chapter 6 addresses forms of payment and the use of NGOs and trusts, and their potential for the movement of ill-gotten gains. Chapter 7 specifically addresses the

[5] Cf. Pedro Caeiro [5].

tax misapplication, which can greatly help to clarify how money-laundering prevention applies to the Internet. International legal cooperation, repatriation, and asset forfeiture are analyzed in Chap. 8. Conclusions are covered under Chap. 9. Final Chap. 10 covers national and international proposals for improving the industry so as to prevent all sorts of crimes on the Internet, like money laundering and the financing of terrorism.

Although this work may, at a glance, appear to cover the entire subject, this is actually far from the case. It has, however, aimed at achieving a logical and practical "completeness" in describing a little or unexplored virtual world, in which cyberspace is used in the commission of serious crimes. The purpose here is to see to it that the use of Internet in the commission of crimes is seldom, if ever, carried to fruition.

References

1. American Bar Association. (2000). Achieving legal and business order in cyberspace: A report on global jurisdiction issues created by the internet. *The Business Lawyer, 55*, 1801–1946.
2. MIT – Technology Review. (2013, October 18). *The secrets of online money laundering*. Retrieved August 14, 2018, from https://www.technologyreview.com/s/520501/the-secrets-of-online-money-laundering/
3. Raiborn, C., Schorg, C., & Bubrig, C. (2003). Guarding against e-laundering of dirty money. *Commercial Lending Review, 18*, 36–39.
4. De Sanctis, F. M. (2013). *Money laundering through art: A criminal justice perspective*. Cham: Springer.
5. Caeiro, P. (2005). Manual distributed in a course sponsored by the OAS and the Brazilian Ministry of Justice and presented to Brazilian judges and prosecutors on October 17–21, 2005. In *Branqueamento de capitais* (p. 4).
6. Shelley, L. I. (2018) Dark Commerce. How a New Illicit Economy is Threatening Our Future. Princeton, New Jersey: Princeton University Press, p. 03.

Chapter 2
Dark Web: Deterring Cybercrimes and Cyber-Attacks

On the one hand, the world is changing since cyberspace has been blanketed all continents. People and their rights (like privacy) are under siege. On the other hand, money-laundering crime laws have become increasingly important in recent years. Many changes have taken place to keep up with the globalization of the economy. Until recently, there were great schisms between East and West and between North and South, and even a Cold War complete with Communist-derived Socialism. As the idea of a market economy gained prevalence, even in countries with no such tradition (such as China), and technological innovations advanced, there grew a need for new managerial practices applied to businesses.

Criminals likewise evolve over time. Despite the positive hopes brought on by the advent of globalization, a cutthroat and destructive competitiveness also developed. There are new and growing fears because we do not know where all of this is headed (though trends look ominous).

The globalization inherent in today's world, with all of its advantages and disadvantages, fosters a transnational and technological criminal enterprise, practiced even by large conglomerates and businesses that necessitate unprecedented cooperative exchanges among nations.

As stated by Ronald Griffin, "…cyberspace technology, when put in the wrong hands, is threatening and unfriendly. Business computers prowl the landscape to compile data about us. Government software spies on people to trap law breakers."[1]

The special field of financial crime, whether committed or not by the Internet, is justified by the simple idea that market rules alone cannot address all of the aspirations emerging within the context of the course of business practices—oftentimes crossing through dangerous, ethical gray areas.

The legal protection of property requires government intervention and social and economic regulation so that the rules of conduct with regard to business practices may be stabilized and hence preserved.

[1] Griffin [1, p. 136].

F. M. De Sanctis, *Technology-Enhanced Methods of Money Laundering*,
https://doi.org/10.1007/978-3-030-18330-1_2

Objects of legal protection enjoy a sort of global protection, not just by criminal law, but rather, through the expectation of general stability engendered by rules fostering the proper and honest functioning of markets (of corporations, of private and public roles, of derivative securities, etc.).

This is an area of criminal law designed to fill in loopholes in the definitions[2] of crimes against property owing, in large part, to increases in criminal infractions resulting from the exponential increase of economic activity within the State and of international financial relationships.

Of course criminal law does apply, albeit in a fragmented, subsidiary (last resort) role, with no expectation that its financial branch will function in more than a supporting, symbolic role. Yet when we see that such principles are invoked indiscriminately, without the slightest basis in reason, the result is a systemic lack of protection to the economic order.

The take-away here is that financial crime, as money laundering, is a very current subject, *whether by the magnitude of the material damage it causes, or by its capacity to adapt to, and survive, social and political changes, or even because of its readiness to come up with defenses and to defeat all efforts to combat it.*[3]

Conceptualizing financial crime is no simple task. It does not lend itself to simple measurement by the extent of resulting damages. The classification of financial crimes rests on the collectivized or supra-individual nature of the legal interests or assets that is to be protected.

Reducing intervention to only those alleged facts actually held meritorious is just as imperative as trimming away criminal liability hidebound by excessive formalism. Yet the fact remains that administrative sanctions alone have not sufficed to enforce the basic duties we as citizens are bound by as actors in the economic system.

Criminal law has from the outset concerned itself with protecting the basic institutions of government, and citizens' most basic interests. Over time, however, in addition to being relied upon to provide minimum standards of coexistence, it began to also lend itself to the protection of new social and economic interests. A radical shift in government intervention strategies was enacted to combat the intimidating phenomenon of organized crime which was petulantly working its will on politicians, journalists, judges, businessmen, and so on.

Crimes must be tackled alongside the image of the criminal and the social effects of that type of conduct. The conclusions advanced by Edwin Sutherland defined white-collar crime as crimes committed by an honorable person with social and professional prestige,[4] which may explain why this type of criminal conduct generates little in the way of social reaction. The same can be said about online crimes.

Perhaps this phenomenon is due to the perception of minimal dangerousness of the criminal in the absence of direct violence or confrontation with the victim, or even because no physical harm is even contemplated. This brings us to the idea

[2] In Pedrazzi [2].

[3] Cf. Oliveira [3, p. 69].

[4] In Cavero [4, pp. 276–277].

advanced by Thomas Lynch, that serious crime is more ink-stained than blood-stained.[5] Hence, perhaps, it involves a certain moral neutrality.

According to Dr. José Ángel Brandariz Garcia, imprisoning financial criminals would not even result in the negative social stigma typically expected for those identified as criminals, given their personal and socioeconomic characteristics.[6]

However, it should not be by any means common knowledge that crimes committed online are less harmful to society than crimes committed by other means, given its penetration into our lives and social fabric. In truth, it ends up fostering ordinary criminality (corruption, unfair competition, fraud, etc.). This hampers enforcement efforts if there is widespread ignorance about the harmful effects on society that result from delinquent practice due to the unlimited range of network usage.

Criminals do, in fact, have great potential for engendering crime. They are highly adaptable within society, and often enjoy considerable tolerance within the dark web community, which leads to their increasingly daring and dangerous criminal behavior.

Furthermore, criminals actually run a sort of cost-benefit analysis on the gains to be had from unlawful conduct and possible sanctions (sentences) imposed by the legal system. By running a utilitarian calculation[7] one could easily conclude that getting caught involves little or no consequence, given the complexity and inaptitude of some inneffective criminal justice systems.

Cláudia Cruz Santos argues that *theories of rational choice and situational prevention seem to fit them like a glove. Their assessment of the costs and benefits associated with misconduct might dissuade them from engaging in it, should the opportunities decrease and the possibility of detection and punishment increase.*[8]

The deciding factor is not will, but rather the impracticability of the behavior prohibited by law. No longer can we afford the luxury of complex theorizing over abstract hazards and social harm. Categories of financial crime have to do with increasingly complex regulatory situations, and conduct that is legally intolerable, irrespective of the intentions of the criminal. Those intentions would only come out afterward, after the decision was made to break the rules of conduct binding upon us all.

Financial crime practiced or not through the dark web, given its scope and potential for damage, is consigned to the jurisdiction of the Federal Government—at least in countries such as Brazil and the USA, which rely on a dual justice system.

> A good portion of this jurisdiction is brought to bear upon crimes that are complex, sometimes on account of the suspects or defendants involved—people of great economic or political power who, as a rule, operate within a network having international ramifications—and other times because of the type of financial crime involved, be it corruption, influence-peddling, money laundering, etc. Its seriousness, its harm to society and that

[5] *Apud* Mir and Genovês [5].

[6] In Garcia [6].

[7] Fischer [7, p. 37].

[8] Cf. Santos [8].

> threat it poses to institutions which safeguard the Rule of Law require a different balance between the rights of the accused and other procedural requirements of speedy trials and the duty of the State to prosecute and punish unlawful conduct.[9]

This harmful and unlawful behavior under federal jurisdiction requires recognition of financial criminal conduct as a violation of a negative legal duty, namely, that of refraining from illegitimately harming others or the public order, and of a positive legal duty, that one's behavior be conducive to the greater good of society. This progressive view of legality is increasingly accepted. It does, however, require more complex analysis, involving the said legal duties (both negative and positive) upon which foundation a specific legal and criminal appraisal is constructed.

If we can affirm about a concern of dual justice system about the financial crime, money laundering has a different approach because it can be achieved by ordinary criminals, deserving the same institutional treatment.

The reintegration of criminals into society must therefore center on making them rethink their behavior. If there is indeed any reasoning behind unlawful conduct involving cost-benefit analyses of the outcomes to the offender, a given crime will be committed if and only if the expected penalty is outweighed by the advantages to be had from committing the act.[10] This also applies in case of online crimes, in which, to the point of exhaustion, we see complexity, anonymity, or fake identities.

Several transactions take place over the Internet each day, and with its inherent features, it has been possible to launder illegally acquired funds by criminal organizations. Due to its complexity, the online accounts become more untraceable, and the more untraceable they are, the more dirty money has been used. In terms of criminal matters, rules of evidence often require the prosecution to establish the chain of custody for the evidence it wishes to introduce at trial.

It is important, as stated by Timothy A. Vogel, "procedures for gathering evidence of a cyber-attack take into account these requirements in case a decision is made later to refer the matter to law enforcement for criminal prosecution."[11]

Avoiding detection, money laundering is experiencing some changes as criminals has been optimized payment mechanisms, by micro laundering via sites like PayPal. This has created an increasing difficulty for many law enforcement bodies.

After blanking the world, cyberspace has changed everything, and criminals are using Internet to poach data from other devices, by assuming somebody's identity, and people taking webs to bully others.

For instance, the number of complaints and consumers becoming victims of auction fraud increases annually. Though host auction websites, according to Dara Chevlin, "should be permitted to govern themselves, claiming that their mechanisms are most effective to prevent fraud, the statistics clearly show that their efforts are ineffective in stemming the growing problem of online auction fraud. The scam

---

[9] Oliveira [3, p. 71].

[10] For more on this, see Sánchez [9, p. 11] and Rodrigues [10, pp. 484–485].

[11] Vogel [11, p. 42].

artists are becoming smarter and using the anonymity of the Internet to their advantage. Several cases have attempted to make eBay accountable for fraudulent activity that occurs on their site because the host auction website makes money at the close of every auction held on their website (fraudulent or not), what incentive does e-Bay have to keep a closer eye on its users? Of course, eBay wants to maintain its reputation. But until host auction sites feel the impact of fraud in their earnings, fraud prevention will not receive the attention and investment of resources that it deserves." The author recommends the imposition of stricter federal regulations on host auction websites.[12]

The transition of crimes to the Internet has created unique challenges for law enforcement. Talking about prostitution on the Internet, Mellissa Farley, Kenneth Franzblau, and M. Alexis Kennedy say that "the prostitution transaction includes not only victim, buyer and trafficker/pimp but the most invisible partner: the online advertiser. When prostitution happened on the street in someone's neighborhood, it was clear whose jurisdiction that was. Enforcement of a range of laws against johns and pimps was sometimes fueled by citizens' concern about prostitution as a neighborhood nuisance rather than concern about prostitution's exploitation and violence. Communities wanted prostitution out of sight and out of their neighborhoods. Because online sex businesses are less visible to the public, victims of sexual exploitation in prostitution are isolated and can be in greater danger from sex buyers." For them, "it is incumbent upon policy makers and law enforcement to enforce existing laws and where needed, to develop new laws and policies that will abolish online (and offline) trafficking and prostitution. While many have been recruited, sold and trafficked into prostitution on social networking sites, the sites can also be turned against traffickers."[13]

Ronald Griffin, citing a case involving business, mentioned the Paradigm Alliance Case. Paradigm and Celeritas were parties to a joint venture and each one placed their business interests in the other's hands on an understanding that they nurture their relationship. One day, long after their relationship was underway, a Celeritas' employee hacked Paradigm's computer. He looted information from the machine and poured the booty into a patent application for new type of software.[14]

It is true that almost every employee is provided with some type of computer access and an email account. The network established on these corporations is increasingly connected to Internet and other companies, raising a new set of threats.

It is interesting to mention here two cases decided in the USA involving the so-called dark web.

Ross Ulbricht, also known as "Dread Pirate Roberts," was sentenced on May 29, 2015 in Manhattan federal court to life in prison in connection with his operation and ownership of Silk Road, a hidden website designed to enable its users to buy and sell illegal drugs and other unlawful goods and services anonymously and beyond the reach of law enforcement between January 2011 and October 2013.

[12] See Clevlin [12, p. 255].

[13] See Farley [13, pp. 1090–1991 and 1094].

[14] Griffin [1, p. 145].