CONDUTAS NÃO ÉTICAS E TRANSGRESSORAS NA INVASÃO DE DISPOSITIVO INFORMÁTICO: APLICAÇÃO DA LEGISLAÇÃO DE REPRESSÃO AO CIBERCRIME.

GUSTAVO ABRAHÃO DOS SANTOS (Professor FATEC e Faculdade do Guarujá)
gustavo.abrahao@hotmail.com

EDUARDO TAGLIAFERRO (Professor Faculdade do Guarujá)
eduardo.tagliaferro@outlook.com

RESUMO

A ética nas relações sociais tecnológicas é a problemática desenvolvida aqui e que envolve as pessoas e empresas nos dias atuais. Como acreditar na verdade ou não das plataformas da internet ou informações que se propagam fora da rede. Alude-se aqui que as regras de comportamento sobre o mal uso de recursos informáticos, vem causando danos as pessoas e a gestão de empresas, bem como as ilicitudes estão aumentando, corroborando em prejuízos patrimoniais. Neste passo, aborda-se as regras legais para repressão ao cibercrime, tornando obrigatória padrões de comportamento às pessoas em suas relações cotidianas. Aborda-se que o *modus operandi* do crime cibernético e a autoria vem possuindo números significativos de prejuízos as pessoas e empresas, sendo coerente a aplicação da legislação que enfatiza a tipicidade do crime cibernético e a legislação do marco civil da internet. Contudo, as regras legais penais são brandas no Brasil, ilustrando-se que os meios de prova e o uso da tecnologia aliada a investigação dos delitos de invasão de dispositivo informático podem contribuir para desvendar autoria e coautoria destes crimes.

PALAVRAS-CHAVE: Ética. Legislação. Cibercrime.

ABSTRACT

Ethics in technological social relations is the problem developed here that involves people and companies in the present day. How to believe in the truth or not of the internet platforms or information that propagates outside the network. It is alluded to here that the rules of behavior about the misuse of computer resources have been causing damage to people and the management of companies, as well as the illicitudes are increasing, corroborating in patrimonial damages. In this step, we address the legal rules for repression of cybercrime, making patterns of behavior compulsory for people in their everyday relationships. It is approached that the modus operandi of cyber crime and authorship has significant numbers of damages to people and companies, being consistent the application of the legislation that emphasizes the typicity of the cyber crime and the legislation of the civil landmark of the internet. However, criminal legal rules are mild in Brazil, showing that the means of proof and the use of technology combined with the investigation of the crimes of invasion of computer devices can contribute to unravel the authorship and co-authorship of these crimes.

***Keywords**:* Ethic. Legislation. Cybercrime.

INTRODUÇÃO

Aqui se aborda a contextualização da ética e legislação aplicada a tecnologia, mais, precisamente, a repressão aos crimes cibernéticos como desafios na gestão e desenvolvimento da sociedade com a tecnologia. O tema refere-se a ética, moral e a prática de atos por pessoas e empresas com recursos informáticos e internet.

A situação problema que o texto aborda são as condutas éticas transgressoras com o uso de recursos tecnológicos, discussão e soluções.

Este estudo tem o objetivo de apresentar como a falta de ética nas relações sociais e empresariais que usam a informática e internet, colaboraram para o surgimento de regras legais, ilustrando-se a Lei do marco civil da internet que determina condutas de comportamento para pessoas e empresas , diante da falta de respeito delas com os princípios da liberdade, privacidade e segurança.

O objetivo geral do trabalho é apresentar como a ética se comporta na sociedade digital e os riscos que surgem com falta da ética e moral, passível de regras legais para tornar obrigatórias condutas de comportamento das pessoas e empresas com os recursos da tecnologia e internet.

O objetivo específico deste trabalho é ilustrar a tipicidade do cibercrime no Brasil, elencando seu surgimento na sociedade com o uso da tecnologia e internet, bem como o *modus operandi* do crime cibernético e autoria e coautoria do mesmo pelas pessoas e empresas, bem como afetações na gestão das empresas e na rede social virtual e presencial no Brasil, e ainda, apresentando as investigações que possam ser realidade aos crimes cibernéticos e o uso de tecnologia nestas investigações policiais de crimes informáticos.

A metodologia utilizada aqui foi revisão bibliográfica, exploratório e qualitativo ao tema ética e legislação para a repressão aos crimes cibernéticos, inserindo-se dados atuais sobre a afetação e dimensionamento destes crimes informáticos nas empresas e sociedade.

A estrutura desta pesquisa é na sua primeira parte, apresentar a ética como fundamental nas relações sociais com os recursos informáticos e de tecnologia, e que através dos anos, as condutas de comportamento na rede virtual, se tornaram um risco para a sociedade.

Na sequência, se apresenta que nas últimas décadas têm se visto uma tendência crescente para a ocorrência de crimes cibernéticos, sendo necessário conhecer seus conceitos legais, tipicidade, autoria e modus operandi.

E ao final, aborda-se como ocorre a investigação nos crimes informáticos, ilustrando-se um exemplo de recurso tecnológico que pode ser utilizado para a repressão do crime cibernético, otimizando gestão e tecnologia.

1 A INTERNET E A ÉTICA: SOCIEDADE IDEAL X SOCIEDADE DE RISCO.

Elucida-se, primeiramente, que as relações sociais e empresariais com o uso de recursos informáticos e a inserção de novas tecnologias e serviços de dados para a sociedade por meio de hardware e software, contribuem para alterações de comportamento no cotidiano das pessoas e empresas.

Segundo Fernandes (2013, p. 264) “a internet surgiu de forma inicialmente restrita, resultando da colaboração entre universidades e centros de investigação, mais ou menos próximos dos meios militares norte-americanos”.

Tais fatos são precursores da atual internet e da sua parte mais conhecida, a World Wide Web.

Segundo Fernandes (2013, p. 263), “computadores interligados surgiram na década de 60 do século XX, no contexto da competição da Guerra Fria, entre os EUA e a ex-União Soviética”.

Posteriormente, a rede mundial de computadores para Spencer Toth Sydow (2015, p. 29) foi “o principal passo dado pelo homem para intercomunicar aparatos, permitindo a troca de informação. Isso se deu com base na aceitação global de uma mesma linguagem adotada por todos os computadores, denominada protocolos TCP/IP”. Frisa-se que TCP/IP é a sigla que significa “Transmission Control Protocol/ Internet Protocol” ou “protocolo de controle de transmissão/protocolo de internet” e nada mais é do que uma série de mecanismos desenvolvidos para interconectar e compartilhar dispositivos através das redes.

Para Castells (2004), “a internet/web e a sociedade em rede eram o resultado de uma encruzilhada insólita entre a ciência, a investigação militar e a cultura libertária”.

Segundo Fernandes (2013, p. 264), “tudo isto sofreu profundas alterações quando, no início da década de 90, a internet foi retirada do controle militar passando a sua gestão para a National Science Foundation (nsf) dos EUA”.

Com a tecnologia para a criação de redes informáticas abertas ao domínio público e as telecomunicações em processo de liberalização, ocorreu a privatização da internet, competitividade e inovação.

Salienta-se o quanto importante foi o engenheiro britânico Tim Berners-Lee e os seus colegas do European Organization for Nuclear Research (Organização Europeia para Pesquisa Nuclear) na Suiça, pois desenvolveu um complexo sistema de documentos interligados que misturava texto, imagem, som e mídia e se inter-relacionava através da internet, por meio de ligações (links) que poderiam ser acionadas, levando o usuário conectado à internet a trafegar por diversos ambientes e plataformas diferentes, num ambiente visual mais rico e amigável. Essa tecnologia foi lançada em 1992 e conquistou os usuários por sua versatilidade, recebendo o nome de word wide web (larga teia mundial ou simplesmente web, e popularmente conhecida pelas letras “www” (SYDOW, 2015, p. 31).

Neste ponto, segundo Castells (2004, p. 34), a cultura da internet foi construída sobre a crença tecnocrática no progresso humano através da tecnologia, praticada por comunidades de hackers que prosperam num ambiente de criatividade tecnológica livre e aberta, assente em redes virtuais, dedicadas a reinventar a sociedade.

A partir daqui, o fornecimento de serviços de internet passou a ser uma atividade econômica empresarial, representada por empresas privadas que oferecem a sociedade uma dependência de aparatos informáticos e da internet.

Segundo FERNANDES (2013, p. 264), “as empresas privadas começaram a fornecer serviços de internet para uso empresarial ou privado”.

A cultura da internet se populariza e estabelece uma relação social entre as pessoas e empresas. Mas a internet se tornou uma sociedade ideal?

Ilustra-se que todos possuem as mesmas condições num meio em que condição social e aparência são irrelevantes. Todos são concomitantemente alguém e ninguém na rede. A internet, porém, é universal e inevitável. E neste passo, surgem as consequências nas relações sociais digitais, as condutas não éticas e transgressoras de regras.

Ilustra e conceitua a ética, o dicionário Aurélio Buarque de Holanda (2018), como sendo “estudo dos juízos de apreciação referentes à conduta humana suscetível de qualificação do ponto de vista do bem e do mal, seja relativamente a determinada sociedade, seja de modo absoluto”.

Segundo Herbert de Souza (1994, p. 13) a ética “é um conjunto de princípios e valores que guiam e orientam as relações humanas. Esses princípios devem ter características universais, precisam ser válidos para todas as pessoas e para sempre”

Logo, analisando-se o conceito acima, o objeto da Ética é a moral e esta é um dos aspectos do comportamento humano. Tanto a ética como a moral, se resumem em um conjunto de normas que regulam o comportamento humano, no meio em que vive. O conhecimento dessas normas se adquire através da educação, do estudo ou da vida prática no meio onde vive o indivíduo. Logo, o homem é um produto do meio onde vive.

Se o homem e as relações sociais das pessoas e empresas ocorrem por meio da internet, a partir da década de 90 do século XX, surgem transgressões as normas de comportamento humano balizadas em ética e moral nas relações sociais e empresariais com o uso da internet.

Frisa-se que a ética é o modo social de agir, ou seja possui característica coletiva. A moral é o modo pessoal de agir, ou seja, característica individual. Tanto a ética como a moral, se resumem em um conjunto de normas de convivência que regulam o comportamento humano, no meio em que vive.

Tendo em vista as transgressões as normas de comportamento humano por meio da internet ou com recursos informáticos, e o surgimento dos casos de “hackers” se apropriarem de dados privados, instalando vulnerabilidades e vírus em computadores, pirataria de programas, divulgação de dados e imagens sem autorização de pessoas e empresas, entre outros problemas de inovação e competitividade tecnológica, frisa-se que a posição da internet e aparatos informáticos não são mais uma sociedade ideal, mas uma sociedade de risco.

Salienta-se que a denominação sociedade de risco foi tecida inicialmente por Ulrick Beck, ao abordar a evolução industrial frente ao acidente com gases letais ocorrido em uma cidade da Índia em 1984, trouxe a ideia de que há uma verdadeira e necessária troca (trade off) por conta da evolução social (SYDOW, 2015, p. 38).

Neste ponto, o acesso a informações, vídeos, fotos, filmes, a potencialização da possibilidade de comunicação e a sensação de segurança fizeram com que houvesse massiva popularização da rede. Contudo, a evolução tecnológica trouxe consigo pessoas antiéticas e imorais, surgindo a sociedade de riscos.

De forma muito simples, ética trata da forma como as pessoas se relacionam.

E internet é mais uma forma desse relacionamento ocorrer.

Neste sentido, há pessoas que não fazem diretamente certos comentários, mas têm coragem de postar ofensas e agressões nas redes sociais da internet.

A sensação de anonimato e de invisibilidade no uso da internet é falsa, pois por meio do IP (PROTOCOLO DE INTERNET) é possível se descobrir de que máquina uma determinada ofensa foi publicada.

Neste sentido é o pensamento de Fugazza e Saldanha (2017,p. 92):

> A valorização da ideia de privacidade na ética informacional é caracteristicamente um valor moral que predomina nas culturas ocidentais, imbricada com os ideais democráticos que defendem os princípios de autonomia e liberdade. Quando

> adentramos as esferas políticas locais, percebemos o conjunto de problemas evocados pelo campo da ética no território das políticas de direito social e na participação cidadã crítica. Exemplo direto disto está na relação entre a atuação do Facebook e a Constituição brasileira, dentre outros confrontos éticos entre Mercado, Estado e Sociedade na contemporaneidade.

Com o advento da Lei do Marco Civil da Internet, por meio do artigo 2º da Lei Federal n. 12.965 de 2014, adveio no ordenamento legal, os princípios de ética para o uso da internet e tecnologia no Brasil, sendo eles: neutralidade da rede, privacidade dos usuários e liberdade de expressão.

Enfim, ao possibilitar o armazenamento, a transmissão e o processamento de informações em meios digitais, a internet torna-se onipresente no cotidiano das pessoas e empresas, e diante dos riscos a privacidade dos usuários e liberdade de expressão, as empresas de gestão da tecnologia, devem segundo a lei do marco civil da internet, respeitar a neutralidade da rede, ou seja, a segurança dos dados e informações, sendo estes os valores éticos preceituados pela Lei do Marco Civil da Internet, dando-se força a repressão ao cibercrime e suas inovações tecnológicas no *modus operandi* do crime informático, bem como otimizando a gestão empresarial.

2 A TIPICIDADE DO CIBERCRIME, MODUS OPERANDI E AUTORIA DAS CONDUTAS ILEGAIS.

A liberdade de se comunicar no Brasil está prevista como garantia fundamental de todas as pessoas no artigo 5º da Carta Magna de 1988, contudo, a falta de ética e moral com o uso da internet, propicia a violação de princípios da vida relacionados a honra, intimidade e privacidade dos dados das pessoas, e caracteriza desrespeito aos direitos constitucionais de liberdade de expressão, privacidade e intimidade da vida, bem como ao direito à segurança dos dados pessoais.

Com a evolução da internet, as comunicações dos usuários no país ficam mais propicias a vulnerabilidades, sendo eivadas de falta de ética e moral, quando da existência de riscos e ameaças na utilização de dados e imagens de pessoas, bem como divulgação por meios informáticos com conexão ou não a internet de dados privados, perante terceiros e sem autorização das vítimas.

A criminalidade na informática conduz a reflexão que a falta de ética e moral leva a necessidade de criminalizar, legalmente, as ações que utilizem computadores e internet e venham a ferir a liberdade, privacidade, segurança e o patrimônio das pessoas e empresas.

Nas palavras de Corrêa (2002, p. 42): “a internet é um paraíso de informações, e, pelo fato de estas serem riquezas, inevitavelmente atraem o crime. Onde há riqueza há crime”.

Lembrando que a lei é a única fonte do Direito Penal, quando se pretende proibir ou tornar obrigatórias condutas sob ameaça de uma penalização. Enfim, o que não estiver expressamente proibido é algo admissível no Direito Penal.

Segundo Paulo Marco Ferreira Lima (2011, p. 9) denomina-se “criminalidade informática todas as formas de comportamento ilegal que venham a, de qualquer forma, provocar danos sociais, por intermédio de um computador”.

Frisa-se a definição dos crimes informáticos de Ivete Serrise Ferreira (1992, p. 139), “toda ação típica, antijurídica e culpável contra ou pela utilização de processamento automático de dados ou sua transmissão”.

Logo, crime que utiliza a tecnologia da informação: computador e seus aparatos; Uso ou não da Internet; e conhecimentos em programação e análise de sistemas.

Neste passo, surgiu por meio da Lei Federal n. 12.737/2012 que insere a tipicidade dos crimes cibernéticos ou informáticos, alterando o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal brasileiro), preceituando como texto legal os artigos 154-A, 154-B e 266 e 298 no Código Penal.

Frisa-se que os crimes de Invasão de dispositivo informático ou crime cibernético são crimes cometidos contra os dados informáticos e sistemas de computadores privados ou públicos de pessoas ou empresas. A previsão do crime cibernético está no Artigo. 154-A do Código Penal Brasileiro. Senão vejamos:

> Art. 154-A. Código Penal. ‘Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita”.

Frisa-se o texto do parágrafo 1º do artigo 154-A do Código Penal:

> Art. 154-A. § 1º. Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

Frisa-se a posição da tipicidade no Código Penal, como sendo o artigo 154-A estar “anexado” ao artigo 154 que trata da violação do segredo profissional, artigo este que integra a Seção IV do Código Penal que trata dos crimes contra a inviolabilidade dos segredos.

Neste passo, o bem jurídico protegido pelo novo tipo penal é a intimidade, a vida privada, a honra e a imagem das pessoas, tendo em vista a tipicidade ser “a invasão de dispositivo informático”. Numerá-lo no artigo 154 é aproximá-lo da violação do segredo profissional, ou seja, a conduta de falta de ética na gestão das empresas, deixando em segundo plano a ideia de proteção pessoal e patrimônio.

Uma outra questão que se observa no crime cibernético é a pena. Demasiadamente, branda para este crime, contém previsão de 3 meses a 1 ano de detenção, mesmo com a existência de agravantes e atenuantes nos parágrafos do artigo 154-A do Código Penal.

Considerando que todo e qualquer ato na prática do crime informático, visa atingir o patrimônio, a honra, com ou sem conexão com a internet, ou ainda, instalar vulnerabilidades para obter vantagens ilícitas, a pena deveria ser mais severa.

Atualmente, de acordo com a SaferNet (2017), que controla a Central Nacional de Denúncias, mais de 115 mil denúncias envolvendo exclusivamente crimes contra direitos humanos foram recebidas e processadas no ano de 2016.

Segundo Adriana (2017, p;18) “os crimes envolvendo fraudes bancárias também não ficaram para trás”.

De acordo com TOZZETO (2010), a Federação Brasileira de Bancos (Febraban) divulgou que bancos brasileiros perderam R$ 1,8 bilhão só em 2015.

Segundo Adriana (2017, p.18) “estes crimes englobam desde o roubo de senhas, via ataques de phishing scam, até os kits boletos, exclusividade do Brasil”.

Enfatiza-se o que é phishing scam, segundo Alexandre Pontieri (2011):

> utiliza-se do envio de e-mails (correio eletrônico) para a caixa postal de diversos usuários. Esses e-mails normalmente vêm com a aparência de serem de grandes corporações, preferencialmente bancos, no qual informam sobre novos serviços, solicitando o preenchimento de dados pessoais. O que ocorre na verdade é que, ao acessar essas falsas páginas corporativas, o usuário estará sendo enganado, pois programas altamente sofisticados entrarão na sua máquina, apoderando-se de informações pessoais como, por exemplo, senha bancária - normalmente para aqueles que utilizam o serviço de internet banking

E os “Kits boletos”, segundo a Kaspersky Lab (2018), empresa especializada em segurança online:

> cada vez mais pessoas estão se tornando vítimas do chamado "golpe do boleto". A disseminação do ataque vem crescendo cada vez mais entre os criminosos, ainda mais com a possibilidade de comprar um "kit fraude" por apenas R$ 500, com todas as informações necessárias para se aplicar o golpe. Novos métodos estão sendo desenvolvidos por quadrilhas e hackers europeus para enganar as pessoas por meio da falsificação de boletos bancários. O objetivo do ataque é fazer com que os usuários paguem boletos falsos e assim transfiram dinheiro para contas de cibercriminosos. Falhas de roteadores, criação de servidores DNS e plugins maliciosos, injeção de códigos que contaminam o computador e muitos outros métodos são utilizados para aplicar o golpe, segundo estudo dos analistas da Kaspersky Lab.

Verifica-se que o *modus operandi* daqueles que violam as condutas de comportamento e chegam a cometer cibercrimes, oportunizam por meio da inovação tecnológica, as descrições a serem ressaltadas de forma mais específica a seguir.

2.1 *Modus operandi* dos crimes cibernéticos.

Importante elencar os *modus operandi* dos crimes cibernéticos, por meio de comportamentos antiéticos, imorais e ilegais de pessoas, frente a sociedade digital.

O primeiro comportamento antiético, imoral e ilegal é a intrusão informática que segundo Spencer Toty Sydow (2015, p. 114) é:

> Ingresso não autorizado de um usuário no sistema alheio, seja ou não para obter alguma vantagem, seja ou não por meios ardilosos, violentos, ou até mesmo por conta de um subterfúgio que venha a enganar o legítimo detentor dos direitos relativos ao sistema, levando-o a permitir o ingresso, sob erro.

Inicialmente, o delito de intrusão informática foi pensado que seria praticado pelos “conhecedores de informática” que atacariam sistemas fechados provocando verdadeiras quebras e aberturas de mecanismos de defesas (breakage), a partir do que obteriam uma via aberta para ingressar nos sistemas alheios. Contudo, não somente, há o uso do mecanismo de violação dos sistemas alheios para a obtenção do acesso. Assim, boa parte dos sistemas operacionais e programas de uso

corriqueiro são lançados no mercado com aquilo que se apelidou de bugs (falhas lógicas de programação). Tais falhas podem gerar brechas na segurança que levam à acessibilidade do sistema e de informações alheias por parte de usuários mal intencionados. Logo, os arquivos geram falhas e criam portas de acesso livre, dando oportunidade para vulnerabilidades na Backdoor (porta dos fundos).

Outro comportamento de *modus operandi* do crime cibernético é o furto de identidade visual que segundo Spencer Toty Sydow (2015, p. 117) “é a apropriação das características e identificações pessoais de outra pessoa para fazer se passar por este, sem que, contudo, tenha recebido autorização para tanto”.

No Brasil, o furto de identidade visual é denominado de "Fake”.

A anonimidade do ciberespaço faz com que cada usuário convida e interaja com outros sem nunca ter a certeza de quem são na vida real. Para diminuir esta insegurança e falta de ética e boa conduta de comportamento, os ambientes de inter-relação terminam por criar sistemas de identificação presumida em que cada interessado em acessá-los vê se obrigado a fornecer certos dados como, por exemplo, apelido, nome completo, endereço, números de identificação, contrassenha de acesso, endereço válido de e-mail, entre tantas outras informações que acabem por compor um delineamento de quem seja o usuário ”anônimo”. O “Fake” situa-se no crime previsto no caput do artigo 154-A do Código Penal, “invasão de dispositivo informático, conectado ou não à rede de computadores”.

Outro modus operandi de crime cibernético é a inserção de código Malicioso.

No pensamento de Spencer Toty Sydow (2015, p. 122-123) :

> Inserção de malware, contágio de dispositivo alheio ou sabotagem informática. Os códigos maliciosos são instruções inseridas em aparatos alheios por meio de arquivos que dão comandos que implicam algum prejuízo, seja na confidencialidade dos dados, seja na disponibilidade (até por perda de velocidade) ou, ainda, na integridade deles. São exemplos: vírus, os rotkis, os worms, os trojan horses, os keyloggers, os sreenloggers, os spywares e até algumas modalidades de Hardwares.

Os meios mais comuns de *modus operandi* para tipicidade dos crimes cibernéticos são o scamming e spamming.

Spencer Toty Sydow (2015, p. 125) diz: “scam representa a ação de defraudar; sendo um esquema fraudulento de negócios. São golpes, armadilhas, venda e negócios irregulares após invasão de dados informáticos”.

Tal modalidade, ocorre após alguém invadir o dispositivo informático, podendo dispor de agravantes do crime do caput do artigo 154-A do Código Penal.

Já o Spam seria a nomenclatura popular para o apelido dado às tais mensagens com cunho comercial que infestam as caixas de entrada dos programas de e-mail e que, tecnicamente, são denominadas UCM ou unsolicited comercial messages ou “envio de mensagens comerciais não solicitadas”. (...) Também são as UPM – Unsolicited pornographic messages – ou “mensagens pornográficas não solicitadas” (SYDOW, 2015, p. 129).

2.2 A autoria e coautoria nos crimes cibernéticos.

Apesar de a cada dia mais perceber-se que a criminalidade informática não exige indivíduos com características particulares, pois os diversos delitos

informáticos podem ser perpetrados com pouca habilidade, ainda assim temos um delinquente com poder aquisitivo, boa quantidade de conhecimento de informática, especialmente, naqueles delitos que envolvem programação e intrusão.

Neste sentido, Spencer Toty Synow (2015, p. 142), afirma:

> É de se concluir que ainda não se pode dizer que há um perfil biológico para um delinquente informático, mas é certo que somente pessoas com certo poder aquisitivo, certa educação para língua estrangeira e considerável capacidade de digitação são capazes de se mostrarem proficientes para a prática de boa parte dos delitos que exigem capacidade técnica.

No país, a autoria e coautoria dos crimes cibernéticos já atingem 42 milhões de brasileiros. Segundo o sítio eletrônico do jornal Estadão (2017), consta a informação que o Brasil ocupa lugar de destaque no cenário global de cibercrimes. Em 2016, 42,4 milhões de brasileiros foram vítimas de crimes virtuais. Em comparação com 2015, houve um aumento de 10% no número de ataques digitais. Segundo dados da Norton, provedora global de soluções de segurança cibernética, o prejuízo total da prática para o país foi de US$ 10,3 bilhões.

Infelizmente, outro dado importante é que o Brasil não ratificou a Convenção Internacional sobre o Cibercrime de 2001.

Enfim, os conceitos dados sobre cibercrimes, justificam-se e explicitam-se de que forma poderão ser investigados tais crimes, abordando-se como resultados, o uso da tecnologia para a investigação dos *modus operandi* destes cibercrimes.

3 A TECNOLOGIA NA INVESTIGAÇÃO DOS CIBERCIRMES

Depois da apresentação da ética na sociedade digital, tipicidade, *modus operandi* e autoria dos crimes cibernéticos, apresentam-se os resultados de como a tecnologia pode ser aliada no combate a repressão destes crimes informáticos.

Segundo Adriana Shimabukuro (2017, p. 19):

> identificar o criminoso cibernético é tão desafiador quanto identificar um criminoso por suas digitais. Se antes os policiais buscavam dados em bancos de digitais, agora estes dados estão em gigantescos arquivos que guardam o IP do usuário de Internet. O IP, ou Internet Protocol, é um número que um computador ou equipamento conectado à Internet recebe. Combinado a uma data e um horário, é possível localizar um usuário da Internet em qualquer parte do mundo. Temos duas versões de IP, a versão 4, utilizada desde 1981 e que está sendo migrada para a versão 6, disponível desde 1999. Veja, a seguir, exemplos de endereços IP nas duas versões. IPv4: 201.199.244.101 e IPv6: FEDC:2D9D:DC28:7654:3210:FC57:D4C8:1FFF.

Importante frisar que a lei do marco civil da internet, ora Lei Federal nº 12.965 de 2014, é um instrumento legal que ajuda nos desdobramentos da tecnologia na investigação dos cibercrimes.

Neste ponto, Adriana Shimabukuro (2017, p. 22):

> A investigação cibernética traz novos agentes: os provedores de conexão e provedores de aplicação. O Marco Civil da Internet tornou obrigatório aos provedores guardar informações

> de usuários que utilizaram determinado serviço, bem como a data e a hora em que a conexão foi realizada. Apesar de existirem questões quanto ao direito de privacidade, a obtenção destas informações é fundamental para a resolução de crimes. Os registros de acesso permitem rastrear e identificar onde surgiu determinada conduta ilícita; são fornecidos somente mediante ordem judicial. Os registros de serviço podem apontar a divulgação ou compartilhamento de conteúdo criminoso

E mais, o artigo 5º da Lei do Marco Civil da Internet, demonstra que há uma compreensão do fenômeno sociológico da rede que supera a limitada conceituação de internet como um ambiente acessível apenas por computadores.

Spencer Toty Sidow (2015, p. 275) diz “nessa toada, a norma utiliza-se da ideia de terminal e demonstra que qualquer dispositivo deve necessariamente ser considerado como potencial para as condutas praticadas no meio virtual”.

Numa investigação dos crimes cibernéticos, as principais evidências estão em inúmeros dispositivos, como computadores, telefones celulares, pen drives, máquinas fotográficas, provedores de Internet, registros de equipamentos de infraestrutura de rede (roteadores, firewalls, web servers, servidores de e-mail, etc.).

E assim, as provas podem ser as mais diversas possíveis: arquivos digitais, registros de servidores, cookies, o histórico de navegadores, fotos ou vídeos, e-mails e registros de conversas on-line.

Neste ponto, os dados estáticos são basicamente registros que um usuário tem na rede, já dados dinâmicos são dados de navegação, conversas, registros de dowloads, logs, sendo estes previstos na lei do marco civil da internet e limitados a serem cedidos apenas com autorização judicial (SIDOW, 2015, p. 276-277).

Uma das formas que a tecnologia pode estar aliada na investigação dos cibercrimes é o hash, técnica para criar uma identificação única para cada tipo de arquivo que é disponibilizado na rede e que segundo Adriana Shimabukuro (2017, p. 26), trata-se basicamente de uma “sequência única de letras e números que, gerados por algoritmos matemáticos, servem para verificar a integridade de um arquivo, armazenar senhas e, neste caso, buscar um determinado arquivo em uma grande base de dados”. Vejamos o Hash na figura abaixo:

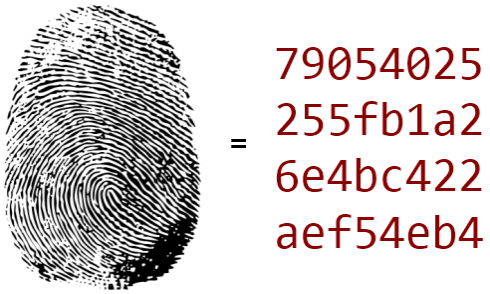

Figura 1: Algoritmos matemáticos geram a identificação única de qualquer arquivo digital. Fonte: Disponível em: <https://blog.codinghorror.com/speed-hashing/>. Acesso em: 03 nov. 2018.

O hash é um importante método para rastrear informações criminosas na rede mundial de computadores, principalmente as imagens de delitos bancários e pornografia infantil. Importantes operações da Polícia Federal foram deflagradas e permitiram localizar e identificar pedófilos que compartilhavam esse tipo de material na Internet.

Enfim, os resultados indicam que os meios de provas com a ajuda da legislação do marco civil da internet e a investigação com uso de tecnologia podem identificar a autoria e/ou coautoria dos crimes cibernéticos, bem como o *modus operandi* a tipificar o delito informático.

CONSIDERAÇÕES FINAIS

Evidencia-se que o tema delimitado possui uma abrangência bem maior que a apresentada neste trabalho, mas o recorte da ética e legislação aplicada no cibercrime, tão somente, no cenário nacional, teve o condão de ilustrar que as regras legais existem para conter as condutas ilícitas com o uso dos recursos informáticos no cotidiano das relações sociais e empresariais, existindo, ainda, muitos desafios na gestão e desenvolvimento tecnológicos para a sociedade da informação.

Certo é que ao aprovarem no Congresso, o texto da Lei n.12.737/2012 que insere o crime cibernético como tipicidade no Código Penal, não ofereceram repressão ao cibercrime, pois a pena sendo muito branda, as ações criminosas de invasão de dispositivo informático e suas consequências ilícitas continuam a atingir milhões de brasileiros, restando demonstrado em dados numéricos nesta pesquisa.

Conforme mencionado da literatura de revisão bibliográfica, observado restou que o *modus operandi* dos crimes cibernéticos vem atribuindo riscos e prejuízos econômicos em grande demasia aos dados informáticos dos cidadãos e pessoas jurídicas, violando condutas pessoais e prejudicando a gestão de empresas no país.

Portanto, na falta de ética, a legislação para repressão do cibercrime não sendo eficiente no Brasil, a tipicidade deste delito continua causando prejuízos.

Sugere-se, portanto, um estudo mais aprofundado da legislação brasileira para conter o cibercrime, tornando a legislação nacional atualizada com o restante da legislação internacional, prevista na Convenção do Cibercrime de 2001, sendo ela, uma norma internacional que o Brasil não a ratificou no seu território nacional.

Enfim, a investigação e os meios de prova para a repressão ao cibercrime possuem uma abordagem bem mais ampla que este trabalho, mas o que se demonstra é a possibilidade de melhorar os aparatos de defesa de dados informáticos, e assim, proteger direitos íntimos da honra e vida privada, liberdade de comunicação, segurança de dados e patrimônio das pessoas e empresas, por meio do aperfeiçoamento de regras da Lei do marco civil da internet, balizando condutas éticas para pessoas e gestão de empresas.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil. Brasília, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm>. Acesso em: 02 nov. 2018.

_____. Lei nº 12.737/12, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de1940 - Código Penal; e dá outras providências: Brasília, 2012.

_____.Lei nº 12.965/14, de 23 de abril de 2014. Estabelece princípios éticos, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 04 nov. 2018.

CASTELLS, Manuel. **A Galáxia Internet: Reflexões sobre Internet, Negócios e Sociedade.** Lisboa, Fundação Calouste Gulbenkian.2004.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 2002

FERREIRA, Aurélio Buarque de Holanda. **Novo Aurélio Século XXI: o dicionário da língua portuguesa.** 3 ed. totalmente rev. e ampl. Rio de Janeiro: Nova Fronteira, 1999.

FERNANDES, José Pedro Teixeira. **Da utopia da sociedade em rede à realidade da sociedade de risco.** Revista do Instituto de Ciências Sociais da Universidade de Lisboa, Análise Social, número 207, volume XLVIII, segundo trimestre, 2013.

FERREIRA, Ivete Serrise. Estudos jurídicos em homenagem a Manuel Pedro Pimentel. Ed. Revista dos Tribunais-SP. 1992, p.139.

FUGAZZA, Grace Quaresma e SALDANHA, Gustavo Silva. **Privacidade, ética e informação: uma reflexão filosófica sobre os dilemas no contexto das redes sociais.** Revista eletrônica de biblioteconomia e ciência da informação, v. 22, n.50, p. 91-101, set./dez., 2017.

Jornal Estadão**. Crimes virtuais afetam 42 milhões de brasileiros.** Disponível em: <https://economia.estadao.com.br/noticias/releases-ae,crimes-virtuais-afetam-42-milhoes-de-brasileiros,70001644185>. Acesso em: 03 nov. 2018.

Kaspersky Lab. **Definição de Kits boletos.** .Disponível em: < https://canaltech.com.br/seguranca/Golpe-do-boleto-tem-crescido-na-Internet-e-kit-para-fraude-e-vendido-por-R-500/ >. Acesso em: 03 nov. 2018.

LIMA, Paulo Marco Ferreira Lima. **Crimes de Computador e Segurança Computacional.** Editora Millennium. 2011.

PONTIERI, Alexandre. **Phishing Scam: nova modalidade criminosa na Internet** . Disponível em: <http://www.lfg.com.br - >. Acesso em: 20 mar. 2018.

SAFERNET**. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos**. Disponível em: <http://indicadores.safernet. org.br/>. Acesso em: 02 nov. 2018.

SOUZA, Herbert de. **Ética e cidadania.** São Paulo: Moderna, 1994.

SYDOW, Spencer Toty. **Crimes Informáticos e suas Vítimas.** Saraiva, 2ªed. 2015.

TOZETTO, Claudia. **Cibercrime faz bancos perderem 1,8 bilhão**. Disponível em: <http://link.estadao.com.br/noticias/cultura-digital,cibercrime-faz-bancos-perderem-r-18- bilhao,10000028721>. Acesso em: 03 nov. 2018.