ISSN 2236-0859

DIREITO & DESENVOLVIMENTO

REVISTA DO PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO E DESENVOLVIMENTO SUSTENTÁVEL

DARK WEB AND BITCOIN: AN ANALYSIS OF THE IMPACT OF DIGITAL ANONYMATE AND CRYPTOCURRENCIES IN THE PRACTICE OF MONEY LAUNDERING CRIME

ROMULO RHEMO PALITOT BRAGA
ARTHUR AUGUSTO BARBOSA LUNA

VOLUME 9 | NÚMERO 2 | AGO/DEZ 2018

DARK WEB AND BITCOIN: AN ANALYSIS OF THE IMPACT OF DIGITAL ANONYMATE AND CRYPTOCURRENCIES IN THE PRACTICE OF MONEY LAUNDERING CRIME

DARK WEB E BITCOIN: UMA ANÁLISE DO IMPACTO DO ANONIMATO DIGITAL E DAS CRIPTOMOEDAS NA PRÁTICA DO CRIME DE LAVAGEM DE DINHEIRO

Recebido: 25/11/2018
Aprovado: 26/11/2018

Romulo Rhemo Palitot Braga*
Arthur Augusto Barbosa Luna**

ABSTRACT: This article analyzes some of the existing digital anonymity technologies, as well as their impact on the process and facilitation of the money laundering process. It presents the concept of superficial Internet and clarifies the difference between the Deep Web and the Dark Web, exposing how it works one of its most important operating structures, the TOR protocol. It also details the operation of Bitcoin, one of the most important cryptocurrencies today, and draws a parallel on how these technologies can impact the practice of money laundering, as well as discusses the capacity of the mechanisms currently in place to curb and punish it.

Keywords: Deep Web. Dark Web. Bitcoin. Money laundry.

RESUMO: Este artigo analisa algumas das tecnologias de anonimato digital existentes, bem como seu impacto no processo e facilitação do processo de lavagem de dinheiro. Apresenta o conceito de Internet superficial e esclarece a diferença entre a Deep Web e a Dark Web, expondo como funciona uma de suas estruturas operacionais mais importantes, o protocolo TOR. Também detalha o funcionamento da Bitcoin, uma das moedas criptográficas mais importantes da atualidade, e traça um paralelo sobre como essas tecnologias podem impactar a prática da lavagem de dinheiro, bem como discute a capacidade dos mecanismos atualmente em vigor para refrear e punir isto.

Palavras-chave: Deep Web. Dark Web. Bitcoin. Lavagem de dinheiro.

1 INTRODUCTION

The technological leaps we have experienced recently have dramatically altered personal and business relationships across the globe. In the last 10 years, people have come to communicate with an unprecedented facility, shortening distances and giving dynamism to the once unusual social and economic phenomena. In this context, virtual currencies have been created and, without regulation or efficient control mechanisms, gain space in transactions performed in virtual environments.

* Doctorade and Master's in Criminal Law from Universidad de Valencia, Espanha; Permanent Professor Permanente of the Post-Degree Programs of the Centro Universitário de Joao Pessoa – PPGD/UNIPE and the Federal University of Paraíba – PPGCJ/UFPB; Auditor of the Superior Court of Sportive Justice of the Brazilian Confederation of Auto Racing; Lawyer. E-mail: romulo.palitot@uv.es

** Master's in Law and Development from the Post-Degree in Law Program of the Centro Universitário de João Pessoa PPGD/UNIPE; Post-Degree Diploma in Business Administration from Langara College, Vancouver – British Columbia, Canada; Lawyer. E-mail: luna@eml.cc

The objective of this article is to bring to light a perspective of the analysis of the phenomenon of money laundering within the Dark Web, focusing on the study of the mechanisms of digital encryption communication existing today, seeking to highlight if they facilitate the practice of money laundering and whether or not there are legal mechanisms that currently allow for highly effective enforcement and enforcement of this type of conduct. To this end, relevant concepts will be presented to understand the theme, such as the Deep Web, Deep Web, Dark Web and TOR, without which the understanding of the subject in the legal environment would be impaired.

This article is divided into three main topics. The first topic turns to the presentation of the Internet, bringing to this a brief history, subdivided into two parts, one aimed at clarifying what makes up the Internet of daily life and the other to present and detail what Dark Web is and what its difference from the Deep Web. The second turns to the presentation of Bitcoin and the cryptocurrencies, in order to clarify its functioning and the reasons for its anonymity. Finally, the third point analyzes the impacts caused by the technologies presented in previous topics in the practice of money laundering.

The methodology chosen for the elaboration of this descriptive research is based on the deductive method, through historical and bibliographical research, from national and international sources, using in large part information directly collected on Internet pages, which is considered the official mechanism of communication by those who operate, work and report on the digital technologies presented here.

2 THE INTERNET

The origin of the Internet dates back to World War II, as a result of events unleashed by it.

In February 1945, the presidents of the governments of the Allied countries met in Yalta, on the Russian peninsula of Crimea. There, Churchill, Roosevelt and Stalin divided the German territory at the end of the war. In the face of the recognition by the British and the Americans of the superiority of the Russian army's power, the Cold War began, in which both sides would wage a veiled struggle for the development of new warfare technologies, richly fueled by espionage and propaganda.

In October 1957 Russia put Sputnik, the first artificial satellite produced by humanity, into orbit, provoking the immediate American technological response, which came through the creation of the ARPA - Advanced Reasearch Project Agency, whose main objective was to develop programs related to satellites and space. Years later, following the creation of NASA - National Aeronautics & Space Administration - in 1958, ARPA shifted its focus and concentrated its efforts on the study of the newborn area of informatics, which provided the further development of network communication protocols between computers - hitherto incompatible with each other - culminating in the creation of ARPANET - on December 1, 1969 - the first computer network ever built, between the University of California (Los Angeles), the SRI - Stanford Research Institute and the University of Utah and University of California (in Santa Barbara).

To seek to evolve from a local network to an international network of communication was a natural consequence. However, although it is the forerunner of the Internet, ARPANET was dismantled in 1990 - after much service to the military - and was replaced by the NSFNET, created by the scientists of the NSF - National Science Foundation in reaction to the military domain over existing digital communication networks the time of its creation. The Internet is the name by which the NSFNET became popular from 1990.

Technological evolution ended up hiding what was clearly and effortlessly seen: the Internet is neither a place nor a service; the Internet is nothing more than a communication channel, a network that allows the connection between computers - and people - just as it was at the time it came. Even before the Internet existed, there were computers, but they did not communicate with each other. There was also record and archiving of data, but everything was done locally, and access was only possible through personal and direct contact with the machine.

This is relevant to the understanding of the present article insofar as it demystifies the concepts of Deep Web and Dark Web to be dealt with further by clarifying that, because it belongs to the Internet, the "deep" network and the "obscure" are nothing more than a variation on how to communicate through the World Wide Web. It also helps in the understanding that data storage is not done on the Internet itself, but through it, on physical machines located around the world.

2.1 The Surface Web

The Surface Web, or superficial Internet (TAYLOR, 2016), is the Internet we know. Also sometimes called cleranet, it is the Internet indexed, public, accessible by all (PC MAGAZINE, 2016), located on trackable servers and whose access and navigation is sufficiently recorded by the activity logs. In other words, it is the Internet that defines the term we know. Clarifies a Trend Micro dossier - one of the largest security companies on the market - on Deep Web:

> [Surface web is] that part of the Internet that conventional search engines can index and standard web browsers can access without the need for special software and configurations. This "searchable Internet" is also sometimes called the "clearnet." (CIANCAGLINI et al, 2015)

Search engines such as Google[3], Yahoo!, Bing, Ask.com, Aol Search, DuckDuckGo, Yandex, and others constantly scour the Internet for new information - links, data, metadata, etc. -, which are indexed and made available in user searches. With each search performed and every link accessed because of the search, the results are refined and become more accurate[4].

This scanning is done by the automated access of the Internet pages by search engine robots or search bots, which access all the accessible links in each page found, supplying the indexes of pages with the new results. Each new page found is also accessed by the robots and each new result added to the index, and this operation is repeated continuously (YANDEX, 2016).

Such an operation, however, is only possible when the robots can access the information contained in the pages and detect the links present there. This is the differential of the Surface Web: its structure allows the indexing, which is done mainly through the backlinks, that is, through the page addresses contained and accessed within the body of a page visited (TAYLOR, 2016). For a better understanding, if a university page contains a link to the CAPES

[3] Despite being one of the most commented search websites, Google is just one of the options available. Similar results for the same search criteria can be obtained through other engines, such as Microsoft's Bing, and Yahoo. DuckDuckGo is one of the most innovative options when it comes to privacy, since, unlike the others, it does not capture metadata from the searcher.

[4] Also included in the equation that generates the result of the searches is the boost resulting from the payment made for advertising purposes, ie some of the results presented in the search are not the result of the improvement of the search engines due to the access by the users, but, yes , the payment of an advertising amount increases the chances that the advertiser will appear in the search results (GOOGLE.COM, 2016).

website, this address, if detectable and accessible, is considered a backlink. When it comes across it the search engine accesses the CAPES page and searches for new addresses[5], indexing all the data and pages found in the course of that scan. This cycle repeats continuously and uninterruptedly.

But that's not all that defines the Surface Web. One of the most striking features of the superficial Internet is still the absence of minimal encryption of access and storage, that is, more often than not the content of the pages is stored and accessed openly - practically public -, allowing broad access and a greater probability of interception and tracking. Internet giants such as BBC, Bing and eBay still do not use the HTTPS encryption protocol[6] - as standard, and this when they do not even have the protocol implemented on their servers (BARRET, 2016; GOOGLE.COM, 2016). It is the HTTPS protocol that allows secure communication between browsers and websites (to the servers that actually store them), widely used by banks when providing virtual account access to customers[7] (ELECTRONIC FRONTIER FOUNDATION, 2016).

But to truly understand the difference in functioning between Surface Web and Dark Web you need to understand how the Internet of everyday life works.

Initially, it is necessary to clarify how the identification of machines connected to the Internet works. To access a computer network, each computer has its own address, which is called the IP address (pronounced "ái-pí" in Portuguese) and corresponds to a binary number. On the Internet the rule is the same: every computer or device that accesses it has an IP address, which is unique throughout the network (LIFEWIRE, 2016). Thus, each Internet user or server computer has its own address, which identifies its geographical location, which internet provider it is located in and the ownership of the access plan to the global computer network (who contracted the Internet service). provision of Internet services).

Such identification and tracking are only possible because the normal functioning of the Internet involves a predictable and cataloged route of access, which part of the user to the website through the Internet provider and the major distribution centers of the Internet signal the backbones[8] (MARTINS, 2009). That is, who knows the part of the signal, where the signal passes and where it goes; adding to this the local information of those who provide the service to the two ends of the connection, user and server of the website, we obtain the location of both and the ownership of who hired the service.

It is clear that identifying users and servers is not so easy because of the dynamism of the system - which is highly changeable - since it involves different jurisdictions and the internal privacy policies of each of the providers involved, among other variables, but in theory it is possible. There are trails for that.

In short, Surface Web is characterized by the indexing of content, the transparency of the data exchanged (not always encrypted) and the easy identification of the route between user and data server, which enables the tracking of the parties involved in the communication.

[5] Backlinks also serve to enhance search results, as they provide evidence of popularity, ie if a given page is heavily referenced on other pages, it is assumed to be a page of greater relevance and as such will be more likely to appear in search results more often

[6] Hyper Text Transfer Protocol Secure.

[7] Without the use of this protocol the communications between client and server (the user's computer and the website) are made in plain text, as they say. This means that everything that is sent and received is done without encryption and can be intercepted with ease. Even the caches, which are local copies of sent and received content made to streamline communication or prevent content loss, are readable. That is, if the user sends an e-mail through the webpage of a provider of this type of service that does not use HTTPS, the message is transferred in plain text as well as being cached in plain text, available for read to any user who has access to the files or to the data stream exchanged between the machines. If this same communication is made using the HTTPS protocol, it is possible to identify the sender and the service used, but not the information generated, sent and received.

[8] In literal translation it means "backbone"; represent the core physical infrastructure of the Internet.

2.2 The Deep Web and a Dark Web

The Deep Web is not a place, it is not limited to a geographical circumscription, it can not be identified and can not be perceived by the human senses. It only represents all Internet content that is not indexed by search engines, either because they belong to private networks or because they are accessible only to users of a specific type of content (CIANCAGLINI et al, 2015). The CAPES internal administrative network, for example, accessible only through the use of credentials, can not be indexed by search engines and therefore integrates Deep Web. This statement may be strange because many people speak Deep Web when referring to Dark This mix of concepts can cause confusion and for this reason both will be detailed here.

Dark Web is a virtual environment created based on protocols of high security and anonymity, such as TOR, Invisible Internet Project (I2P) and Freenet (CIANCAGLINI et al, 2015). It is a subdivision of the Deep Web, and it is it is the focus of this article. In the Dark Web, that is, in the virtual environment of the Internet in which pages are divulged and accessed with privacy and anonymity; the navigation is almost completely anonymous, and the privacy of the data exchanged is ensured by the high complexity of the encryption used.

To better understand the Dark Web, it is necessary to understand the concept of Deep Web, which is a genre of which it is a species. Trend Micro, in its dossier and through its research team, defines and Deep Web as being:

> The deep web refers to any content on the Internet that, for various reasons, can not or is not indexed by search engines like Google. This definition therefore includes dynamic web pages, blocked websites (such as those that require you to respond to a CAPTCHA to access), hostile sites, private sites (those that require login credentials), non-HTML/-context/-script, and limited access networks. Limited access networks cover all those features and services that would not normally be accessible with a standard network configuration and thus offer interesting possibilities for malicious actors to act partially or totally undetected by law enforcement. [...] Also in the limited access networks are darknets or sites stored in infrastructures that require the use of specific software such as TOR for access. (CIANCAGLINI et al, 2015)

And he clarifies, making the distinction between the deep and the dark internet:

> Much confusion lies between these two [concepts], with some outlets and researchers freely interchanging them. But the Dark Web is not the Deep Web; it's only part of the Deep Web. The Dark Web relies on darknets or networks where connections are made between trusted peers. Examples of Dark Web systems include TOR, Freenet or the Invisible Internet Project (I2P) (CIANCAGLINI et al, 2015).

Such a clear distinction between concepts imposes adaptations in this article to avoid confusion. Thus, the concept of Deep Web and Dark Web will be adopted as detailed above, pointing out the caveat when necessary, that is, when the source searched causes confusion between the two.

Thus, Dark Web represents a secure and private channel of communication in which distinct, unidentifiable and untraceable parts communicate, without supervision, surveillance or interception possibility, through special protocols such as TOR[9]. This means that this network can be used as a channel of viability and practice of crimes, although it does not serve only that.

The idea behind TOR - which supports the motto "Surveillance = Oppression", which stands for "TOR is the heart of Internet freedom" – is noble: it promises to give users back

[9] Accessible at https://www.torproject.org/.

their privacy and security in an environment in which they feel exposed - every day new security holes and new tracking technologies emerge. Thus, due to the anonymity and privacy it provides, Dark Web is widely used by the press or by people victimized by totalitarian, extremist, or similar regimes to circumvent the unjust censorship imposed (BRAGA, MARTINS, 2014). Facebook itself created an access to its network in October 2014 through the TOR[10] protocol, which in April 2016 already had more than one million hits (FACEBOOK.COM, 2016). Large companies, activists, law enforcement, military, government, and privacy-seeking people also use Dark Web (TORPROJECT.ORG, 2016). According to TOR developer group TOR (TORPJECT.ORG, 2016):

> Using Tor protects you against the common form of Internet surveillance known as "traffic analysis." Traffic analysis can be used to infer who is talking to whom over a public network. Knowing the source and destination of your Internet traffic allows others to track your behavior and interests. This can impact your checkbook if, for example, an e-commerce site uses price discrimination based on your country or institution of origin. It can even threaten your job and physical safety by revealing who and where you are. For example, if you are traveling abroad and you connect to your employer's computers to check or send mail, you can inadvertently reveal your national origin and professional affiliation to anyone observing the network, even if the connection is encrypted. (TORPROJECT.ORG, 2016)

However, like any good tool, its use can be misrepresented, as it has in fact been and has been. It was precisely this inappropriate destination that made Dark Web famous in 2013, when Silk Road, a page that openly and unrestrictedly offered illicit drugs, was taken off the air by the Federal Bureau of Investigation (FBI) (ROHR, 2013). By the mixture of concepts and the confusion already mentioned, it was popularized under the name of the genre to which it belongs, that is, Deep Web.

Crimes of the most varied possible are associated with the use of Dark Web, such as the trade of personal data, sales of secret documents of governments, various tutorials (homemade bombs, homemade poisons, etc.), false documents, rent killers, torture, snuff movies (movies that register real people's murderers), trafficking of people, guns and drugs, terrorism, human organ trafficking, pedophilia, cannibalism, dolls makers (transformation of people, especially children and women, in sex slaves after amputating members and transforming them into "living dolls"), money laundering, among others that have their practice linked to the Internet not indexed, anonymous and encrypted (DEEP WEB: O SUBMUNDO..., 2015). The anonymity and difficulty of seeing the materiality and authorship prevent the absolute proof that everything that is touted as being practiced via this channel of communication is in fact real, but cases like the one of Silk Road show that crimes of the most varied can be practiced quite easily, in the sly and with impunity - for the most part.

The fundamental difference between Dark Web and the Internet of everyday life is its functioning: while it has plenty of connection records, a known data flow route, plain text information and the possibility of associating IP addresses with activities carried out online, that is not the case. The use of the TOR, for example, changes the dynamics of the connection in such a way that it damages the connection registers, the data flow path becomes uncertain, the information exchanged becomes encrypted and, consequently, the association of IP addresses with activities performed remains undermined.

Clearly the scope of this article is not to go into the technical details of the tools used in Dark Web, but only to present them to help understand how new technologies can impact the practice of money laundering. Therefore, definitions and detailing of systems could not, and

[10] Accessible at https://facebookcorewwwi.onion.

are not, extenuating, especially since there is no interest from those involved in the illicit use of such technologies in publicly disclosing all the tools that make the obscure part of Internet communication a comfortable place for criminals. Information about the TOR is only publicly accessible because it is intended for a noble purpose, as discussed above. Mentioned the caveat, this is how this protocol works.

As stated on its official website, TOR works by hiding from everyone - internet providers, enforcement authorities, law enforcement officers, companies, malicious third-parties (hackers), etc. - the route of the data sent, so that it will no longer be possible to identify its origin and destination. To achieve this goal, TOR creates a twisted and difficult route to follow, then deletes its tracks. It works as follows: (i) the user's computer connects securely (encrypted) to the TOR server and downloads the list of currently available connection points - each connection point represents a computer similar to it within the TOR network; (ii) the TOR client on the user's computer then creates a route to reach its destination through those peers, which act as small servers, receiving and supplying information; (iii) the connection is established peer-to-peer, with each machine only knowing where the data came from and what is the next machine to which the data will go, and no information about the complete route is transferred; (iv) reached the destination, that is, the server that the user intended to reach - a page, a data storage service, an e-mail server - the created connection is maintained for a maximum of 10 minutes, after which route is created, again without any record (TORPROJECT.ORG, 2016).

Each of these peers can be located anywhere on the globe. So, for example, a computer located in Brazil connects to one in China, which connects to one in Switzerland, which connects to one in Bolivia, which connects to one in Greece, which connects to one in Guatemala which, only then, it reaches the destination initially intended by the user TOR. Hence, the analogy to onion: just like one, the onion network has several successive layers of security, anonymity and encryption.

By operating in this way, the TOR ensures the privacy of the route and the codification of the data transported, so that not only the origin remains hidden, but also the content of the information transferred. The degree of anonymity of the activities performed, however, depends on the sophistication of the applications that communicate through the TOR network and the skill of its users.

Although unprecedented on the Surface Web, the anonymity and data security possible in the Dark Web environment allows servers with illicit content to be mounted on notebooks or easy-to-carry computers stored in the backyard of a common residence. Such freedom does not exist on the indexed Internet, which allows in a reasonably easy way the identification of content made available on the site, its ownership and location.

While on the Web the identity of the computer that accesses the Internet, the path and destination of the data are easily observable, in Dark Web this information is practically impossible to obtain or is extracted with great difficulty, cost, technical apparatus and professionals with vast technical knowledge - and submitted to constant updates of knowledge.

3 BITCOIN: THE CRIPTOCURRENCY OF THE DARK WEB

In a world where anonymity rules, the lack of accountability is common. In this context, Dark Web is a hostile environment in which each is by itself and caution is the greatest rule of survival. Sitters comfortably seated on their sofas, hidden by layers, and more layers of security and privacy, patiently wait for innocent users to provide their personal data and credit card numbers to be fraudulent by themselves, or to sell that information to others. For this reason, the currencies used in the Dark Web are not conventional, but virtual.

Bitcoin (BTC and XBT - official abbreviation) is the most popular and widespread cryptocurrency in the world, so for this reason it is the official currency of Dark Web. It is not the only one, however. There are others such as Litecoin (LTC or Ł), Peercoin (PPC), Feathercoin (FTC), Terracoin (TRC), Freicon (FRC), PhenixCoin (PXC) and AnonCoin (ANC) (SOUZA, 2013), but Bitcoin remains the strongest among them and has gained more and more fans around the world (BRAGA; MARTINS, 2014). Each Bitcoin is quoted today at R$5,093.03 (five thousand, ninety-three reais and three cents)[11].

Bitcoin has as its characteristic a fiduciary currency[12] (it does not have metal ballast - gold or silver -, nor intrinsic value) and decentralized – do not depend on intermediaries or central institution –, and depend on the trust that its users deposit in them (KIVIAT, 2015). Therefore, it has a value proportional to the credibility attributed to it, the fees involved in the transactions are low (inviting to use), have no limits of territorial use, cannot be frozen or confiscated and have no prerequisites for use or limits imposed per transaction (any amount may be transferred to any person, by any person, to any person, without prior authorization or further justification) (BITCOIN.COM, 2016).

Bitcoins are stored in digital is done in digital wallets, that are accessible through any device that can operate with the technology (computers, tablets, smartphones, etc.). The payments are done digitally, without intermediaries. The authenticity of the transction, however, is verifies by Bitcoin miners, that receive a payment in Bitcoins generated autoamatically to pay for their services. Once audited and verified the authenticity of the transaction by them, it is registered in a virtual ledger, public and transparent (BITCOIN.ORG, 2016), debiting the payer and crediting the payee. The act of recording the transactions, however, does not mean that they are fiscalized in any manner. This auditing exists with the sole purpose of validating the transfer, in what concerns to the transfer of the amount from one party to another, so that there are no fraudulent payments, not identifying any of the parties.

In essence, Bitcoin does not actually exists, but is presumed to exist. In the ledger, called blockchain, the balances of the accounts of each user are logged, which are identified by a unique cryptographic code, as well as the record of the transactions performed (each one generates a transaction hash, which identifies it among the others). Each time a payment is made, payer and payee sign the transaction using their private key, which verifies the identities of the parties involved accurately, allowing the account linked to the key of the debtor to be debited from the amount paid and the balance of the creditor linked to the informed key is increased by the transaction value. Once the transfer is done and propagated in the network, the other users and the miners start to validate it, in a process that usually starts about 10 minutes later (NAKAMOTO, 2016).

Although all transactions are recorded in a pubic record, the identity of buyers and sellers is never revealed, and only the identification of their wallets is visible. You can remain completely anonymous if you do not associate your true identity with your wallet. Hence the anonymity associated with Bitcoin, in line with the 1993 cypherpunk manifesto, which assumes that virtual transactions should be as private as cash transactions in which parties do not need to identify themselves or expose their motives (HUGHES, 1993).

The anonymity guaranteed by the use of Bitcoin is so much, that in during the time the present work, hackers infected thousands of computers in dozens of coutnries (in a number somewhere in between 74 to 99 countries), including Brazil, United Kingdom, USA, China, Russia, Spain and Italy, encrypting computer files and explicity demanding a payment of a

[11] Quotation between XBT (BitCoin) and BRL (Brazilian Real) obtained on 05/12/2017 at http://www.xe.com.
[12] Also known as fiat currency.

ransom in Bitcoins equivalent to US$600 to restore the access the files, in a practice that is now called ransomware (BBC.COM; G1.COM, 2017).

The conversion of Bitcoin into traditional currency can be done in exchange offices spread around the world or made directly with a seller. Since there is no regulation nor requirements, it can be made in cash and in an untraceable way.

4 IMPACT OF DARK WEB AND BITCOIN IN MONEY LAUNDERING PROCESS

Over the years, the Brazilian legislature has been reforming the text of Law 9.613 / 98 on the typical figure of the crime of money laundering, with a criminal policy that signals a clear and forceful criminal response to this phenomenon of transnational proportions, in particular, in order to comply with the commitments signed in international texts (INIESTA, 1996).

After more than a decade since the entry into force of Law 9,613/98, the Brazilian legislature has undertaken yet another reform in its text, however, this time, in a more meaningful way and that approximates the international norms that deal with the matter. Law no. 12,683/12 brings as one of its main modifications to the text of Law 9.613/98 the withdrawal of the exhaustive list of previous crimes, which from these, generate economic benefits and which are now subject to the washing process (BRAGA, 2013).

The Brazilian legislator established the main delict in art. 1º, which refers to the conduct that is indispensable for the typical nature of the crime of money laundering, to "conceal or conceal" the nature (permanent crime) of origin (origin, ie the process by which the property was achieved), location current situation or place where it is located, where the object is located, the good), disposition (onerous or gratuitous), movement (the direction of financial movement, circulation of values and goods) or property (ownership, mastery over the thing, the quality of the owner, the use, enjoyment and disposition of goods), rights and values arising, directly or indirectly, from a criminal offense.

The subject of money laundering is current and its use for criminal activities is imperative, in this way, both Dark Web and Bitcoin prove to be extremely suitable tools for its facilitation. They are two revolutionary technologies that open the Pandora's box of the money laundering process. If Bitcoin itself makes it extremely difficult to trace origin, when it is well used in the Dark Web environment, anonymity is absolute.

Combating the money laundering crime carried out through cryptocurrencies such as Bitcoin, would force the creation of enforcement and control mechanisms, but the existence of such mechanisms of regulation runs head-on with the motives and purposes of cryptocurrencies, whose structure ensures the anonymity. The only possible oversight of Bitcoins appears to be that of validating the legitimacy of transactions, without which their very existence would be threatened. Other than that, there is not – at least not of public knowledge. Thus, even if there were regulations, how could it be made efficient against a currency that is easy and fast to circulate around the globe, created in an ideology that is contrary to state control (MAY, 1992) and is anonymous? Is it worth it to predict harsh penalties if they can not be applied, especially within the obscure environment of Dark Web? Hardly, at least with the tools available today. In an optimistic scenario, goodwill people, the ordinary citizen, would yield to the dictates of regulatory legislation, but if the citizen is "good" he or she is not the one who practices the crime of money laundering. True criminals would remain undetected.

And "undetected" is, in fact, the correct expression, because there are many cases of money laundering of large size, but that simply are not detected. One of the most emblematic cases of this kind of secrecy is the "Cannibal of Rotenburg[13]", which only came to light and became public because it was taken to the authorities. However, they would never have discovered the crime if Meiwes himself – after performing his fantasies – had not returned to the chat channel and commented that he needed more meat after consuming the flesh of the victim of his cannibalism. The authorities were only aware of the fact because of the denunciation of another user, meaning that the crime was only discovered because the social environment in which the criminal was inserted did not respond in unison to the mentality behind the crime committed, and someone informed the police about the possible evidence that one was committing a crime. But would it have the same outcome if it had happened in a place that fully absorbed the idea behind illicit conduct, as in a specific thematic forum within the Dark Web where anonymity is assured? The feared truth is that you only fight what is known to exist.

What is certain is that there is still no abundant, effective or direct regulation that allows the prevention, detection and combat of money laundering through Dark Web or through the use of cryptocurrencies. Far from it. There is today what may be considered to be a draft legislation, still incipient, only in some developed countries, in some operations and in cases where these are declared (usually by official exchange houses). Regulation, fiscalization and control of cryptocurrency is something that may still be non-existent when compared to the official currencies. And it should be remembered that Bitcoin is just one of many existing cryptocurrencies, and of those still to exist. There are already others of this kind in development, that promises, for example, absolute anonymity and encrypted blockchains (and no more transparent like those from Bitcoins) such as StealthCoin[14] and Vertcoin[15], designed to openly prevent state regulation, in line with "A Cypherpunk's Manifesto" and "The Crypto Anarchist Manifesto".

Epecifically regarding money laundering through Bitcoins, the laundering process can be done by the use of cryptoopcurrency in its original form (virtual/digital, through direct transfer), or by the undetectable transference of amounts arising from illegal acts from one country to another through digital means - for further conversion into local official currency or in foreign currency (which can be done, for example, by conversion with payment in cash, between individuals or through a fake business). The absence of regulation is definitely a driving force behind this system, but even if regulation was there, it is not known how effective it could be, due to the nature of the tools used.

In this context, the struggle for the adoption of virtual currencies in the daily lives of ordinary people around the globe intensifies every day and aggravates the scenario. More and more people are attracted to the virtual world of Bitcoin to facilitate international transfers of values - now complex, expensive and slow if made with official currencies and through central banks - and to avoid bank charges. More and more ordinary people have embraced the use of cryptocurrencies, and many commercial establishments have been receptive to the idea of using them. If, on the one hand, this gives the tax layers a relief, in the sense that the transactions carried out in Bitcoins may be taxed, even indirectly, as income, for example, on the other hand, arouse criminal layers, since it will continue to be impossible impossible to trace the payers, the origin and nationality of the amounts transfered in the transactions.

The acceptance of cryptocurrencies in the daily life can be a nightmare for authorities and countries, because it will become increasingly easy to use the values virtually accumulated by criminals, without the need for conversion into official currency of any country - which

[13] Armin Meiwes, "The Cannibal of Rotenburg", is a German who became internationally known for eating, after killing, a voluntary victim with whom he had arranged the meeting via the Internet. After finishing consuming the corpse, he placed another ad on the Internet, was denounced by an Internet user and later arrested (Wikipedia).

[14] Available at https://www.stealth-coin.com.

[15] Available at https://vertcoin.org.

today is it is still the weakest link in such a scheme. Virtual currencies are as good as their purchasing power - after all, a currency is nothing more than an instrument of exchange and concentration of wealth. For all intents and purposes, Bitcoin is today a form of money, such as the Dollar, the Real or the Euro (SILVA, 2014), even though it still has its use almost totally limited to the virtual world. If, however, amounts derived from ilegal practices can be spent directly on virtual currencies, once the amounts are converted to their equivalent in cryptocurrencies, it will be virtually impossible to prove the practice of money laundering and impunity will remain assured.

Even if there is an attempt to regulate, due to the characteristics of the cryptocurrencies, it will only be effective to the extent that it is able to efficiently discipline the conversion of virtual currencies into traditional currencies. The problem is that the virtual currency knows no boundaries, but the jurisdiction of each country, yes. Achieving a level of international cooperation that ensured an effective regulation of cryptocurrencies in a short-term would require a surreal effort and optimism, given the peculiarities, goals, and priorities of each nation. And the achievement of such long-term cooperation - which is the most realistic scenario - can be ineffective, since there is a real possibility that until then, virtual currencies gain autonomy and independence, leaving the world totally virtual and integrating the day-to-day life of people – mainly because the technology needed for their daily use already exists: the smartphones that everyone carries in their pockets.

Of course, we can not speculate about the future of the economy and the possible use of cryptocurrencies in people's daily lives, but it is a possible scenario and would certainly impact the way money laundering would be practiced. The city council of Zug, Switzerland, for example, even though experimentally, has been receiving fees from some public services in Bitcoin since July 2016 (NEGHAIWI, 2016; BBC.COM, 2016). And before that, in 2013, the SIX Interbank Clearing, which operates on behalf of the Swiss National Bank and composes several international payment standardization committees, endorsed the use of the International Standards Organization (ISO) code for Bitcoin, the XTB, an acronym for which is now officially known in the foreign exchange markets (MATONIS, 2013). Microsoft today receives payment for its services through Bitcoin (MICROSOFT.COM, 2017). As Silva argues, "surely, we are witnessing the initial steps of a globalized currency, free, transparent and open-source[16]" (SILVA, 2014). The technologies have evolved faster than the law has been able to follow, and therefore it is necessary that the legal sciences awaken to this reality and become more dynamic and able to keep up with the pace of the changes.

The same is true of the Dark Web environment, which is a environment that amplifies and fosters the misuse of cryptocurrency: the more users adhere to its use, the more difficult it becomes the harder it is to use any kind of monitoring tools that has already been developed or that is yet to be invented. This is because of the fact that the increase in the number of users also increases the volume of encrypted information to be searched, as well as allows the creation of larger, more fragmented and more complex routes used by softwares such as TOR.

And cryptography activists against state control do not want to stop. On the contrary, they openly declare their goals, as Jacob Appelbaum, cypherpunk belonging to the core of the TOR network anonymity project, stated in the documentary Deep Web (2015)[17]

> Force of authority is derived from violence. One must acknowledge that, with cryptography, no amount of violence will ever solve a math problem. This is the important key. It does not mean that you can not be tortured. It does not mean they can not try to bug your house or try to subvert you in some way, but it means that if they find

[16] Free code, open to public development.
[17] Available on Netflix.com.

> an encrypted message, it does not matter if they have the force of the authority behind. Everything that they do, they can not solve that math problem. (WINTER, 2015)

If access data exchanged for mere everyday messaging applications has proved to be a Herculean task for the national judiciary, as was recently seen in the case that cause the blockage of the WhatsApp messaging application throughout Brazil by force of a Court order (MIGALHAS, 2017), an environment completely encrypted, then, represents a new paradigm still to be understood and unveiled.

However, the impact of these technologies on the money laundering crime does not end with these issues. Protected by anonymity, the creativity of criminals takes forms never thought of in the physical, real and palpable world. In addition to the traditional ways of money laundering and the possibility of anonymous use of value in the virtual world, there is also a Bitcoins laundy, available for those who want to hire – offered in the same way that drugs are offered on pages like Silk Road. With the Bitcoins laundry, the transference of any figure in this cryptocurrency can not even be traced inside the blockchains. The amount to be trasnfered is fragmented smaller values, divided irregularly, which are transferred several times between different people so that, in the end, they reach the destination by summing the transfers – as does the EasyCoin page in the Dark Web, which auto entitled “Bitcoin Mixer/Laundry” (CIANCAGLINI et al, 2015).

5 FINAL CONSIDERATIONS

The absence of privacy in modern society raises, in fact, real concerns. We live no longer under the constant monitoring of surveillance cameras almost everywhere, but we also have our intimate life exposed. Our data is no longer ours, our lives - today largely embedded in the digital world - and our habits are continually tracked and cataloged by companies and governments. How much we earn, where we go, who we talk to, what we buy, everything is recorded and transforms into metadata or even in a personal profile record. Everything seems to be valid in the name of profit and national security.

In this seemingly hostile scenario, pro-privacy activists organize and declare war against the control, which they do not consider legitimate. The mechanisms used on this war are only meant to guarantee your privacy and the privacy of so many more who want your protection. They have created secure communication protocols, systems that prevents tracking efficiently, and untraceable cryptocurrencies that now transcend the boundaries of the virtual world and enters the world of ordinary people. We live in an age that even twentieth-century science fiction could not predict.

Using the required expertise, it is possible for a malicious person within Dark Web to provide, access and exchange information without its identification or location. Hundreds of thousands of dollars circulate in Bitcoins around the world every hour without the knowledge of any government. The control that was previously made physically in airport boarding areas in search of money in kind, which later came to be realized within the computer systems of central banks, nowadays does not exist in the universe of virtual encrypted currencies, such as Bitcoin. Current laws show signs of weariness in its fight against money laundering and in favor of the modern Democratic State.

Changes are needed, but not just in the laws, as some boast. It is necessary to change the way of thinking, to foresee the future and to ensure compliance with laws without suffocating the citizen of goodwill, who is generally who docilely absorbs the imposed regulations. A new social reality is in the planning stage and the operators of the law need to awaken to this construction, dealing not only with the already clarified issues but also with the unknowns of a world that, even in its most elementary form, seems to be a mystery to most ordinary people: the digital world, which increasingly ceases to be virtual and takes shape in people's daily lives.

In this process, the traditional dogmatic needs to be replaced by transdisciplinary dialogue. The law must realize that this reality can only be overcome with the technical support of other areas of knowledge. After all, if the Law deals with the "must be", it is necessary before we constantly understand what the "being" represents today, otherwise it will become obsolete and outdated in some cases.

REFERENCES

BARRET, Brian. Most Top Websites Still Do not Use the Basic Security Feature. **Wired**, 17 Mar. 2016. Available at: <https://www.wired.com/2016/03/https-adoption-google-report/.> Accessed on: 12 Dec. 2016.

BBC.COM. **Swiss Council to accept Bitcoin payments**. 10 mai. 2016. Available at: <http://www.bbc.com/news/blogs-news-from-elsewhere-36257465.> Accessed on: 15 Dec. 2016.

______. **O que se sabe até agora do 'sequestro' de computadores em grandes empresas ao redor do mundo**. 12 mai. 2017. Available at: <http://www.bbc.com/portuguese/geral-39903918.> Accessed on: 17 May 2017.

BITCOIN.COM. **What is Bitc oin?** Available at: <https://www.bitcoin.com.> Accessed on: 13 Dec. 2016.

BITCOIN.ORG. **How does Bitcoin work?** Available at: <https://bitcoin.org/en/how-it-works.> Accessed on: 13 Dec. 2016.

BRAGA, Romulo Rhemo Palitot, **Lavagem de dinheiro: fenomenologia, Bem Jurídico Protegido e Aspectos Penais Relevante**. Curitiba: Juruá, 2013.

BRAGA, Romulo Rhemo Palitot; MARTINS, Fabiano Emídio de Lucena. Blanqueo de capitales y el tráfico de drogas en la deep web: el avance de la delincuencia virtual. In: Caty Vidales Rodrigues. (Org.). **Trafico de Drogas y Delincuencia Conexa**. 1st ed. Valencia: Tirant lo Blanch, 2014, v. 01, p. 405-424.

BRANDON, John. Why Email Will Be Obsolete by 2020. **Inc.com**, 16 Apr. 2015. Available at: <http://www.inc.com/john-brandon/why-email-will-be-obsolete-by-2020.html.> Accessed on: 12 Jan. 2017.

CCM BENCHMARK GROUP. **História da Internet**. Available at: <http://ccm.net/contents/231-historia-da-internet.> Accessed on 14 Dec. 2016.

CIANCAGLINI, Vincenzo et al. **Below the Surface**: Exploring the Deep Web. 2015. Available at: <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf.> Accessed on: 03 Dec. 2016.

CRESPO, Marcelo. Deep Web: o submundo do crime. **Jusbrasil,** 2015. Available at: <https://canalcienciascriminais.jusbrasil.com.br/noticias/211380741/deep-web-o-submundo-do-crime.> Accessed on: 06 Dec. 2016.

G1.COM. **Ciberataques em larga escala atingem empresas no mundo e afetam Brasil**. 12 mai. 2017. Available at: <http://g1.globo.com/tecnologia/noticia/hospitais-publicos-na-inglaterra-sao-alvo-cyber-ataques-em-larga-escala.ghtml.> Accessed on: 12 May. 2017.

GOOGLE.COM. Como exibir seus anúncios acima dos resultados da pesquisa do Google. **Google Ads Help**. Available at: <https://support.google.com/adwords/answer/1722087?hl=en.> Accessed on: 04 Dec. 2016.

______. HTTPS nos principais sites. **Google Ads Help.** Available at: <https://www.google.com/transparencyreport/https/grid/.> Accessed on: 06 Dec. 2016.

INIESTA, Diego J. Gómez, **El Delito de Blanqueo de Capitales en el Derecho Español**, Barcelona: Cedecs, 1996.

HUGHES, Eric. A Cypherpunk's Manifesto. **Eletronic Frontier Fundation**, 1993. Available at: <https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto>. Accessed on: Dec. 13 2016.

KIVIAT, Trevor I. BEYOND BITCOIN: issues in regulating blockchain transactions. **Duke Law Journal.** p. 569-608, v. 65. 2015. Available at: <http://scholarship.law.duke.edu/dlj/vol65/iss3/4>. Accessed on: 01 Dec. 2016.

MARTINS, Fabiano Emídio de Lucena: **Lavagem de Dinheiro e Paraísos Fiscais: a Captura da Economia pelo Crime Organizado**. Lumen Juris: Rio de Janeiro. 2018.

MARTINS, Elaine. **O que é um backbone?** TechMundo, 10 Mar. 2009. Available at: <https://www.tecmundo.com.br/conexao/1713-oque-e-backbone-.htm>. Accessed on: 06 Dec. 2016.

MATONIS, Jon. Bitcoin gaining market-based legitimacy as the XBT. **CoinDesk**, 17 Sept. 2013. Available at: <http://www.coindesk.com/bitcoin-gaining-market-based-legitimacy-xbt/.> Accessed on: 15 Dec. 2016.

MAY, Timothy C. **The Crypto Anarchist Manifesto**. 1992. Available at: <http://www.activism.net/cypherpunk/crypto-anarchy.html.> Accessed on: 07 Dec. 2016.

MICROSOFT.COM. **Adicionar crédito a sua conta da Microsoft usando Bitcoins**. 12 May 2017. Available at: <https://support.microsoft.com/pt-br/help/13942/microsoft-account-add-money-with-bitcoin.> Acessed on: 12 May 2017

MIGALHAS. **Juiz que determinou bloqueio do WhatsApp diz que empresa zomba do Judiciário**. 17 set. 2013. Available at: <http://www.migalhas.com.br/s/17,MI240083,101048Juiz+que+determinou+bloqueio+do+WhatsApp+diz+que+empresa+zomba+do.> Acessed on: 12 mai. 2017.

MITCHELL, Bradley. What is an IP Address? **Lifewire**, Oct. 29. 2016. Available at: <https://www.lifewire.com/what-is-an-ip-address-818393>. Accessed on: 10 Dec. 2016.

NAKAMOTO, Satoshi. Bitcoin: **A Peer-to-Peer Electronic Cash System**. Available at: <https://bitcoin.org/bitcoin.pdf.> Accessed on: Dec. 14 2016.

NEGHAIWI, Brenna Hughes. Low tax Zug aims to become Switzerland's 'Crypto Valley'. **Reuters**, 08 Sep. 2016. Available at: <http://www.reuters.com/article/us-swiss-fintech-cryptovalley-idUSKCN11E0L9>. Accessed on: 15 Dec. 2016.

PC MAGAZINE. **Definition of: surface Web**. Available at: <http://www.pcmag.com/encyclopedia/term/52273/surface-web.> Accessed on: 12 dez. 2016.

ROHR, Altieres. FBI fecha Silk Road, site secreto para comércio de drogas ilícitas. **G1.com**, Oct 02 2013. Available at: <http://g1.globo.com/tecnologia/noticia/2013/10/fbi-fecha-silk-road-site-secreto-para-comercio-de-drogas-ilicitas.html>. Accessed on: 12 Dec. 2016.

SILVA, Douglas Emanuel da. **Aspectos de segurança na rede Bitcoin**. In: Coletânea Luso-Brasileira: Gestão da Informação, Cooperação em Redes e Competitividade. Francisco Alberto Severo de Almeida; Armando Barreto Malheiro da Silva, Mário José Batista Franco and Carla Conti de Freitas (organizers). Porto (Portugal): University of Porto, 2014, p. 221-249.

SOUZA, Ramon de. Além dos bitcoins: conheça outras moedas virtuais. **TechMundo**, Nov 05 2013. Available at: <https://www.tecmundo.com.br/bitcoin/46659-alem-dos-bitcoins-conheca-outras-moedas-virtuais.htm>. Accessed on: 11 Dec. 2016.

UNIVERSIDADE DO MINHO. Museu Virtual da Informática do Departamento de Sistemas de Informação. **Breve história da INTERNET**. Available at: <http://piano.dsi.uminho.pt/museuv/INTERNET.PDF.> Acesso em: 14 dez. 2016.

TAYLOR, McCartney. Deep Web vs. Surface Web. **Deep Web Search**. Available at: <http://deep-web.org/what-is-the-deep-web/deep-web-vs-surface-web/>. Accessed on: 13 Dec. 2016.

WINTER, Alex; SCHILLER, Marc; ZIPPER, **Glen. Deep Web**. [Movie-video]. Production of Alex Winter, Marc Schiller and Glen Zipper. Available on: <http://www.netflix.com.> Accessed on: 13 Dec. 2015.

YANDEX.COM. **What is a search engine robot**. Available at: <https://yandex.com/support/webmaster/robot-workings/robot.xml.> Accessed on: 07 dez. 2016.