REVISTA INTERNACIONAL
CONSINTER
DE DIREITO

DIREITO E JUSTIÇA
Aspectos Atuais e Problemáticos

REVISTA INTERNACIONAL CONSINTER DE DIREITO, ANO I, Nº I, 2º SEM. 2015

≋JURUÁ
EDITORIAL

Editor:
Luiz Augusto de Oliveira Junior

Diretores da Revista:
David Vallespín Pérez
Germán Barreiro González
Gonçalo S. de Melo Bandeira
María Yolanda Sánchez-Urán Azaña

COLABORADORES:

Adel El Tasse
Adriano Fábio Cordeiro da Silva
Alcides Goelzer de Araújo Vargas e Pinto
Aloísio Krohing
Ana Cláudia Corrêa Zuin Mattos do Amaral
Angela Cassia Costaldello
Angelina Isabel Valenzuela Rendón
Antonio Pele
Camila Clarisse Romero Gomes
Carlos Trujillo Hernandez
Celso Antonio Pacheco Fiorillo
Cinthia Obladen de Almendra Freitas
Danielle Portugal de Biazi
David Vallespín Pérez
Dirce Nazaré de Andrade Ferreira
Fabiane Grando
Fabiano Dolenc Del Masso
Fernando Gustavo Knoerr
Fernando Rister de Sousa Lima
Francisco Carlos Duarte
Gonçalo S. de Melo Bandeira
Gregorio Saravia
Greice Patrícia Fuller
Guilherme Augusto Souza Godoy
Idir Canzi
Iraci de Andrade
Irene Portela
Isa Filipa António
J. Eduardo López Ahumada
Jardel de Freitas Soares
Jessica Ramos da Silva

Jordi Garcia Viña
Jorge de Oliveira Vargas
José Adércio Leite Sampaio
Karin Kässmayer
Linara Oeiras Assunção
Mª Ángeles Pérez Marín
Maraluce Maria Custódio
Marcel Magalhães e Guerra
Marco Antonio Lima
Mateus Eduardo Siqueira Nunes Bertoncini
Nancy Carina Vernengo Pellejero
Nuria Belloso Martín
Paulo J. B. Faiad
Paulo Junior Trindade dos Santos
Paulo Ricardo Opuszka
Priscila Luciene Santos de Lima
Rafael Lima Torres
Rita Daniela Leite da Silva
Robert Carlon de Carvalho
Rodrigo Andrés Poyanco Bugueño
Rubén Miranda Gonçalves
Rui Miguel Zeferino Ferreira
Saulo Tarso Rodrigues
Sônia M. P. Wiedmann
Tarcísio Maciel Chaves de Mendonça
Valesca Raizer Borges Moschen
Vinícius Almada Mozetic
Vitor de Medeiros Marçal
Viviane Coêlho de Séllos-Knoerr
Zulmar Fachin

Integrantes do Conselho Editorial do

APRESENTAÇÃO

A **Revista Internacional CONSINTER de Direito** é uma publicação de cariz periódico do **CONSINTER – Conselho Internacional de Estudos Contemporâneos em Pós-Graduação** que tem por objectivo constituir-se num espaço exigente para a divulgação da produção científica de qualidade, inovadora e com profundidade, características que consideramos essenciais para o bom desenvolvimento da ciência jurídica no âmbito internacional.

Outra característica dos trabalhos seleccionados para a **Revista Internacional CONSINTER de Direito** é a multiplicidade de pontos de vista e temas através dos quais o Direito é analisado. Uma revista que se pretende internacional tem o dever de abrir horizontes para temas, abordagens e enfoques os mais diversos e, através deste espaço, colaborar com um melhor diálogo académico.

Resultado de um trabalho criterioso de selecção, este volume que agora se apresenta destina-se a todos aqueles que pretendem pensar o Direito, ir além da sua aplicação quotidiana, mas sem deixar de lado o aspecto prático, tão característico das ciências.

THE DRUG TRAFFICKING INSERTED IN CYBER SPACE – HOW SOCIAL NETWORKS, VIRTUAL CURRENCIES, BIG DATA AND SOFTWARE APPLICATIONS INFLUENCE IT – AN ANALYSIS OF THE UNITED NATIONS ORGANIZATION MEMBERS

Guilherme Augusto Souza Godoy[1]
Jardel de Freitas Soares[2]

Resumo: Com o avanço da tecnologia, as gerações y e z estão cada vez mais cedo envolvidas no mundo virtual, onde há ótimas informações a serem extraídas quando sabe-se os caminhos certos para buscá-las, no entanto, a criminalidade está dissipando-se na mesma velocidade do avanço tecnológico.

A UNODC[3] age em cooperação com o Grupo Pompidou – Grupo de Cooperação para Combater o Abuso e o Tráfico Ilícito de Drogas do Conselho da Europa. O programa de trabalho 2015/2018 inclui a identificação de oportunidades e desafios para as políticas de drogas provenientes da internet.

A legislação penal de diversos países vem alterando-se a fim de tipificar especificamente os *cybercrimes*, ou tais atos são penalizados por analogia.

Palavras-chave: Cybercrime. Narcotráfico. Big Data.

Abstract: With the advancement of technology, generations Y and Z are increasingly involved early in the virtual world, where there is great information

---

[1]   Doutorando e Mestrando em Criminologia pela Escola de Criminologia da Faculdade de Direito da Universidade do Porto – Portugal, Pós-Graduado em Direito Penal e Processual Penal pela Universidade Federal do Mato Grosso, Pós-Graduado em Direito Público pelo Instituto Cuiabano de Educação, Graduado em Direito pela Universidade de Cuiabá. (g.a.s.godoy@gmail.com – <http://goo.gl/xJoagy>)

[2]   Doutor em Ciências Jurídicas e Sociais, Universidad Del Museo Social Argentino (UMSA), Buenos Aires-Argentina. Professor de Direito Penal e Direito Processual Penal, Universidade Federal de Campina Grande (UFCG), Paraíba-Brasil.

[3]   United Nations Office on Drugs and Crime.

to be extracted when the right way is known to pick them up, however, crime is dissipating as fast technological advancement.

The UNODC acts in cooperation with the Pompidou Group – Cooperation Group to Combat Drug Abuse and Illicit Trafficking of Council of Europe. The work program 2015/2018, includes the identification of opportunities and challenges for drug policy from the internet.

The criminal law of many countries is changing the order to specifically criminalize the cybercrimes, or such acts are penalized by analogy

Keywords: Cybercrime. Drug trafficking. Big Data.

INTRODUCTION

> *Cyber crime, in a general sense, is an act that covers the entire range of crimes which involves computer, computer network, cell phones, etc., either as its target or as an instrumentality or associate. Thus any kind of criminal activity that takes place with the help of or against such electronic equipments and in the cyber space, comes under the purview of the word cyber crimes. Like other criminal activities, the motive or intention to cause an injury is one of the ingredient and the same is not limited to any specific type. The criminal conduct in the cyber world begins from the activity of stealing computer hardware and ends to the extent of transferring, altering or damaging, the computer data to cause harms to Net users*. (SINGH, 2007)

The black market of drugs has been setting up through anonymous systems that allow access to sites without IP[4] identification. For anonymous purchase uses up the crypto currency or virtual currency. It is the usual system that allows anonymous access, called TOR (The Onion Router), through it has been accessed the site "Silk Road" known as "Ebay of drugs" or "Amazon to drugs" where, with virtual currencies, usually called Bitcoin, it can buy numerous illegal products, including illicit drugs.

The internet is currently divided into "Surface Web" and "Deep Web", the Surface is where social networks are in addition to any websites that can be accessed freely by the general public. The "Deep Web" are anonymous services, through which allows transaction of illicit products. It would be the "Deep Web" the new path to drug trafficking? The Internet has come since its appearance greatly facilitating people's lives is the great tool that transmits information and allowed a development of globalized society. However, unfortunately, this facilitation does not limit access only on moral, ethical and legal activities. Internet access covers a broad and expanded space to distribute information from various fields for global access.

---

[4] Internet Protocol.

Several illustrations show the "Surface Web" as the tip of the iceberg, as other ships and fish swimming in shallow seas, while the "Deep Web" is located in the depths of the oceans in little explored areas, where few have Access.

> *The Deep Web refers to content hidden behind HTML forms. In order to get to such content, a user has to perform a form submission with valid input values. The name Deep Web arises from the fact that such content was thought to be beyond the reach of search engines. The Deep Web is also believed to be the biggest source of structured data on the Web and hence accessing its contents has been a long standing challenge in the data management community.* (MADHAVAN, 2009)

> *Although many have not heard about the 'Dark Net' or 'Deep Web', James Martin has been actively researching this new cyber-frontier, producing to my knowledge the first and only criminological and sociological analysis of the traffic of illegal drugs through what Martin has creatively coined an online 'cryptomarket'.* (ADORJAN, 2015)

Below we can understand through an illustration, the ratio of drug sales (and other illicit products) in anonymous black market (Silk Road) using virtual currencies whose users are also anonymous (Bitcoin).
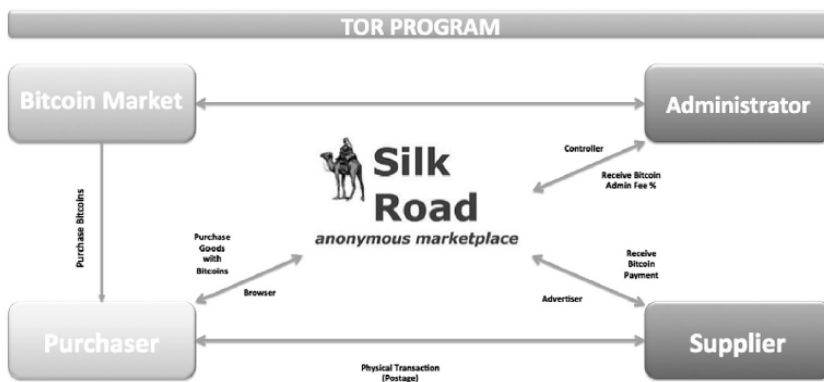
(PHELPS and WATT, 2014)

Products sold in the above mentioned site can be identified in the following table:

Top 20 categories of items available worldwide on Silk Road.[a]

Category	#. Items	Pct.
Weed	3338	13.7%
Drugs	2207	9.0%
Prescription	1784	7.3%
Benzos	1193	4.9%
Books	955	3.9%
Cannabis	880	3.6%
Hash	821	3.4%
Cocaine	633	2.6%
Pills	473	1.9%
Blotter	441	1.8%
Money	406	1.7%
MDMA (ecstasy)	393	1.6%
Erotica	385	1.6%
Steroids, PEDs	376	1.5%
Seeds	375	1.5%
Heroin	370	1.5%
Opioids	344	1.4%
DMT	343	1.4%
Stimulants	292	1.2%
Digital goods	261	1.1%

[a] This table is being displayed with the permission of its author, Nicolas Christin.

(PHELPS and WATT, 2014)

The next illustration we can understand the way that, strategically, if anonymous access sites that allow the black market in illicit products anonymously through the TOR System:
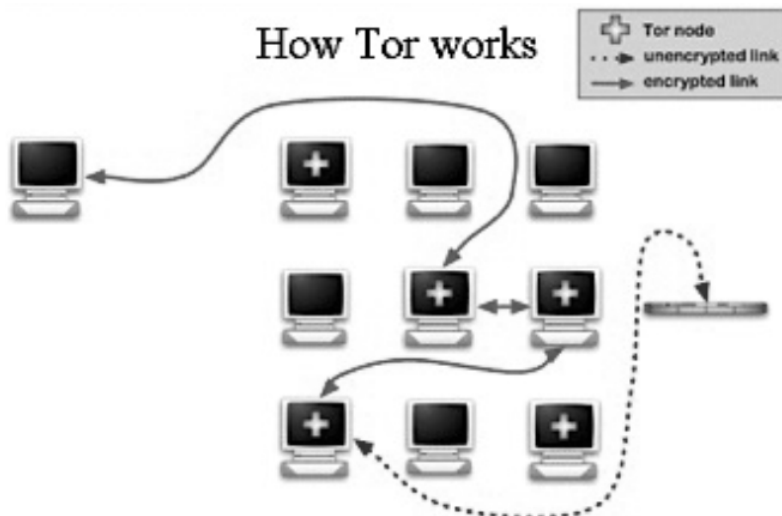
(BLOMM, 2013)

> Having a responsible Tor (without criminals) would put big internet companies face their responsibilities ie ensuring that their users have responsible anonymity when using their applications (protect the users of their networks as long as those ones remain within the limits of legality).
>
> On the other hand, the current Tor (with criminals) will always be an excuse for governments and big Internet compagnies to refuse to participate in the fight against mass surveillance. But beyond these pretexts what would we do if our child was kidnapped by a pedophile using Tor? would we be willing to help Tor after that? would we try to break the anonymity of the offender?
>
> In addition, can we oblige someone who is trying to help cyber dissidents to also help pedophiles, drug traffickers and the NSA while it is against its philosophy? (KANE, 2015)

METHODOLOGY

According to the literature "*a number of researchers have developed efficient methods for qualitative analysis of different types of materials. The character of some of these methods is suggested by their names*" (STRAUSS, 1994).

Such methods can be called: "*conversation analysis, network analysis (qualitative), biographical analysis, sociolinguistic analysis Dramaturgic analysis or social tragedy, textual analysis*" (STRAUSS, 1994).

The methods or combinations of techniques "developed in conjunction with certain lines of research and theoretical interests or commitments" (STRAUSS, 1994).

The method used in this work was the textual analysis typified by Strauss. Let's look at the development of documentary analysis, according to Lüdke; André (1986) suggest that the methodology of content analysis, "*a category of explicit procedures of textual analysis for social research purposes*" (BAUER, 2002). The content analysis "*is a technique to produce inferences of a focal text for your social context objectified way*" (BAUER, 2002), in which a text is studied in view of its inclusion in a broader social context. Textual materials are worked systematically, trying to keep the analysis is mistaken for a random subjective interpretation.

It has been analyzed a compendium of specific scientific papers on topics covered here, making up extraction of essential topics that complement a structured way the topics covered. It added up own ideas for a study to be developed empirically in order to substantiate the development of the theme. Articles cited used, mostly empirical methods, with users of the surveyed services.

Official sites checked were accessed through the papers to certify the data presented concerning the Deep Web and anonymous access with illicit purposes that fuel the black market of drugs marketed with virtual currencies.

For the criminal profile analysis committing crimes under the here discussed topic, which is scheduled to be developed in a deeper aspect, it used classical literature of criminology to present theories that initially characterized the criminal profile of the time, namely, the base trace to check the characteristics of offenders.

THE LIST OF SOFTWARE APPLICATIONS THAT COMBINE DRUG USERS TO THE BLACK MARKET OF THE SUBSTANCE

Software Applications such as "High there" in the United States, known as the "tinder marijuana" and "Who is happy" in Brazil, known as "Foursquare marijuana", which are known as such because of *tinder* be an software application where known people close to the user, with flirting purposes, "high there" is similar, the difference is that adherents identify on your profile that are marijuana users, conveniently to find other people who use it, who has more affinity. But the "Who is Happy" is known as *Foursquare*, for this treat is a location software application of close people, on a map, but in the case that, identifies people who are using marijuana nearby, using a similar platform.

With this facility to install software applications and be able to identify people and groups of friends, drug users, combined with big data, ie the data tracking of users, which will be explained in the next section, it becomes vulnerable to malicious hackers, seeking to attract people to the black market in drugs contained in cyberspace.

THE USE OF BIG DATA OF SOCIAL NETWORKS TO FILTER CLIENTS ON THE BLACK MARKET

Now the leading social network used is called Facebook, it's a privacy policy that "through cookies" with information of this use given to users, but that goes unnoticed, uses big data to track access favoring the promotion marketing. Similar methods are used in Google adsense, which tracks the sites accessed by Internet users in order to disseminate advertisements for products and services that more users are interested.

Such information can be extracted and manipulated by anyone who wants to promote a page or make a marketing through Facebook, using private services that the site offers.

As in the case of mobile software applications, explained in the previous section, an individual with malicious intent, can request this data and use them directed to the black market.

> *Facebook continues manipulating what you see in your timeline. This is defined by an algorithm called EdgeRank, was created by own face and originally followed three criteria: affinity (how you interact with the author of that post), engagement (number of likes, comments and shares that the post had) and time (old news has no time). Today, the algorithm is much more complex – according to Facebook, estimates more than 100,000 variables, adjusted according to each user. The company does not say what, even by a trade secret – otherwise, the algorithm could be copied by other social networks. But some say that secrecy is also a way to tamper with the contents distributed to users to capitalize on that. "Facebook is on the border of ethically questionable. Sometimes it is ethical, sometimes it's unethical. He gives you benefits, but charges for it", says Raquel Recuero, communications professor at the Catholic University of Pelotas and researcher of social networks.*
> *It is common to see users of Facebook wary of company policies, or fearful that she has too much information.*
> *Facebook knows where I've been on the internet. You know when you enter a site, anyone, he has a little button that allows us to like something? This button is a convenience to you, and a monitoring mechanism for Facebook: when you enter that page, he learns (even if you do not hit the like button). This system serves to the Facebook show ads related to things you think of buying. If you enter a shop and looking for a refrigerator, for example, this*

information is passed to the Facebook – which now display refrigerators ads. The mechanism is present in much of the Internet, including sites that have nothing to do with e-commerce, and allows the serious face in his footsteps over the web, quiet and uninterrupted. He is not the only: Google also does something.

The system works thanks to cookies, small text files that are placed on your computer or cell phone and identify it as you browse the internet. In Europe, the law requires that the user has to approve each of the cookies deposited on your computer. But a report from the Privacy Commission of Belgium, released in March, concluded that Facebook is violating the law by planting cookies on people's computers without their permission. According to the report, it uses cookies to track users who are not logged on your network – and even people who never had a Facebook account.

The most strange is that I agreed to give all that access to Facebook. "By clicking Open an account, you agree to our Terms, including our use of Cookies". Hardly anyone reads: only 7% of users, according to a 2011 survey. In the case of Facebook, the official document has more than 23,000 characters, and pass 80,000 by adding the sub-items. Ie, it is very difficult to read. (SANTI, 2015)

THE ILLEGAL AND ANONYMOUS USE OF VIRTUAL CURRENCY / CURRENCIES CRYPTO

The best known virtual currency is the Bitcoin, to obtain it is not necessary to reveal the identity. For shopping in black markets, as a rule, the method of payment is with such coins. Providers set up for access to websites that sell illegal products do not reveal the IP number, which would be the only way to identify the individual who conducted the transaction, tracking your computer, since the transaction is completely anonymous through these coins. The best-known site, accessed through the system coded The Onion Router – TOR, is called "Silk Road".

"*Tor is a free software designed for online anonymity and resisting censorship*" (KANE, 2015)

The Bitcoin network was launched in 2009 by the mysterious Satoshi Nakamoto, a developer who worked extensively on the project but only interacted with people on developer forums. At the end of 2010, Nakamoto disappeared from view, announcing his departure and handing off the project to the open source community. No one knows his (or her) true identity, but what is known is Nakamoto's wealth. He is said to have roughly $100m worth of bitcoins by today's value, and hasn't spent any of it. (BRADBURY, 2013)

Including, recently, it was reported on a website called "Everything about everyone" (Tudo sobre todos), providing personal data through payment

made with Bitcoin. Such an act is not permitted by Brazilian law, where the site encompasses, in addition to allowing access to data to any malicious individuals, assuming that it facilitates the selection of people from clan to access black markets of illicit products, just as was explained in this paper, the extracted data in social networks and applications (NUNES, 2015).

THE SCOPE OF THE LEGISLATION TO WRONGFUL ACTS IN CYBERSPACE ANALOGOUS TO CRIMES ALREADY TYPED. THE CRIMINAL, LIKE THE WHITE COLLAR CRIME, IS NOT IDENTIFIED AND DENOUNCED AS A RULE? WHICH THE NEW CRIMINAL PROFILE THAT CREATES PLATFORMS FOR SELLING ILLEGAL PRODUCTS ON THE DEEP WEB?

Some crimes already typed, specific in certain cyber acts, however, some others again may be typified by analogy non-specific crimes, but which allow an analog interpretation.

This fact occurs due to the advance of new techniques and creative alternatives tend prepared in accordance with the technological advancement allows. The legislative process of any country would not reach such speed, regardless of the political system that follows.

"*With all marvels of Information Technology (IT), a reasonable apprehension about abuse of the technology has followed the rapid growth of net service*" (SINGH, 2007)

Cyber crimes under terrorism and sale of infringing products, or which are legal in their home country but illegal in countries covering the sale destination field (worldwide), cause a difficulty towards the penalty,

> *in order to find an effective solution of the problem, the enforcement of the cyber law should not be territorial but global. The representative of states or UNO should sit together and propose a internationally enforceable law. Such enactment is possible only through the cooperation and coordination at international level. Such law must have an extradition clause so that an offender committing crime in one country may be extradited to the country where prosecution have been launched against the offender. The ultimate aim of all combined efforts should be to control the cyber crimes based on globally accepted principles.* (SINGH, 2007)

The White Collar Crime covers numerous types of crime committed by criminals with a different profile of commonly featured in "Blue Collar Crime". In property crimes such as petty theft and shoplifting, commonly characterized the criminal, basically as poor, while in the White Collar Crimes, is characterized as rich, who commit embezzlement, tax evasion, among others. Because this context, those who commit white-collar crime is not, often identified /

denounced as acts intelligently in shares calculated and strategically, without a trace and without directly damaging the property of specific people, are crimes that reach people often do not realize they have been met or do not give much importance to the injury that had, perhaps not understanding that had such an injury.

> *White-collar offenders are on average older than offenders who commit conventional crimes; Usually they have stable jobs and have an education level higher than that of conventional crime offenders and similar to non-offenders; Usually they belong to the ethnic majority in your country; Mostly are male gender; They have social ties and religious superior to conventional and substantially similar to the criminals of people who commit no crimes.* (CRUZ, 2011)

In the case of offenders who commit crimes in cyberspace, crimes that fall under this work, similarly, hardly identify the criminal, because of anonymity, not computer IP identification. Need for such a state concern by police intelligence, waking up the interest in having technicians on staff, extremely experts in hacking methods at the same level or higher to those who commit such crimes. As for the economy class, as a rule, will not be very poor because they need to have access to their own computer to manipulate such acts, however need not be so rich, to achieve certain positions, as is the case of White Collar Crimes actors.

To trace the profile of who commits such acts is necessary to further empirical study, but with some observations and logic, one can anticipate that are anonymous, hackers, young, curious and ambitious.

Veerasamy (2010), who traces the profile is recruited to work with cyber-terrorism, being a person "young, middle-class and technologically competent". Framing or not such activities reported here, as cyber terrorism, it is believed that, superficially and generally, this is the profile of those who commit such unlawful acts.

> *We may say that there are many inherent factors that attract and facilitate their activities in the cyber space. Sometime for money and some other times for fun, but the criminals are bound to be attracted towards the cyber world. Cyber criminals have no dearth of motivation for committing crimes. The advantage of anonymity is the most advantageous among them. The motivational factors of cyber world are the similar to that of traditional world of crimes. They could be greed, lust, power, revenge, adventure and desire to taste the "forbidden fruit". Unlike perpetrator of a traditional crime, the greed of money or similar monetary lust may not always be a factor of motivation. The motive in the cyber world may be malice, mischief or revenge and fun also.* (SINGH, 2007)

The likely rise of cybercrime in the form that The Silk Road has taken is not only challenging to law enforcement efforts and legislative agendas, but also undermines the very regime of prohibition of international trade in illicit drugs. It does so legally and culturally.

During the rise of this global regime in the past few decades, intersecting with neoliberal globalization, have resulted in unprecedented harmonization in anti-drug laws.

However, from a legal standpoint focusing on North-America, Canada has become known as a Bitcoin-friendly jurisdiction with positive approaches taken by the authorities. The regulatory and legislative landscape in the US is different and more complicated. In the latest US Senate hearing on virtual currencies, the Senators confidently proclaimed, "existing federal laws, as well as law-enforcement, are capable of addressing the concerns relating to emerging digital assets, although developments are constantly being monitored in the areas of money laundering and other illicit uses". The US Federal regulations relying on the PATRIOT Act require digital assets service providers to be registered as a Money Service Business (MSB), which in turn bound Bitcoin providers and marketplaces to an array of obligations. Additionally, anti-money laundering laws require MSBs to follow financial information reporting policies in order to comply with various requirements under the PATRIOT Act and Bank Secrecy Act. Correspondingly, they also may be subject to analogous requirements under similar state laws.

However, this system of laws is grossly inadequate in engaging virtual currencies.

The lack of clear legislative guidance exacerbates the ambiguous situation Bitcoins are in with the lack of legal classification. Bitcoins are not legally classified, but are vaguely categorized as virtual assets. Law enforcement cannot possibly be effective relying on aged legislation that belongs to the era when most large-scale transactions took place exclusively in banks. This also does not allow Bitcoin to fully realize its economic potential. The Silk Road's use of Bitcoin provides a legal challenge and in turn, challenges the global regime of prohibition of trade in illicit drugs. (RAEESI, 2015)

CONCLUSION

While you work forms that have been used to promote the sale of drugs were presented. The advancement of technology and globalization bring many benefits, but at the same time, there are malicious actions in the virtual environment.

This paper presents a compendium of studies and academic research that has been made about the topic discussed here. There are numerous specific jobs on the black market that has been disseminated in cyberspace.

However, some threads explained here, do not still are discussed in terms that have exposed, and thus an introduction of this academic study to be developed in the course of the analysis are used so that technological innovations

and software for that generation born on the Internet and virtually interact increasingly through innovative gadgets.

As for the topic which deals with the profile of criminals who commit illicit acts demonstrated in the work, it is very important to treat this profile, which fits in the timeline of criminology, passing by Lombroso, saying that criminals were born, after other theorists have shown that the criminal is created by the social environment they live in, ending the timeline in studies of White Collar criminals, when today there is a completely new profile, those criminals who commit crimes in cyberspace.

BIBLIOGRAPHY

ADORJAN, Michael: Drugs on the dark net: how cryptomarkets are transforming the global trade in illicit drugs, by James Martin, Palgrave MacMillan, 2014, 96 pp., $55.90 (hard cover), $38.00 Kindle edition. **British Journal of Criminology**, v. 55, n. 4, p. 835-836, 2015.

ALHOGBANI, A. Going Dark: Scratching the Surface of Government Surveillance. **CommLaw Conspectus**: Journal of Communications Law and Technology Policy, v. 23, n. 2, p. 469-501, 2015.

ALI, S. T.; CLARKE, D.; MCCORRY, P. **Bitcoin**: Perils of an Unregulated Global P2P Currency, 2015.

BARRATT, M. J. Silk Road: eBay for drugs. **Addiction**, v. 107, n. 3, p. 683-683, 2012.

BARRATT, M. J.; FERRIS, J. A.; WINSTOCK, A. R. Use of Silk Road, the online drug market-place, in the United Kingdom, Australia and the United States. **Addiction**, v. 109, n. 5, p. 774-783, 2014.

BAUER, M. W.; GASKELL, G. **Pesquisa qualitativa com texto, imagem e som**: um manual práti-co. Petrópolis: Vozes, 2002.

BERGMAN, M. K. White paper: the deep web: surfacing hidden value. **Journal of electronic publishing**, v. **7**, n. 1, 2001.

BLOOM, C. **Silk Road-Anonymous Deep Web Marketplace**, 2013.

BRADBURY, D. The problem with Bitcoin. **Computer Fraud & Security**, n. 11, p. 5-8, 2013.

BUXTON, J.; BINGHAM, T. **The Rise and Challenge of Dark Net Drug Markets**, 2015.

CHEUNG, K. H.; PRUD'HOMMEAUX, E.; WANG, Y.; STEPHENS, S. Semantic Web for Health Care and Life Sciences: a review of the state of the art. **Briefings in bioinformatics**, v. 10, n. 2, p. 111-113, 2009.

CHRISTIN, N. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. **Proceedings of the 22nd international conference on World Wide Web**. International World Wide Web Conferences Steering Committee, May 2013. p. 213-224.

CRUZ, José. Jurisdições de Sigilo: A Verdadeira Identidade dos Paraísos Fiscais, o que Mudou? **Revista Portuguesa de Contabilidade**, v. II, n. 8, p. 473-500, 2012.

CRUZ, José N.; CARDOSO, Carla S.; LEITE, André L.; FARIA, Rita. **Infrações Económicas e Financeiras**: Estudos de Criminologia e Direito. Coimbra: Coimbra, 2013.

DAVID O. Friedrichs. – **Trusted Criminals**: White Collar Crime in Contemporary Society, 4th edition, Wadsworth, USA, 2010.

Drug related cybercrime and associated use of the Internet. Overview, analysis and possible actions by the Pompidou Group. Disponível em <http://www.coe.int>. Acesso em: 20 jun. 2015.

GERHART, S. Do Web search engines suppress controversy? **First Monday**, v. **9**, n. 1, 2004.

GUEDES, Inês; CRUZ, José N. Personalidade e Crimes de Colarinho Branco. **Revista de Reinserção Social e Prova**: Ousar Integrar, v. 10, p. 47-60, 2011.

HE, B.; PATEL, M.; ZHANG, Z.; CHANG, K. C. C. Accessing the deep web. **Communications of the ACM**, v. 50, n. 5, p. 94-101, 2007.

HE, H.; MENG, W.; YU, C.; WU, Z. Wise-integrator: A system for extracting and integrating complex web search interfaces of the deep web. *In*: **Proceedings of the 31st international conference on Very large data bases**. VLDB Endowment, August 2005, p. 1.314-1.317.

HOUT, Marie Claire Van. **Drugs on the dark net**: how cryptomarkets are transforming the global trade in illicit drugs, by James Martin, New York, Palgrave, 2015.

MACMILLAN, £45.00 (hardback), **Global Crime**, 2014, 102 p.

KANE, A. M. A revocable anonymity in Tor, 2015.

KNUTTILA, L. User unknown: 4chan, anonymity and contingency. **First Monday**, v. 16, n. 10, 2011.

LIU, W.; MENG, X.; MENG, W. Vide: A vision-based approach for deep web data extraction. **Knowledge and Data Engineering, IEEE Transactions on**, v. 22, n. 3, p. 447-460, 2010.

LOMBROSO, Cesare. (1897). **Presentazione di Armando Torno. L'uomo delinquente**. 5. ed. Milano: Bompiani, 1953.

LU, Y., HE, H., ZHAO, H., MENG, W., & YU, C. (2007, April). Annotating structured data of the deep Web. *In* **Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on** (pp. 376-385). IEEE.

MADHAVAN, J.; AFANASIEV, L.; ANTOVA, L.; HALEVY, A. Harnessing the deep web: Present and future. **arXiv preprint arXiv:0909.1785**, 2009.

MADHAVAN, J.; KO, D.; KOT, Ł.; GANAPATHY, V.; RASMUSSEN, A.; HALEVY, A. Google's deep web crawl. **Proceedings of the VLDB Endowment**, v. 1, n. 2, p. 1.241-1.252, 2008.

MARTIN, J (). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. **Criminology and Criminal Justice**, v. 14, n. 3, p. 351-367, 2014.

MOORE, T. The promise and perils of digital currencies. **International Journal of Critical Infrastructure Protection**, v. 6, n. 3, p. 147-149, 2013.

NUNES, Emily Canto. **'Tudo sobre todos'**: site vende dados pessoais e mostra até endereço no mapa, 2015. Disponível em: <http://tecnologia.ig.com.br>. Acesso em: 25 jul. 2015.

PHELPS, A.; WATT, A. I shop online-recreationally! Internet anonymity and Silk Road enabling drug use in Australia. **Digital Investigation**, v. 11, n. 4, p. 261-272, 2014.

Pompidou Group Work Programme 2015-2018. **Drug policy and human rights**: new trends in a globalised context. Disponível em <http://www.coe.int>. Acesso em: 20 jun. 2015.

RAEESI, R. The Silk Road, Bitcoins and the Global Prohibition Regime on the International Trade in Illicit Drugs: Can this Storm Be Weathered?. **Glendon Journal of International Studies/Revue d'études internationales de Glendon**, v. 8, n. 2, 2015.

SANTI, Alexandre de. ().O lado negro do Facebook. **Superinteressante**. São Paulo: Abril. Edição 348, p. 30-34, 2015.

SINGH, Pramod Kr. **Laws on Cyber Crimes**. Book Enclave. Jaipur, Índia, 2007.

STEFAŃSKI, R. **Social Order and Network Security**. Exploratory Research on TOR Hidden Network.

STRAUSS, Anselm L. Qualitative Analysis. **For Social Scientists**. Austrália: Cambridge University Press, 1994.

VAN HOUT, M. C.; BINGHAM, T. 'Silk Road', the virtual drug marketplace: A single case study of user experiences. **International Journal of Drug Policy**, **24**(5), 385-391. 2013

_____; _____. 'Surfing the Silk Road': A study of users' experiences. **International Journal of Drug Policy**, v. 24, n. 6, p. 524-529, 2013.

_____; _____. Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. **International Journal of Drug Policy**, v. 25, n. 2, p. 183-189, 2014.

VANDERVALK, B. P.; MCCARTHY, E. L.; WILKINSON, M. D. Moby and Moby 2: creatures of the deep (web). **Briefings in bioinformatics**, v. 10, n. 2, p. 114-128, 2009.

VEERASAMY, N. **Motivation for cyberterrorism**, 2010.

WU, W.; DOAN, A.; YU, C. Webiq: Learning from the web to match deep-web query interfaces. *In*: **Data Engineering, 2006. ICDE'06. Proceedings of the 22nd International Conference on**. IEEE, April 2006. p. 44-44.

WU, W.; YU, C.; DOAN, A.; MENG, W. An interactive clustering-based approach to integrating source query interfaces on the deep web. *In*: **Proceedings of the 2004 ACM SIGMOD international conference on Management of data**. ACM, June 2004. p. 95-106.