XXVI ENCONTRO NACIONAL DO CONPEDI BRASÍLIA – DF

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

IRINEU FRANCISCO BARRETO JUNIOR

VIVIANE COÊLHO DE SÉLLOS KNOERR

AIRES JOSE ROVER

Copyright © 2017 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos.
Nenhuma parte deste anal poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Prof. Dr. Raymundo Juliano Feitosa – UNICAP
Vice-presidente Sul - Prof. Dr. Ingo Wolfgang Sarlet – PUC - RS
Vice-presidente Sudeste - Prof. Dr. João Marcelo de Lima Assafim – UCAM
Vice-presidente Nordeste - Profa. Dra. Maria dos Remédios Fontes Silva – UFRN
Vice-presidente Norte/Centro - Profa. Dra. Julia Maurmann Ximenes – IDP
Secretário Executivo - Prof. Dr. Orides Mezzaroba – UFSC
Secretário Adjunto - Prof. Dr. Felipe Chiarello de Souza Pinto – Mackenzie

Representante Discente – Doutoranda Vivian de Almeida Gregori Torres – USP

Conselho Fiscal:
Prof. Msc. Caio Augusto Souza Lara – ESDH
Prof. Dr. José Querino Tavares Neto – UFG/PUC PR
Profa. Dra. Samyra Haydêe Dal Farra Naspolini Sanches – UNINOVE
Prof. Dr. Lucas Gonçalves da Silva – UFS (suplente)
Prof. Dr. Fernando Antonio de Carvalho Dantas – UFG (suplente)

Secretarias:
Relações Institucionais – Ministro José Barroso Filho – IDP
Prof. Dr. Liton Lanes Pilau Sobrinho – UPF
Educação Jurídica – Prof. Dr. Horácio Wanderlei Rodrigues – IMED/ABEDi
Eventos – Prof. Dr. Antônio Carlos Diniz Murta – FUMEC
Prof. Dr. Jose Luiz Quadros de Magalhaes – UFMG
Profa. Dra. Monica Herman Salem Caggiano – USP
Prof. Dr. Valter Moura do Carmo – UNIMAR
Profa. Dra. Viviane Coêlho de Séllos Knoerr – UNICURITIBA
Comunicação – Prof. Dr. Matheus Felipe de Castro – UNOESC

D597

Direito, governança e novas tecnologias [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Aires Jose Rover; Irineu Francisco Barreto Junior; Viviane Coêlho de Séllos Knoerr - Florianópolis: CONPEDI, 2017.

Inclui bibliografia
ISBN: 978-85-5505-443-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: Desigualdade e Desenvolvimento: O papel do Direito nas Políticas Públicas

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 3. Cidadania. 4.Tecnologia.

5. Liberdade de expressão. XXVI EncontroNacional do CONPEDI (26. : 2017 : Brasília, DF).

CDU: 34

CONPEDI

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito
Florianópolis – Santa Catarina – Brasil
www.conpedi.org.br

XXVI ENCONTRO NACIONAL DO CONPEDI BRASÍLIA – DF

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

Apresentação

A comunidade científica do Direito celebra a superação de duas décadas em estudos e pesquisas sobre as interfaces entre fenômeno jurídico e internet, novas tecnologias comunicacionais e avanços informáticos. Desde a gênese desse campo de estudos jurídicos, a doutrina nacional e internacional analisa os reflexos no direito material, processual, individual e coletivo oriundos da sociedade da informação e das redes comunicacionais planetárias.

Os encontros nacionais do Conselho Nacional de Pesquisa e Pós-graduação em Direito (Conpedi) têm se consolidado como referência na disseminação de pesquisas que abordam esses novos fenômenos. Foi o que novamente ocorreu no XXVI Encontro Nacional do Conpedi, realizado em Curitiba entre 19 e 21 de julho de 2017, no Grupo de Trabalho Direito, Governança e Novas Tecnologias. Pesquisadores de diferentes regiões do Brasil apresentaram seus estudos e debateram a contemporaneidade e novos efeitos do paradigma estabelecido entre Direito e Internet.

Destaca-se entre os artigos apresentados a originalidade e notável convergência entre os temas abordados, que podem ser compilados sob enfoques atuais e relevantes, conforme será apresentado a seguir. A proteção dos Direitos Humanos no ambiente de internet perpassou diversos artigos, sob perspectivas que foram desde os conflitos entre liberdade de expressão versus proteção da privacidade, até a responsabilidade dos provedores de conteúdo na remoção de conteúdos que atentem contra a dignidade da pessoa humana e o direito ao esquecimento. A possibilidade de ampliação do exercício da cidadania e fortalecimento dos regimes democráticos também foi objeto de pesquisas apresentadas no GT, o que coaduna com acontecimentos recentes, nos quais a internet esteve no centro de levantes mundiais contra regimes de exceção e autoritários.

A abordagem da prevenção de crimes eletrônicos, cada vez mais recorrentes, fez-se presente em artigos que tratam das formas de composição dos conflitos que ocorrem na internet – particularmente a responsabilização administrativa por meio das ordenações, como vem ocorrendo em Portugal e na Alemanha –, e da aplicação da tecnologia na prevenção tais delitos. O foco da violência contra a mulher e do discurso homofóbico na internet esteve presente, justificado pela constância de casos que aviltam contra os direitos humanos em redes sociais, grupos de WhatsApp ou na rede mundial de computadores.

Questões específicas, mas que também dialogam com a preservação de direitos fundamentais na sociedade informacional, fizeram-se presentes em artigos que versam sobre a acessibilidade de portais de órgão públicos para pessoas com deficiência e das inovações na educação superior brasileira, frente o ensino a distância e o exercício da docência.

Em suma, os trabalhos apresentados renovam os compromissos da pesquisa jurídica brasileira e a preservação de direitos, da dignidade da pessoa humana e do aperfeiçoamento do regime democrático. Os coordenadores do GT convidam os leitores para desfrutarem do teor integral dos artigos, com a certeza da profícua leitura, e encerram agradecendo a possibilidade de novamente dirigir os debates com a participação de pesquisadores altamente qualificados.

Prof. Dr. Aires José Rover (UFSC)

Profª. Drª. Viviane Coêlho de Séllos Knoerr (Unicuritiba)

Prof. Dr. Irineu Francisco Barreto Junior (FMU)

BLOCKCHAIN E A PREVENÇÃO DE CRIMES ELETRÔNICOS NA SOCIEDADE DA INFORMAÇÃO

BLOCKCHAIN AND THE PREVENTION OF ELECTRONIC CRIMES IN THE INFORMATION SOCIETY

Irineu Francisco Barreto Junior [1]
Juliana Moreira [2]

Resumo

Este artigo analisa a possibilidade de prevenção de crimes digitais com a utilização do novo recurso tecnológico denominado Blokchain, que promete revolucionar a armazenagem de dados digitais com mais segurança e transparência, pois trata-se de sistema que rompe o padrão usual de bancos de dados, inclusive usados por instituições financeiras, para guardar informações de seus clientes. Perante as funcionalidades informáticas da nova estrutura de banco de dados denominada Blokchain, e após levantamento e análise das principais modalidades de crimes informáticos, torna-se possível concluir pela efetiva possibilidade de aplicação da ferramenta na prevenção de algumas das principais modalidades delitivas na internet.

Palavras-chave: Sociedade da informação, Blockchain, Crimes eletrônicos, Bitcoin

Abstract/Resumen/Résumé

This article analyzes the possibility of preventing digital crimes using the new technology called Blokchain, which promises to revolutionize the storage of digital data with greater security and transparency, because it is a system that breaks the usual database standard, Including used by financial institutions, to store information for its customers. Due to the computational functions of the new database structure called Blokchain, and after surveying and analyzing the main types of computer crimes, it is possible to conclude that the tool is effective in preventing some of the main delinquencies on the Internet.

Keywords/Palabras-claves/Mots-clés: Information society, Blokchain, Eletronic crimes, Bitcoin

---

[1] Docente do Programa de Mestrado em Direito da Sociedade da Informação– FMU-SP. Docente Convidado da ESA-OAB-SP. Analista de Pesquisas do Seade – SP. Doutor em Ciências Sociais pela PUC-SP

[2] Mestre em Direito da Sociedade da Informação– FMU-SP. Professora de Direito Penal na FMU-SP. Pós-Graduada em Direito Penal e Processo Penal pela Universidade Presbiteriana Mackenzie. Advogada.

Introdução

Este artigo analisa a possibilidade de prevenção de crimes digitais com a utilização do novo recurso tecnológico denominado Blokchain, que promete revolucionar a armazenagem de dados digitais com mais segurança e transparência, pois trata-se de sistema que rompe o padrão usual de bancos de dados, inclusive os usados por instituições financeiras, para armazenar informações de seus clientes. Atualmente os servidores de dados são centralizados, sejam pessoas jurídica ou físicas, mantidos em máquinas e computadores sobre os quais há consenso quanto à vulnerabilidade. O Blockchain, surgido em 2008 como a infraestrutura responsável pela moeda virtual Bitcoin, tem como uma de suas possibilidades práticas a aplicação nos contratos eletrônicos inteligentes, ao determinar que ações aconteçam automaticamente segundo parâmetros determinados entre as partes.

A tecnologia Blockchain permite que no lugar de concentrar todos os registros em uma única máquina, os bancos de dados possam ser espalhados por redes com vários servidores conectados, diversos locais com cópias do conteúdo e gerenciado de forma compartilhada. Os dados são armazenados em blocos de informação criptografada, "que se conectam como uma corrente –daí o nome "cadeia de blocos", em inglês. A revolução tecnológica ocorrida nos meios de comunicação deu origem a uma nova era denominada como *Sociedade da Informação*. A sua principal característica é a facilidade de obtenção de informações advindas de qualquer lugar do mundo em tempo quase que real, de forma jamais vista na história da humanidade. Denota-se que a *informação é o centro gravitacional* desta nova era, em outras palavras, é possível afirmar que ela possui valor comercial. Barreto Júnior (2015, p. 410) ao tratar do tema esclarece que:

> O advento do *Informacionalismo* é, indubitavelmente, a principal marca econômica da sociedade em rede. Reorganiza a produção de riqueza no sistema econômico, no qual há uma gradativa valoração da informação como mercadoria e fator de geração de valor econômico, o que torna a *National Association of Securities Dealers Automated Quotations* (Nasdaq), bolsa de valores das empresas tecnológicas, tão estratégica, em termos de organização econômica, quanto a tradicional *New York Stock Exchange*, denominada bolsa de *Wall Street*. As megacorporações informativas (*Google*, *Facebook* e *Yahoo*, entre outras) acumulam vestígios de informações sobre os usuários da Internet, tais como seus padrões de navegação, compras realizadas on-line, preferências culturais, religiosas e ideológicas, *websites* de interesse, verbetes e expressões pesquisadas nos *websites* de busca, entre outras, "*impressões digitais eletrônicas"* que servem para estabelecer uma categorização minuciosa de cada usuário na rede. (...). Circunscreve-se no fato de que há inúmeros usos para esses perfis eletrônicos, tal como direcionamento de publicidade *on-line*,

> oferta de mercadorias relacionadas ao perfil do consumidor, além de montar cadastros de valor incomensurável sobre os cidadãos da sociedade em rede. (BARRETO JUNIOR (2015, p. 410)

A metodologia aplicada neste artigo visa compreender de forma mais acurada essa nova ferramenta tecnológica e compilar os principais crimes cometidos na Internet. O seu intuito é analisar o potencial dessa ferramenta na prevenção de delitos perpetrados em meio eletrônico.

1. Blockchain e a incessante inovação tecnológica na Sociedade da Informação

Conforme reportagem publicada no Jornal Folha de São Paulo[1], uma "nova tecnologia chamada Blockchain promete revolucionar a armazenagem de dados digitais, com mais segurança e transparência. Esse sistema rompe o padrão usado atualmente por bancos de dados, inclusive os usados por instituições financeiras, para armazenar informações de seus clientes." A matéria explica que atualmente os servidores de dados são centralizados, sejam pessoas jurídica ou físicas, mantidos em máquinas e computadores sobre os quais há consenso quanto à vulnerabilidade. Transações como transferência de dinheiro pela internet exigem que o banco A, por exemplo, necessite verificar em seus registros se há fundos disponíveis para informar o banco B.

O Blockchain surgiu em 2008 como a infraestrutura responsável pela moeda virtual Bitcoin. Segundo reportagem do New York Times[2], desde que o Blockchain foi fundado em 2011, na Grã-Bretanha, ganhou respeito na indústria por aderir à filosofia original da moeda virtual de anonimato e descentralização. Roger Ver, um libertário conhecido em alguns círculos como o *"Jesus Bitcoin"*, foi o primeiro apoiador e apoiador da empresa. "Ao longo dos próximos 10 anos, Bitcoin vai ter um grande impacto", disse Jeremy Liew, um parceiro da Lightspeed, que vai se juntar placa Blockchain." Onde está o nexo central da criação de valor em toda esta indústria? Tem que ser a carteira ", disse ele. A rodada de financiamento da Blockchain segue uma série de grandes investimentos em empresas da Bitcoin, particularmente aquelas que oferecem serviços de

[1] JORNAL FOLHA DE SÃO PAULO. **Tecnologia 'Blockchain' promete revolucionar armazenagem de dados.** 15. abr. 2017.
[2] EMBLER, Sidney. Blockchain é o mais recente lançamento da Bitcoin para atrair grande investimento. **Jornal New York Times**, 06. Out. 2014.. Disponível em <https://dealbook.nytimes.com/2014/10/06/blockchain-is-latest-bitcoin-start-up-to-lure-big-investment/?_r=0>. Acesso em 15, abr. 2017.

armazenamento. Para que a Bitcoin seja mais amplamente adotada, dizem os simpatizantes, a moeda virtual deve encontrar uma aplicação única que o leve para além do campo da especulação. E para que isso aconteça, as empresas devem primeiro construir uma plataforma robusta, que é o que Blockchain diz que está tentando fazer.

Uma das possibilidades práticas para sua aplicação são os contratos virtuais inteligentes, ao determinar que ações aconteçam automaticamente segundo parâmetros determinados entre as partes. Por exemplo, fazer o pagamento de uma multa caso um termo não seja cumprido. Seu uso ampliado, porém, é algo novo e está em fase de estudos, por isso ainda não há muitas aplicações concretas disponíveis. A tecnologia Blockchain permite que no lugar de concentrar todos os registros em uma única máquina, os bancos de dados possam ser espalhados por redes com vários servidores conectados, diversos locais com cópias do conteúdo e gerenciado de forma compartilhada. Os dados são armazenados em blocos de informação criptografada, “que se conectam como uma corrente –daí o nome "cadeia de blocos", em inglês. Com tudo interligado, é impossível excluir uma informação depois que ela foi inserida no sistema. ” A tecnologia exige, portanto, para que alguma alteração aconteça, o Blockchain deva “entrar em consenso”. As várias máquinas que guardam a informação precisam concordar que aquele processo é válido.

> O Blockchain é muito similar à internet em 1994. Muitas pessoas falam sobre seu potencial, mas poucos sabem aproveitá-lo", resume Brian Behlendorf, diretor-executivo do Hyperledger, projeto colaborativo mantido pela Linux Foundation –que tem apoio de gigantes como Intel e IBM–, que visa o desenvolvimento desse sistema. "A sensação é de uma revolução." Segundo especialistas, as implementações vão desde sistemas para evitar fraudes em bancos a postes inteligentes que alertam a polícia ao ouvir barulhos de tiros e mecanismos para ajudar a controlar a qualidade da carne. Tal Eisner, diretor de produtos da empresa israelense de cibersegurança ThetaRay, diz que o mercado ainda não compreendeu a tecnologia. "Essas conexões de certa forma invisíveis são ainda um problema, pois atraem hackers e ameaças", afirma.

Em suma, o Blockchain funciona da seguinte forma. Uma informação sobre uma transação na Internet (transferência de valores entre bancos, compra e venda de Bitcoins ou contratação eletrônica, por exemplo) é adicionada à rede mundial de computadores e, simultaneamente, várias outras máquinas (chamadas de nós) validam a transação. Se os registros de alguma dessas transações, supra exemplificadas, forem confirmados pelos vários nós conectados ao Blockchain, a informação fica registrada junto ás demais dos blocos. Os blocos interligados formam uma rede e as operações registradas nessa interconexão não podem mais ser alteradas. Seus divulgadores apontam como vantagens

a segurança, transparência, imutabilidade e redução de custos nas transações eletrônicas. Pode ser ainda aplicada para evitar fraudes, registro de histórico de serviços médicos (Cadastro do SUS e do Cartão Nacional de Saúde poderiam ir para a rede), serviços financeiros, transferências de moedas, contratos inteligentes e combates à pirataria. Seus principais problemas são o escasso conhecimento atual sobre suas possibilidades e a impossibilidade de retirar informações do ar, caso decorra de alguma decisão judicial.

2. Sociedade da Informação e os Crimes Eletrônicos

O estudo das relações entre Direito e Sociedade adquire *status* estratégico na era da Sociedade da Informação, uma vez que as novas relações sociais, interpessoais e interinstitucionais, muitas vezes travadas em cenário internacional, exigem uma nova reflexão sobre paradigmas, teorias e aplicação do Direito que, como fato social, não se mantém indiferente aos novos arranjos e contornos desse atual modelo de sociedade. Como exemplo desta perspectiva tem-se o fenômeno dos crimes informáticos.

Nesse ponto cumpre esclarecer que ao tentar nominar os crimes cometidos mediante a internet, percebe-se que inexiste consenso quanto à denominação deste tipo de delito na bibliografia relacionada ao tema, pois diversos autores procuram encontrar a melhor definição para o conceito de crime informático, o que leva à apresentação de diversas denominações que, na prática, se referem à mesma modalidade delitiva.

Desta feita, encontram-se variadas definições sobre o assunto, tais como crimes de informática, crimes digitais, crimes eletrônicos, crimes informáticos, delitos ou crimes virtuais, crimes com computador, cybercrimes, e-crime, crime *hitech*, crimes eletrônicos, dentre outras denominações. E apesar de inexistir consenso quanto à melhor nomenclatura, parece ser mais viável adotar a denominação “crimes informáticos”. Fiorillo e Conte (2013, p. 142) destacam a diversidade de denominações e classificações, concluindo que a mais oportuna é “crimes informáticos”, principalmente pela sua abrangência, “[...] que permite abarcar um campo de estudo maior, levando em consideração toda a delinquência relacionada com a informática e as novas tecnologias”.

Portanto, a denominação “crimes informáticos” se baseia no bem jurídico efetivamente tutelado quando a internet é utilizada para a prática delitiva, que é a

inviolabilidade das informações automatizadas. De fato, com o advento da internet surgiu uma nova modalidade de crimes cometidas no espaço virtual, através de *e-mails* (correio-eletrônico), *websites* (sítios pessoais, institucionais ou apócrifos) ou mesmo ocorridos em comunidades de relacionamentos, a exemplo do Facebook. De igual forma, as transações comerciais e financeiras, que ganharam relevo ao longo das últimas décadas na rede mundial de computadores, contribuíram para fomentar os delitos informáticos, pois as transações exigem a identificação do número de cartão de crédito, dados referentes às contas bancárias, senhas e demais mecanismos de segurança, contribuindo para fomentar os crimes informáticos ou crimes virtuais.

De acordo com Fiorillo e Conte (2013, p. 233), na atualidade as instituições financeiras, por exemplo, "[...] operam e prestam serviços quase que integralmente e por meio da Internet, e a paralisação de suas atividades sou a interferência, mínima que seja, em suas atividades, gera insegurança aos seus usuários e significa prejuízos incomensuráveis", sendo de suma importância a segurança no processamento de dados. A violação de dados no Brasil, perpetrada das mais variadas formas, é problema é tão grave que Fiorillo e Conte (2013, p. 140) destacam que o ano de 2011 (399.515 casos registrados) marcou pelo grande número de casos envolvendo problemas relacionados à vírus, códigos maliciosos e tentativas de fraude, triplicando o número se comparado ao ano de 2010 (142.844 casos registrados).

Nesse cenário, os crimes virtuais constituem novos temas de investigação para a pesquisa jurídica, não apenas quanto à sua tipificação, mas também investigações sobre a existência ou não de legislação brasileira para coibi-los ou solucionar conflitos surgidos no espaço virtual, dentre questões outras, voltadas a suprir a vulnerabilidade dos indivíduos que se valem da internet para as mais diversas atividades e se veem expostos. No Brasil, o assunto crime informático está começando a se difundir, várias notícias já circulam na mídia como forma de tentar alertar os usuários sobre os perigos e consequências de um uso incorreto do computador. Os campos informática cresceram rapidamente, tornando possível a distribuição e captação de dados em larga escala para toda a sociedade. Isso se deve principalmente em virtude da expansão das novas tecnologias, da facilidade de acesso à computadores e a internet, da rapidez com que as informações são difundidas, representando um momento único na história da humanidade.

Em meio a esse cenário a internet acaba por estimular a prática de diversos crimes, alguns que somente podem ser praticados por meio da rede mundial e computadores; e, alguns delitos como furto, calúnia, ameaça, difamação, dentre outros, que encontram tipificação na legislação esparsa, mas que encontram na internet terreno fértil para a sua propagação, até mesmo porque os indivíduos infelizmente ainda acreditam que se trata de uma "terra sem lei", principalmente pelo anonimato que possibilita.

Mas, afinal, o que é crime informático ou virtual? Infelizmente, assim como ocorre com a nomenclatura, em que não há consenso entre os estudiosos, também quanto à definição, principalmente pela inexistência de um diploma legal que efetivamente tutela os crimes informáticos no Brasil, há divergências quanto ao conceito. Rosa (2002, p. 53) chama a atenção para o fato de que diversos autores definem os crimes informáticos, embora sua grande maioria veem os crimes na internet como uma conduta ilegal, realizada por meio do uso do computador e da internet. Trata-se de conceito amplo.

Já Fiorillo e Conte (2013, p. 142) definem o crime informático como "ilícitos perpetrados por intermédio da Internet ou com o auxílio desta, causando algum tipo de dano à vítima", conceito este que, segundo os próprios autores, é amplo e abarca situações nas quais há o uso do computador para a prática delitiva, bem como aquelas praticadas contra o sistema informático. Portanto, trata-se de uma conduta que no mundo real já está tipificada no ordenamento jurídico brasileiro, ferindo assim um bem jurídico tutelado, e para a sua consumação o meio essencial utilizado é o auxílio de um computador, embora alguns delitos informáticos somente possam ser praticados no mundo virtual, como a invasão a sistemas, alteração de dados, dentre outros. A esse respeito preleciona Lima (2005, p. 29):

> Em verdade, os crimes de computador são, na maior parte das vezes, os crimes comuns cometidos com o auxílio de um computador, podendo os crimes de furto, apropriação indébita, estelionato ou dano, ser cometidos por esse meio com consideráveis prejuízos patrimoniais. Entretanto, há algo além de uma nova ferramenta, de um novo meio, de um novo *modus operandi* para o cometimento de crimes: estamos também diante de novas condutas não tipificadas.

Dessa forma, percebe-se que os crimes informáticos são todos aqueles relacionados aos dados arquivados nos computadores, acessados ilicitamente, utilizados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico (CORRÊA, 2000, p. 43), o que não afasta, por conseguinte, os delitos

praticados através da internet. Isso se deve porque os princípios fundamentais do ciberespaço é a distribuição, produção e o compartilhamento de dados e informações na rede mundial de computadores, a internet, já que com ela se pode conectar a diversas partes do universo, sem sair de casa.

Questão que não pode ser ignorada é que a internet permite a quebra de fronteiras, pois as pessoas interagem com diversas culturas, nacionalidades, podem se relacionar com inúmeras pessoas a partir da identificação de afinidades e interesses comuns, rompendo, assim, com as barreiras geográficas. Desta feita, são inúmeros os benefícios que a internet proporciona. Ocorre que ao mesmo tempo o espaço cibernético proporciona benesses, também evidencia as vulnerabilidades. Logo, os mesmos comportamentos que se concretizam no mundo físico podem ser levados ao mundo virtual, a exemplo de relacionamentos, contratações, compras, etc.

Fiorillo e Conte (2013, p. 13) ressaltam que o crescimento da utilização dos computadores e o acesso facilitado à internet, embora seja um inegável avanço para a sociedade, possibilitando que atividades diversas sejam realizadas de forma célere, também abriu espaço para uma nova espécie de criminalidade. Logo, a Internet apesar de ser uma ferramenta de acesso à informação e ter como finalidade a expansão da comunicação, traz consequências desastrosas, uma vez que as pessoas utilizam de uma forma errada, sendo utilizada para outras finalidades, como a prática de crimes, clamando a intervenção estatal.

Várias são as classificações encontradas na doutrina quanto aos crimes virtuais, já que várias são as maneiras de materialização dos delitos, como, por exemplo, quando o computador serve apenas como ferramenta para a prática, quando o computador é o instrumento de execução, e outros crimes originados no mundo virtual, porém expandidos para a vida real. Furlaneto Neto, Santos e Gimenes (2012, p. 31) explicam, de forma clara, as três categorias dos crimes informáticos: os que utilizam a tecnologia eletrônica como método, ou seja, condutas criminais nos quais os indivíduos utilizam métodos eletrônicos para obter um resultado ilícito; os que utilizam a tecnologia eletrônica como meio, ou seja, condutas criminais em que para a realização de um delito utilizam o computador como meio; e, por último, os que utilizam a tecnologia eletrônica como fim, ou seja, condutas dirigidas contra a entidade física do objeto ou máquina eletrônica o seu material com o objetivo de danificá-lo.

Fiorillo e Conte (2013, p. 144), por sua vez, classificam os crimes informáticos em puro (toda conduta ilícita que tenha por objetivo exclusivo o sistema de computador, atentando contra os seus aspectos físicos ou técnicos, componentes, inclusive dados e sistemas), mistos (quando o uso da internet é condição *sine qua non* para a efetivação da conduta, apesar do bem jurídico ser diverso do informático) e comum (quando se utiliza da internet para a prática de delitos outros, tipificados na legislação penal). Já Vianna e Machado (2013, p. 30-36) classificam os crimes informáticos em quatro categorias: crimes informáticos impróprios, crimes informáticos próprios, crimes informáticos mistos e crime informático indireto. Porém, percebe-se que apesar de nomenclatura diversa, os autores acabam por concluir pela existência do crime informático puro, impuro e misto, a depender do alcance e *modus operandi*.

Os crimes informáticos impróprios são aqueles onde o computador é a ferramenta para a execução do crime, porém não existe alteração ou furto da informação, ou seja, o computador está sendo utilizado para cometer os ataques. Como por exemplo, usar o computador para disseminar e-mails com calúnia, difamação, injúria e até mesmo para jogos ilegais. Neste sentido, nada mais são do que a evolução através do *modus operandi* daqueles delitos já previstos tradicionalmente (VIANNA; MACHADO, 2013, p. 30).

Logo, sempre que o computador servir tão somente para a execução de um delito, sem que haja ofensa direta aos dados armazenados no computador ou mesmo na rede mundial de computadores, realidade cada vez mais presentes, principalmente pelos serviços de armazenagem em nuvens, se está diante de um crime informático impróprio. Dessa forma, utilizar a informática somente como ferramenta para a inovação de um crime já tipificado pela lei penal, por exemplo, a pornografia infantil divulgada pela internet, e não mais de outros meios antigos como jornais, revistas ou periódicos (PINHEIRO, 2013, p. 76), se encaixa na modalidade crimes informáticos impróprios.

Na classificação de Furlaneto Neto e Guimarães (2003, p. 69) os delitos em comento são classificados como delitos virtuais comuns, que se configura sempre que a utilização da internet é para a realização de delitos já tipificados na legislação penal. Por sua vez, os crimes informáticos próprios são aqueles onde o computador é o instrumento para a execução do crime e a informação é violada, a exemplo da interceptação ilegal em sistemas de informática e telemática, ou a criação e divulgação de programas de computadores destrutivos (vírus). Conforme definem Vianna e Machado (2013, p. 32),

“crimes informáticos próprios são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados) ”.

Assim, quando a prática delitiva tem como alvo o computador em si, ataque este que pode ser físico ou técnico, ou seja, atingir a máquina em si ou seus componentes, a exemplo de programas, trata-se de crime próprio. Conforme Furlaneto Neto e Guimarães (2003, p. 69), o “crime virtual puro seria toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas”. Logo, crime virtual puro ou próprio são denominações para uma mesma categoria delitiva.

Tem-se, ainda, os crimes informáticos mistos, que são aqueles mais complexos, pois além da informação violada, está previsto em lei a proteção sob o equipamento de qualquer natureza diversa. É o que ocorre quando configurada a invasão do dispositivo informático vinculado ao sistema eleitoral, figura típica prevista no art. 72, inciso I, da Lei nº 9.504/1997 (FURLANETO NETO, GUIMARÃES, 2003, p. 69). Vale esclarecer que no caso em comento a punição se volta à invasão do dispositivo informático vinculado ao sistema eleitoral. Por isso o bem jurídico tutelado é misto, pois ao mesmo tempo em que se viola a informação contida no dispositivo informático, que de forma mediata visa tutelar o sigilo dos votos, também se resguarda a manifestação da vontade dos eleitores, que no ordenamento jurídico brasileiro é segredo.

Por último, mas não menos importante, tem-se os crimes informáticos indiretos, que são aqueles onde o crime que se concretizou na vida real, sendo originado pelo meio informático (FURLANETO NETO, GUIMARÃES, 2003, p. 69). Segundo Vianna e Machado (2013 p. 35), tem-se o “crime informático mediato ou indireto é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação”. Tal delito ocorre, por exemplo, quando há a invasão de um dispositivo informático de um banco, onde o agente transfere valores para sua conta. Nesse caso são cometidos dois delitos diferentes: um seria a invasão do dispositivo e outro o furto, sendo assim o primeiro crime informático e o segundo crime patrimonial.

Furlaneto Neto e Guimarães (2003, p. 69) também apresentam o conceito de crimes informáticos indiretos. Nesse caso o “[...] uso da internet é condição *sine qua non* para a efetivação da conduta [...]”. Fiorillo e Conte (2013, p. 143) ressaltam que são os crimes informáticos ou virtuais puros, ou seja, aqueles que atacam os programas informáticos ou a parte física do computador, por não possuir respaldo na legislação

brasileira, é que apresentam grande desafio, pois há dificuldade no enquadramento da conduta em tipos penais previstos no Código Penal ou legislação esparsa, por clara violação ao princípio da legalidade. Isso não ocorre, por exemplo, quando um crime contra a honra é praticado por meio da internet, pois basta a aplicação do Código Penal para que seja o agente infrator punido.

Há de se ressaltar, ainda, que algumas expressões ganham relevo quando se trata de crimes informáticos. Segundo Fiorillo e Conte (2013, p. 149-153), tem-se o *hacker*, que objetiva vulnerar programas informáticos; o *cracker*, que não apenas invade os programas e acessa informações, mas também as adultera; *pheackers*, especialistas em telefonia que atacam sistemas de telecomunicação móvel ou fixa; *cardes*, que são os criminosos que se apropriam de números de cartão de crédito de usuários da rede para transações diversas; *cyberterrorists*, atividade daqueles que desenvolvem vírus ou bombas lógicas para sabotar computadores e provocar quedas em grandes provedores.

Evidencia-se, portanto, que os crimes virtuais ou informáticos são aqueles atos ilícitos que alcançam os computadores com acesso à rede mundial de computadores, ocasionando danos de natureza patrimonial ou moral, sendo certo que computador e internet podem ser usados para a prática de crimes diversos, que se materializam no mundo físico, tal como ocorre com a distribuição de material pornográfico, crimes contra a honra e/ou patrimônio, ressaltando a amplitude do conceito e o seu alcance prático.

De acordo com o Sydow (2015, p. 114), alguns delitos são mais comumente praticados na internet, a exemplo da intrusão informática, que "[...] refere-se ao ingresso não autorizado de um usuário no sistema alheio, seja ou não para obter alguma vantagem, seja ou não por meios ardilosos, violentos", ou seja, o simples fato de alguém entrar sem permissão, com intuito de obter ou não vantagem. De fato, quando há uma invasão em sistema alheio, como de uma empresa ou instituição financeira, prejuízos diversos podem restar configurados, seja pelo vazamento de informação, transferência de fundos, alteração nos dados, etc. É modalidade de delito informático que precisa ser combatido.

Tem-se, ainda, o furto de identidade virtual, que consiste na apropriação de dados, a exemplo de "[...] características e identificações pessoais de outrem para fazer-se passar por este, sem que, contudo, tenha recebido autorização para tanto" (SYDOW, 2015, p. 117). Neste caso, o usuário criminoso se passa por outra pessoa, utilizando de fotos ou dados pessoais, por exemplo. Infelizmente é comum, na rede mundial de computadores, a utilização de dados de terceiros para os mais diversos fins, tais como

aquisição de serviços e produtos, manifestação de opinião, etc. Não raras vezes indivíduos se passam por outras pessoas, envolvendo terceiros que sequer tem ciência do furto de identidade virtual, prática comum nas redes de relacionamento.

Outra prática comum é a inserção de código malicioso, que segundo Sydow (2015, p. 122), consiste em "instruções inseridas em aparatos alheios por meios de arquivos que dão comandos que implicam algum prejuízo", ou seja, tipos de arquivos, dados, e-mails e toda forma de programa que modifique, altere ou destrói de alguma maneira o sistema de dados, o computador. Tem-se, ainda, o *scamming*, que consiste no "o ato de utilizar-se do meio informático para agir visando obter algum tipo de vantagem sobre o usuário" (SYDOW, 2015, p. 125). Percebe-se que o autor está fazendo referência aos crimes típicos de estelionato, golpes ou armadilhas, ou seja, uma forma de tomar controle de máquinas alheias com o objetivo de obter vantagens.

Já o *spamming* "[...] são mensagens com cunho comercial que infestam as caixas de entrada dos programas de e-mail" (SYDOW, 2015, p. 129). São aquelas mensagens recebidas sem autorização, contendo informações muitas vezes pornografia, propaganda eleitoral, uso de marketing excessivo até disseminação de vírus. A prática em comento, qual seja, o envio de mensagens eletrônicas das mais diversas ordens, principalmente de natureza publicitária sem a solicitação do usuário, ganha espaço a cada dia. Dentre os mais comuns tem-se as propagandas, não raras vezes enganosas; correntes que pedem para que seja a mensagem repassada a outros contatos; brincadeiras, dentre outros conteúdos, que visam instigar o usuário a acessá-los, tornando-se assim vulnerável.

A interceptação de e-mail, que consiste em "impedir que a mensagem de correio eletrônico, enviada por um remetente, atinja seu destinatário" (SYDOW, 2015, p. 133), também é modalidade de crime informático. Independentemente da forma como o crime virtual se configura, prejuízos inúmeros podem ser causados no âmbito patrimonial e moral, como já dito alhures. Fiorillo e Conte (2013, p. 234-235) citam algumas situações em que a prática de crimes informáticos conduziu instituições bancárias a grandes prejuízos, a exemplo do ocorrido em 2008, no banco francês *Société Générale*, que culminou na perda de aproximadamente US$ 7,16 bilhões em virtude de um esquema elaborado por um operador que realizou inúmeras transações fictícias.

Por isso Fiorillo e Conte (2013, p. 238) chamam a atenção para a vulnerabilidade que falhas de segurança pode ocasionar aos usuários em geral, empresas e instituições financeiras, já que a internet faz parte do cotidiano das pessoas. Porém, falhas, em

determinados casos, são cometidas pelos próprios usuários, sendo mister adotar medidas de prevenção, repressão e muita cautela ao lidar com a rede mundial de computadores. Destarte, não há como negar a magnitude dos crimes cometidos pela internet e a necessidade de se investir em tecnologias, em segurança, pois a prática de ilícitos é constante, prejuízos das mais diversas ordens configuradas; e, infelizmente, a legislação não acompanha a criminalidade informática, tanto que, como já dito, inexiste legislação específica a regulamentar o tema no Brasil, dificultando a punição dos envolvidos.

Conclusões

Perante as funcionalidades informáticas da nova estrutura de banco de dados denominada Blokchain, e após levantamento e análise das principais modalidades de crimes informáticos, torna-se possível concluir pela efetiva possibilidade de aplicação da ferramenta na prevenção de algumas das principais modalidades delitivas na internet. A adoção da nomenclatura "crimes informáticos" voltada ao bem jurídico efetivamente tutelado quando a internet é utilizada para a prática delitiva, a inviolabilidade das informações automatizadas pode ganhar nova proteção com a implementação do Blokchain.

Conforme citado anteriormente por Fiorillo e Conte (2013, p. 233), as instituições financeiras "[...] operam e prestam serviços quase que integralmente e por meio da Internet, e a paralisação de suas atividades sou a interferência, mínima que seja, em suas atividades, gera insegurança aos seus usuários e significa prejuízos incomensuráveis", sendo de suma importância a segurança no processamento de dados. Dessa forma, uma tecnologia que possa mitigar a possibilidade de que dados arquivados nos computadores ou na rede sejam acessados ilicitamente, utilizados para ameaçar ou fraudar, indubitavelmente poderá atenuar os delitos praticados através da internet.

Mesmo nos crimes que utilizam a tecnologia eletrônica como meio, condutas criminais nos quais os agentes utilizam métodos eletrônicos para obter um resultado ilícito, terão suas práticas dificultadas com o Blokchain. São os crimes informáticos impróprios, supracitados, nos quais o computador é a ferramenta para a execução do crime (VIANNA; MACHADO, 2013, p. 30).

Ainda quanto aos crimes informáticos que decorrem da invasão do dispositivo informático, o Blokchain representa uma possibilidade de atenuação da ocorrência desta modalidade de delito, pois cada vez mais os dados estarão disponíveis nos blocos de armazenagem na nuvem e serão, por consequência e por todo o exposto, mais seguros. Essas categorias de ilícitos provocadores de danos de natureza patrimonial ou moral e comumente praticados na internet, são modalidades de delitos informáticos que precisam ser combatidos. Fiorillo e Conte (2013, p. 238), citados, alertam para falhas de segurança que podem ampliar a magnitude dos crimes cometidos pela internet e a necessidade de se investir em tecnologias de em segurança, frente à prática de ilícitos é constante e causam prejuízos das mais diversas ordens.

Referências

ASCENÇÃO, José de Oliveira. *Direito da Internet e da sociedade da informação*. Rio de Janeiro: Forense, 2002.

BARRETO JUNIOR, Irineu Francisco. Atualidade do Conceito Sociedade da Informação para a pesquisa jurídica. In: PAESANI, Liliana Minardi (coord.). *O Direito na Sociedade da Informação*. São Paulo: Atlas, 2007.

_____. MARGATO, Luís Roberto Soares; QUEIROZ, Maurício Veloso. Eficácia dos Direitos Humanos na Sociedade da Informação. *Revista Constituição e Garantia de Direitos.* Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Norte. v. 7, n. 1, 2014, p. 1-15.

_____. Sociedade da informação e as novas configurações no meio ambiente do trabalho. *Revista Brasileira de Direito Ambiental*. V. 27, p. 251-262, 2011.

_____. Proteção da Privacidade e de Dados Pessoais na Internet: O Marco Civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells. In: DE LUCCA, Newton; SIMÃO FILHO; Adalberto; DE LIMA; Cintia Rosa Pereira. (Org.). *Direito & Internet III: Marco Civil da Internet.* 1ed.São Paulo: Quartier Latin, 2015, v. 2, p. 100-127.

BRASIL. MINISTÉRIO DA CIÊNCIA E DA TECNOLOGIA. *Livro Verde da Sociedade da Informação no Brasil*. Brasília: Ministério da Ciência e Tecnologia, 2000.

CASSEB, Paulo Adib. Democracia na Sociedade da Informação. *Revista do Curso de Direito da UniFMU*, São Paulo, *UniFMU*, v. 28, p. 5-12, 2005.

CASTELLS, Manuel. *A Era da Informação: economia, sociedade e cultura.* Volume I, a sociedade em rede. 5 ed., São Paulo: Paz e Terra, 2001.

CORRÊA, Gustavo Testa. *Aspectos jurídicos da Internet*. 2 ed. rev., São Paulo: Saraiva, 2002.

CORRÊA, Gustavo Testa. *Aspectos jurídicos da internet*. São Paulo: Saraiva, 2000.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto (coords.). *Direito e Internet: aspectos jurídicos relevantes*. Bauru, SP: Edipro, 2001.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. *Crimes do meio ambiente digital.* São Paulo: Saraiva, 2013.

FURLANETO NETO, Mario; GUIMARÃES, José Augusto Chaves. *Crimes na internet*: elementos para uma reflexão sobre a ética informacional. Direito da Informática, Brasília, p. 67-73, 2003. Disponível em: <http://www.cjf.jus.br/revista/numero20/artigo9.pdf>. Acesso em: 10 maio 2016.

FURLANETO NETO, Mario; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. *Crimes na internet e inquérito policial eletrônico.* São Paulo: Edipro, 2012.

LEMOS, André; LÉVY, Pierre. *O futuro da internet*: em direção a uma ciberdemocracia

planetária. São Paulo: Paulus, 2010.

LIMA, Paulo M. F. *Crimes de computador e segurança computacional*. Campinas: Millennium, 2005.

LIMA, Venício A. Sociedade da Informação, comunicações e democracia. *São Paulo em Perspectiva.* São Paulo, Fundação Seade, v.12, n.4, 1998.

MALIN, Ana. O mal-estar brasileiro na Sociedade da Informação. *São Paulo em Perspectiva.* São Paulo, Fundação Seade, v.12, n.4, 1998.

ORRICO JUNIOR, Hugo. *Pirataria de Software*. São Paulo: MM Livros, 2004.

PAESANI, Liliana Minardi; BAPTISTA, Ézio Carlos S. A privacidade na Sociedade da Informação: breves reflexões. *Revista do Curso de Direito da UniFMU*, São Paulo, *UniFMU*, v. 28, p. 13-24, 2005.

PINHEIRO, Patrícia Peck. *Direito digital.* 5. ed. São Paulo: Saraiva, 2013.

ROSA, Fabrízio. *Crimes de informática*. Campinas: Bookseller, 2002.

SANTOS, Coriolano Aurélio de Almeida Camargo; CRESPO, Marcelo Xavier de Freitas. *Crimes digitais e o Marco Civil da internet.* 2015. Disponível em: <http://www.ibccrim.org.br/tvibccrim_video/235-Crimes-digitais-e-o-Marco-Civil-dainternet>. Acesso em: 10 maio 2016.

SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*: de acordo com a Lei n. 12.965, de 2014 -Marco Civil da Internet. 2. ed. São Paulo: Saraiva, 2015.

VIANNA, Túlio; MACHADO, Felipe. *Crimes Informáticos*: conforme a Lei nº 12.737/2012. Belo Horizonte: Fórum, 2013.

WACHOWICZ, Marcos. *Propriedade intelectual do software e revolução da tecnologia da informação*. Curitiba: Juruá, 2005.