Data de aprovação: 11/12/2020

CRIMES VIRTUAIS: UMA ANÁLISE SOBRE AS DIFICULDADES DO ESTADO NA PERSECUÇÃO PENAL

MANOEL GUILHERME DOS SANTOS DE CASTRO LIMA 1

JOÃO BATISTA MACHADO BARBOSA 2

RESUMO

O estudo destaca, em conjunto com a importância e a evolução da internet, o surgimento de pessoas que fazem o uso dos meios virtuais para cometerem atos ilícitos podendo afetar financeira e psicologicamente os demais usuários da rede. Este artigo tem como principal objetivo abordar, conceituar e caracterizar os crimes virtuais e os meios utilizados para cometê-los. A partir de uma pesquisa bibliográfica, cuja abordagem é explicatória sobre o tema, entrará em destaque, também, as dificuldades do Estado na persecução penal e no combate aos crimes cibernéticos no âmbito das redes sociais, plataformas de compartilhamento de vídeo entre outros meios. Deste modo, é imprescindível a decretação de lei específica, que venha complementar as vigentes, a fim de que proteja os usuários e puna os infratores.

Palavras-chave: Crimes virtuais. Meios Virtuais. Persecução Penal.

VIRTUAL CRIMES: AN ANALYSIS ON THE DIFFICULTIES OF THE STATE IN CRIMINAL PERSECUTION

ABSTRACT

The study highlights, together with the importance and evolution of the internet, the emergence of people who use virtual means to commit illegal acts that can affect the other users of the network financially and psychologically. This article has as main

[1] Acadêmico do Curso de Direito do Centro Universitário do Rio Grande do Norte – UNI-RN. Email: mguilherme.castro@gmail.com

[2] Professor Orientador do Curso de Direito do Centro Universitário do Rio Grande do Norte – UNI-RN. Email: jbmb@unirn.edu.br

objective to approach, conceptualize and characterize virtual crimes and the means used to commit them. From a bibliographic research, whose approach is explanatory on the subject, the difficulties of the State in criminal prosecution and in the fight against cyber crimes in the scope of social networks, video sharing platforms and other media will also be highlighted. Thus, it is essential to enact a specific law, which will complement those in force, in order to protect users and punish violators.

Keywords: Virtual crimes. Virtual Media. Criminal persecution.

1 INTRODUÇÃO

A era da informação traz consigo o desenvolvimento tecnológico nos computadores seja no âmbito profissional ou pessoal, a cada ano que se passa é notável a evolução exponencial da capacidade de armazenamento e processamento de dados, além da compactação dos elementos físicos dos computadores. Esta era, mais conhecida como o período pós Era Industrial, teve suas bases realmente fundadas no século XX, mais precisamente na década de 70 com a invenção do microprocessador.

É sabido que o surgimento e evolução tecnológica trouxeram benefícios para o convívio em sociedade propiciando uma facilidade na comunicação, no mercado financeiro, entre outras benesses, mas vale ressaltar que também há problemas de diversas ordens a serem discutidas como: a “Era da Desinformação”, termo criado por Kanitz (Revista Veja, 2007) para determinar a possibilidade de qualquer pessoa ter a liberdade de expressar sua opinião, muitas vezes sem nenhum embasamento teórico, gerando conteúdo sem significado ou até distorção de informações sérias.

A partir daí podemos chegar às questões ligadas ao funcionamento e segurança dos sistemas da Tecnologia da Informação (TI). Em todas as áreas de nossas vidas necessitamos fazer uso de algum meio tecnológico, seja no trabalho ou em casa, nisso ficamos sujeitos a registros de dados pessoais no banco de dados das TIs, sendo assim, em razão dessa vinculação, estamos expostos a condutas ilícitas que prejudicam de diversas formas as pessoas, assim como pode prejudicar a economia de uma nação inteira. Pensando nisso, surgem os questionamentos:

Qual é a importância da evolução das TIs e da internet? Por que os crimes virtuais vêm acontecendo com tanta frequência? Como identificar um crime virtual? As leis existentes são suficientes para o combate efetivo desses delitos?

Os crimes virtuais envolvem ações de pronto desenvolvimento, tornando-se assim um grande problema. É de conhecimento de todos, que com a evolução da internet também há uma evolução dos infratores que atuam nela. Sendo assim, é necessário o desenvolvimento de uma fiscalização mais rigorosa ou normas mais severas para que ocorra uma diminuição na incidência desses crimes.

Deste modo, o presente artigo tem como objetivo central identificar os tipos de crimes virtuais, as limitações e as possibilidades existentes na legislação, promovendo uma reflexão e análise sobre a melhoria das formas de fiscalização para que se possa identificar os infratores e aplicar uma punição coerente com o ato ilícito cometido. Por fim, o trabalho foi constituído por meio da pesquisa bibliográfica e apresentará as informações colhidas de forma descritiva, com a intenção de poder proporcionar um melhor entendimento ao referido tema.

2 SURGIMENTO, EVOLUÇÃO E IMPORTÂNCIA DA INTERNET

2.1 INTRODUÇÃO

Sabemos que a internet é uma vasta rede que interliga vários computadores, celulares e mais diversos dispositivos de todo o mundo, tornando possível uma comunicação rápida e fácil. Mas surge uma questão, de onde e como surgiu a internet?

É possível afirmar que a internet surgiu em meados da década de 60, no ambiente da Guerra Fria (1945 – 1991), onde os Estados Unidos da América e a União Soviética, grandes potências mundiais, se dividiam nos blocos socialistas e capitalistas e disputavam a supremacia e poderes.

Com a intenção de tornar fácil a comunicação, temendo ataques soviéticos, algumas universidades norte-americanas se uniram para desenvolver um sistema de compartilhamento entre pessoas que se encontravam distantes umas das outras, para viabilizar a articulação de estratégias de guerra, daí surgiu a ARPANET (Advenced Research Projects Administration – Administração de Projetos e Pesquisas Avançados).

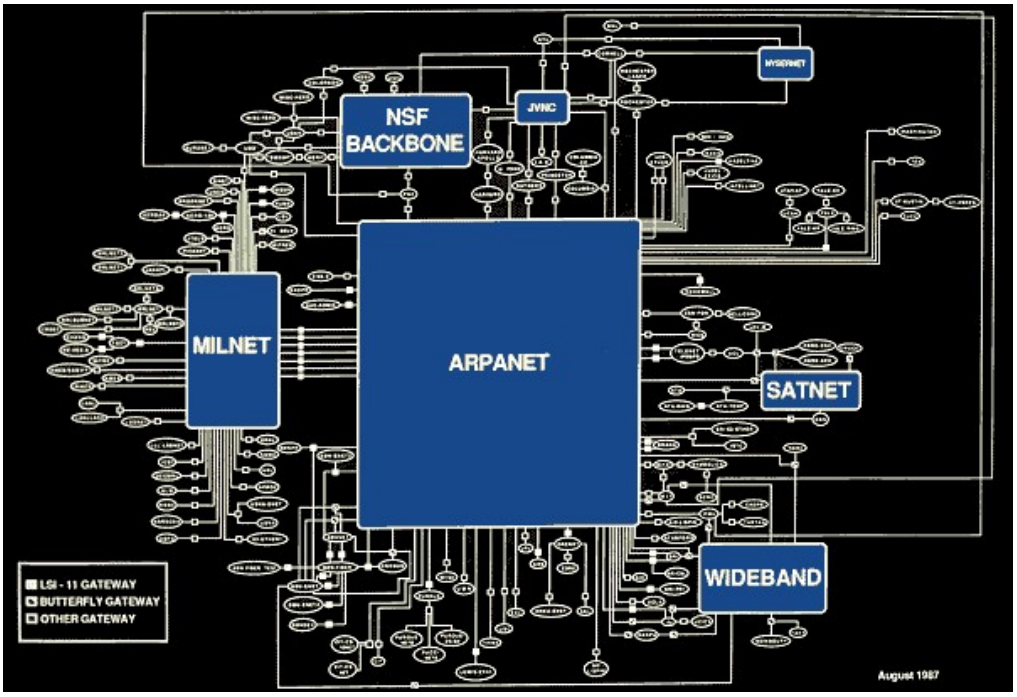

Figura 1 – Internet em um chip
Fonte: *An Atlas Of Cyberspaces*[3]

No dia 29 de outubro de 1969 foi estabelecida a primeira conexão entre o Instituto de Stanford e a Universidade da Califórnia, se tornando um momento marcante para a história, tendo em vista que o primeiro e-mail foi enviado.

O tempo passou e na década de 90 a internet se tornou cada vez mais popular em todo o mundo, com o surgimento de novos navegadores e browsers a década ficou conhecida como o “boom da internet”. Através disso foram surgindo diversos sites, redes sociais e afins, possibilitando uma expansão rumo à globalização. Alguns cientistas e curiosos acreditam que o surgimento e evolução da internet foram um marco fundamental para o progresso da tecnologia.

No Brasil, a internet surgiu no final da década de 80 com o primeiro contato de algumas universidades brasileiras com os Estados Unidos da América (EUA). No entanto, apenas em 1989, quando foi fundado a Rede Nacional de Ensino e Pesquisa que o projeto ganhou visibilidade e força. Após alguns anos, em 1997, mais precisamente falando, foram criadas as redes nacionais de conexão onde ocorreu uma grande expansão do acesso.

[3] Este mapa interessante mostra o estado do núcleo da internet em agosto de 1987. Versão colorida disponibilizada por Craig Partridge.

2.2 CRIMES VIRTUAIS E SUAS CLASSIFICAÇÕES

Basicamente toda evolução traz consigo benefícios, mas com ela também surgem os riscos. Não seria diferente com a internet. É de conhecimento de todos que o seu surgimento trouxe desenvolvimento e evolução do meio tecnológico, mas vale lembrar que também fez surgir os crimes cibernéticos.

Com a ampliação do uso da internet, surgiu a preocupação com a segurança de seus usuários. Apesar de antigo, o termo “cibercrime” só surgiu em meados da década de 90, em uma reunião do G-8, onde tinham como assunto central o combate de atitudes ilícitas no meio virtual, planejando uma maneira de deter e punir quem cometesse tal ato.

Assim como a internet passou por processos de aperfeiçoamento, os agentes criminosos que atuam através dela também, criando novas formas que permitam que ajam sem serem pegos. Com o número crescente de usuários, que já ultrapassa a marca de três bilhões, se torna ainda mais difícil identificar o infrator o que acaba por se tornar um estímulo para que se cometam ainda mais crimes e que surjam mais e mais criminosos.

Poucas pessoas têm total consciência dos riscos que correm ao acessar um e-mail, uma mensagem em rede social ou ao clicarem em uma propaganda. É possível que por ser um problema relativamente recente, as pessoas não tenham a noção do quão importante é proteger seus computadores e eletrônicos dos quais fazem uso diariamente e muito menos chegam ao conhecimento das classificações dos crimes eletrônicos.

Segundo Carlos Alberto Rohmann (2005), existe dois tipos de crimes eletrônicos, os que utilizam os computadores como meio para prática criminosa e aqueles quem tem como finalidade o próprio computador. O cybercrime ou crimes da informática são classificados de diversos modos, para Damásio de Jesus, por exemplo, são classificados como: próprios, impróprios, mistos e mediatos. Os crimes próprios são aqueles que são praticados somente com a utilização de sistemas operacionais ou de computadores, como, por exemplo, a criação de vírus.

Os crimes impróprios são aqueles que estão tipificados na legislação vigente e fazem o uso de computadores para a execução do ato, são, por exemplo, os “velhos crimes” com um novo *modus operandi*, por exemplo, assédio sexual, racismo e estelionato.

Como explica Damásio de Jesus (2016, p. 52):

> Os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

Os crimes virtuais mistos são aqueles que a legislação protege em dois âmbitos, ou seja, protege o bem informático e o bem jurídico. E o último, o crime mediato são delitos praticados com a intenção de chegarem a outro fim, citando caso análogo, é quando uma pessoa utiliza da tecnologia para roubar dados de vítimas e acessar sua conta bancária.

As classificações são de extrema importância por viabilizar a identificação e o entendimento de qual crime está sendo cometido e qual enquadramento será adequado para cada ato infracional, ainda assim, é difícil acompanhar e caracterizar as classificações devido à evolução constante que esse meio apresenta.

Martins (2012, p.78) leciona que:

> Destarte, o mundo cibernético tem sido alvo da atuação crescente de criminosos, que encontram na internet um meio fácil de cometer crimes, muitas vezes, aproveitando-se do anonimato, o que é vedado pela Constituição Federal, e da falsa impressão de que são impunes, ou pela falta de legislação específica, ou pela dificuldade na investigação criminal em encontrar os autores. É importante ressaltar que os usuários facilitam muito a prática destes ilícitos, tornando-se presas fáceis, pois ao acessar informações bancárias utilizando dados sigilosos, bem como a exposição da imagem, sem os devidos cuidados, acabam por favorecer a criminalidade cibernética.

2.3 SUJEITO ATIVO E PASSIVO

Os crimes virtuais representam, sem dúvida alguma, um novo modelo no Direito Penal. É notável que os Organismos Internacionais e os Estados estejam buscando considerar todos os vieses da criminalidade informática, sendo a imputação do crime e sua confirmação difícil devido a ausência do sujeito ativo, um fator que impede a identificação do autor, surge a necessidade de classificar esse perfil. Deste modo, as pessoas que praticam crimes cibernéticos são denominadas como *hackers* ou *crackers.*

O *Hacker*, em síntese, é aquele que invade sistemas em benefício próprio, tendo acesso a dados e informações de terceiros, mas sem que cause dano ao

dispositivo. Ele usa o seu conhecimento para achar brechas no sistema obtendo, assim, o poder de executar ações que podem ser positivas ou negativas. Nem todo hacker, como muitos imaginam, tem o intuito de prejudicar alguém ou alguma empresa, alguns chegam a se auto-intitular de "*hackers* do bem", porque, ao invadirem um computador, deixam uma mensagem para a vítima expondo a fragilidade e dando recomendações para o reparo da mesma.

Os *Crackers* são os verdadeiros criminosos do mundo cibernético, o seu maior objetivo é causar dano ou obter informações ilegais, destruindo sites e atingindo reputações de empresas. Também são considerados ladrões, pois consegue invadir computadores interligados a rede para roubar dinheiro e informações. São considerados fanáticos por vandalismo.

Os *Carders* recebem esse nome por realizarem compras com cartões de créditos gerados por programas ou de outras pessoas, eles invadem os computadores de administradoras de cartão, extraindo e distribuindo os números; assim várias pessoas podem ter acesso, dificultando ainda mais a identificação do infrator.

Os *Lammers,* diferentemente dos outros já mencionados, não detêm tanto conhecimento quanto imaginam ter. Eles acreditam que são excelentes e que possuem um conhecimento tão amplo, que seriam capazes de invadir qualquer site ou sistema operacional, mas não passam de novatos.

Os *Wannabes*, não são detentores de um vasto conhecimento nesta área, são pessoas que aprenderam um pouco sobre como invadir contas, computadores e afins, mas não são capazes de fazer muito mais que isso. O que os torna diferente dos *Lammers* é que eles têm consciência que são apenas amadores.

Por fim, os *Phreakers*, esses são os especialistas em telefonia. Eles usam o seu conhecimento para realizarem ligações gratuitas e escutas, vale ressaltar que essas escutas são feitas através de um mecanismo no computador, que o permite, quando o telefone toca, ouvir toda a conversa.

O sujeito passivo é qualquer pessoa que tenha acesso a um documento ou informações violadas ou arquivos confidenciais.

2.4 OS CRIMES VIRTUAIS MAIS RECORRENTES

Os crimes virtuais podem acontecer de duas maneiras: A primeira pode ocorrer de um agente ou infrator faz o uso do computador com a intenção de cometer um ato criminoso e a segunda pode ocorrer pelas ações de usuários contra outros já tipificados no Código Penal.

O computador é o meio principal para que se cometa esse tipo de crime, sem ele não haveria possibilidade de existir o *cibercrime.* A internet é uma forma de comunicação regulada pela ANATEL (Agência Nacional de Telecomunicações), desta maneira é competência da União, sendo classificado como serviço de telecomunicação, amparada pela Constituição no seu artigo 21, inciso XI.

O Código Penal, em seu Art. 6º, especifica o local do crime, mas quando se trata do crime virtual, não é possível definir apenas um local, tendo em vista que ele transcende os limites territoriais físicos. Com a criação do ciberespaço, também surgiu pareceres sobre o tempo e espaço, gerando empecilhos para aplicação correta e eficaz da lei penal.

Nesse cenário, é de grande valia que se possa classificar e conhecer os métodos que são mais utilizados pelo criminoso virtual. Alguns desses métodos são: o *phishing*, o trojan e a engenharia social.

2.4.1 O *Phishing*

O *phishing,* que significa pescaria, é uma técnica muito comum entre os cibercriminosos. Ela consiste em envios de e-mails não solicitados para a vítima contendo vírus ou de maneira que a incentive a acessar links e preencher formulários, assim, possibilitando o acesso do criminoso a informações das quais poderá fazer uso para extorquir dinheiro ou acessar contas bancárias.

2.4.2 O *Trojan*

É um dos vírus mais conhecidos. Ele se infiltra no computador através de jogos, downloads de música ou de vídeo, entre outros meios. Instala-se no computador de modo que a vítima não perceba a presença dele e age por meio de funções como a *keyloggers* – ferramenta que captura todas as execuções feitas pelo o usuário, como digitar e clicar – que acaba favorecendo a obtenção de informações para o infrator.

2.4.3 A Engenharia Social

O criminoso se vale da confiança da vítima para cometer o ato ilícito. Normalmente ele se disfarça como outra pessoa ou instituição e vai adquirindo a confiança da vítima até que ela lhe entregue alguma informação que possa usar em proveito próprio e passa a explorar o padecente a partir disso.

É válido lembrar que além dessas modalidades do crime virtual existem muitas outras que afetam diretamente a vida da vítima, seja psicologicamente ou financeiramente. Podemos citar: o cyberbullying, crimes contra honra, entre outros.

De acordo com Cassanti (2014, p.35), o cyberbullying é definido como:

> A ação intencional de alguém fazer uso das tecnologias de informação e comunicação para hostilizar, denegrir, diminuir a honra ou reprimir consecutivamente uma pessoa. Contrário do tradicional e não menos preocupante bullying, que é presencial, ou seja, as ações do agressor têm lugar certo, no cyberbullying o agressor não consegue presenciar de forma imediata os resultados da sua ação, minimizando um possível arrependimento ou remorso.

2.5 LEGISLAÇÕES NACIONAIS PERANTE OS CRIMES VIRTUAIS

A cada dia que se passa, se torna mais frequente relacionar o Direito e a Informática, alguns chegam a afirmar que deveria ser criado um novo ramo jurídico. Afinal, diariamente esses criminosos buscam novas maneiras de cometer esses crimes, formulando novos vírus, métodos para invadir computadores e outras diversas formas. Deste modo, é necessário que a lei também fique em constante atualização.

Os crimes virtuais podem ser cometidos de qualquer lugar do mundo, de diversas formas e meios, por exemplo, através de smartphones, smart tv e outros dispositivos informáticos. Diante da globalização promovida por estes dispositivos eletrônicos, torna-se difícil determinar uma norma universal competente para julgar, não havendo uma legislação especifica para esse tipo de crime, no âmbito internacional.

Para os atos ilícitos do meio virtual cometidos em território brasileiro, o Código de Processo penal afirma que:

> Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.
> § 1o Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.
> § 2o Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.
> § 3o Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção.

Pode-se dizer que a legislação brasileira já possui uma abrangência sobre os crimes virtuais mais comuns. Mas retomando um pouco da história no que se refere a legislação nacional, a criação do Plano Nacional de Informática e automação realizado através da Lei 7.232 de 1984, que se referia as diretrizes da informática em território brasileiro, é considerado um dos primeiros atos legislativos tomados no Brasil. Logo em seguida foi elaborada a Lei 7.646 de 1987 sendo revogada para a Lei 9.609 de 1998 tornando-se a primeira lei a descrever em seu ordenamento as infrações de informática.

Mesmo não possuindo muitas leis específicas e punitivas para os cibercrimes, existem artigos no Código Penal que tipificam condutas relacionadas a esses atos ilícitos. Podemos citar como exemplo o artigo 139 do Código Penal que prevê pena de detenção de três meses a um ano e multa pelo crime de difamação ou contra honra, sendo admitida a consumação do crime pelo meio virtual ou físico, ele será punido da mesma maneira.

Grande parte dos crimes não é denunciada ou divulgada pelas empresas e pessoas físicas, às vezes por receio de vir a acontecer novamente expondo essa fragilidade, deixando o infrator na impunidade. Apesar de o Código Penal já ser hábil em punir certas condutas praticadas no meio tecnológico, sendo capazes de punir crimes de plágio, crimes patrimoniais ou contra honra a falta de leis mais específicas ou delegacias que tratem desse assunto, acabam deixando as vítimas se sentindo inseguras, o que reforça ainda mais a necessidade de profissionais adequados e leis mais severas.

Diante dessa falta no ano de 2012 entraram em vigor as Leis 12.735 e 12.737, onde surgiu a possibilidade de concretizar a responsabilização do agente infrator que invadem contas ou dispositivos para roubar dados.

A Lei 12.735 regulamenta a Polícia Judiciária da seguinte maneira:

> Art. 4o Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.
> Art. 5o O inciso II do § 3o do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação: “Art. 20. II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;

Já a Lei 12.737, durante o período de sua criação a atriz Carolina Dieckmann teve seu dispositivo de computador invadido e fotos de cunho íntimo vazadas na internet, tendo ocorrido este fato a lei ficou conhecida com o nome da atriz. A lei trata de tipificar os delitos virtuais de invasões de dispositivos informáticos, perturbação ou interrupção de serviços telefônicos, telegráficos, informáticos ou de informações de utilidade pública e da falsificação de cartões ou documentos particulares, como RG e CPF. Além dos já citados, também tipifica outras condutas que não estavam previstas no Código Penal.

Apesar de ser considerado um avanço por muitos, causou descontentamento em outros. Sendo uma lei muito restrita, diante das formas diversas de cometer crimes virtuais, acaba por causar ambiguidade e confusão entre os peritos, juristas e profissionais em segurança da informação. O desagrado também teve como origem as baixas penas aplicadas, podendo algumas situações ser encaixadas nos Juizados Especiais, contribuindo para ineficácia na inibição dos crimes virtuais.

Há outras leis, decretos, resoluções e portarias que versam sobre o tema, dentre elas podemos citar: Lei 11.829 de 25 de novembro de 2008, publicada no Diário Oficial da União que altera a lei 8.069 de 13 de Julho de 1990, o Estatuto da Criança e do Adolescente que fala sobre pornografia infantil e outras condutas praticadas relacionadas à pedofilia através da internet.

Conforme a sociedade evolui, o direito também precisa evoluir simultaneamente. Diante disso é possível notar as atualizações na legislação que estarão presentes de forma constante na busca pela inibição das práticas dos crimes virtuais.

2.5.1 LEI GERAL DE PROTEÇÃO DE DADOS

Depois de anos de batalha foi aprovada, no dia 14 de agosto de 2018, a Lei Geral de Proteção de Dados a qual estabelece limites e proteção para coleta de

dados pessoais dos consumidores. Um dos aspectos principais da lei é a exigência de que as empresas possuam a autorização do consumidor/usuário para utilização dos dados que tiverem acesso, assegurando, ainda, a revogação do consentimento.

Figura 2 – Conceito da LGPD

Fonte: SAJ ADV 2018

As determinações impostas pela lei são de suma importância para a proteção dos consumidores, visto que a necessidade desenfreada das empresas de obter informações, criarem inúmeros bancos de dados e o compartilhamento dos mesmos deixa em evidência a potencial violação de direitos dos consumidores.

> [...] o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. (STJ, REsp 22.337-9/RS, 4ª Turma, Min. Rel. Ruy Rosado de Aguiar, julgado em 13.02.1995.)

Ainda que o cidadão tenha o conhecimento da coleta de dados em determinados sites ou empresas, é possível que não tenha consciência da importância deles, visando alcançar o objetivo primário do acesso foca apenas no querer momentâneo acaba por “trocar” os dados para alcançar seu objetivo:

> O ser humano tem a tendência de focar nos benefícios imediatos, o que, de acordo com o arranjo e os modelos de negócios da economia informacional,

> é representado pelo acesso a um produto ou serviço on-line. Por tal razão, deixa de sopesar os possíveis prejuízos à privacidade, que são temporariamente distantes. De fato, os possíveis danos com relação à perda do controle sobre as informações pessoais só podem ser experimentados no futuro. (BIONI, 2019, p. 147).

A LGPD, lei nº 13.709/18, trouxe consigo mudanças que precisaram de tempo para serem efetivamente cumpridas pelas entidades, empresas e o governo. Dentre tais alterações, podem ser citadas: A indicação explicita do *Data Privacy Office* (encarregado pelo tratamento de dados pessoais), política de retenção e backup de dados dos consumidores, gestão de consentimentos, definir políticas e disponibilizar avisos de privacidade, entre outras medidas.

Quando se trata do tratamento de dados a Lei Geral de Proteção de Dados caracteriza como “toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização de acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle de informação, modificação, comunicação, transferência, difusão ou extração.” Nesse caso só poderá ocorrer em determinadas situações, um exemplo, e o mais recorrente, é a obtenção de dados por meio do consentimento do usuário. A administração pública também tem a liberdade de coletar e tratar os dados para o cumprimento de políticas públicas.

Todas as pessoas que estão no Brasil ou atividades realizadas no país estão sujeitas as determinações da Lei Geral de Proteção de Dados, também é válida para coletas realizadas em outros países, desde que tenham relação a serviços realizados no território brasileiro. Mas existem exceções, como é o caso de obtenção de informações pelo Estado para defesa nacional e segurança pública. A lei também não inclui a coleta de dados para fins particulares, acadêmicos, jornalísticos e artísticos sem fins econômicos.

2.6 FISCALIZAÇÃO E INVESTIGAÇÃO

Existe uma grande diferença quando falamos em provedor de internet e provedores de acesso, apesar de muitos acharem que é a mesma coisa, eles se distinguem. Quando falamos de provedores de internet, estamos falando daqueles que disponibilizam os serviços de conexão à internet, já os provedores de acesso

são aqueles que fornecem o acesso a provedores de conteúdos nas páginas da web, por exemplo, o acesso ao e-mail.

É necessário fazer essa distinção para que possamos compreender como se dá a fiscalização e penalidade desses meios.

Desta forma, podemos apontar algumas atitudes que podem ser de responsabilidade do provedor de acesso, como o caso de desobediência, quando descumprem requisição de autoridades, débitos não autorizados em contas bancárias, o que poderia ser enquadrado no crime de estelionato. A doutrina estrangeira responsabiliza penalmente o provedor de acesso/conteúdo dando ênfase a crimes de pornografia infantil ou/e terrorismo, todavia, os provedores de internet só seriam penalizados se tivessem conhecimento sobre o conteúdo ilícito. Sendo essencial que haja uma mudança para melhor fiscalizar e punir esses infratores.

A fiscalização e investigações dos crimes virtuais envolvem quebra de sigilo, quando aberta uma denúncia. O processo pode ser lento e bem longo, podendo demorar em torno de dois meses ou anos, devido aos déficits já mencionados.

Com o crescimento do uso dos computadores e a popularização dos smartphones, vários métodos auxiliam a polícia no processo de investigação e fiscalização, como exemplos podem citar os mapeamentos, identificações, rastreamento e correta preservação do dispositivo alvo do crime.

Os exames realizados nos dispositivos consistem em analisar os arquivos e programas do disco rígido, seguindo as fases de preservação, extração, análise e formalização.

A preservação dá a garantia que os dados armazenados no dispositivo não sejam corrompidos ou alterados, a extração é o processo que recupera as informações copiadas da primeira fase. A análise tem como finalidade analisar as evidências recolhidas nos materiais obtidos na fase anterior. A última fase é a formalização, cuja responsabilidade é a elaboração do laudo do pericial. É válido ressaltar que quando se trata de dispositivos móveis os exames seguem a mesma regra e sequência de fases.

Existem outras formas de perícia além das já citadas, elas são realizadas em sites verificando seu conteúdo, podendo ser realizadas em servidores remotos de diversos serviços da internet. A realização dessa verificação se dá através de dois programas, o WDET e o HTTrack, cuja função é realizar a cópia do conteúdo de

forma automática, preservando os dados obtidos evitando uma futura perda de informações, já que os administradores do site analisado podem excluir o conteúdo tornando-o inacessível. A definição dos responsáveis pelo conteúdo é realizada através do IP (*Internet Protocol*), que possibilita a consulta no site r*egistro.br* para obtenção do responsável pelo conteúdo.

Uma última forma de investigação que deve ser ressaltada é a análise de mensagens eletrônicas (e-mail) que é feita através da verificação do conteúdo das mensagens. Seu objetivo é descobrir, por meio de uma análise profunda, o remetente da mensagem. Para isso, o perito precisa verificar o registro no DNS (Domain Name System). Como boa parte das empresas dispõe de contas de forma gratuita, se torna viável identificar remetentes de mensagens falsas, desde que o perito ou autoridade competente faça a solicitação dos dados cadastrais e endereços de IP que estão sendo usadas nas contas de e-mail.

No processo de fiscalização e investigação o perito é uma peça fundamental e indispensável, sendo ele responsável pela busca e apreensão dos dispositivos, regendo a equipe para realizar os exames do material colhido. Só realizando todo o processo de forma correta se tornará possível punir o agente realizador do crime virtual, por isso é de suma importância que o se tenha um profissional qualificado orientando uma equipe, afinal, qualquer erro pode ocasionar numa perda de provas.

2.7 OS DESAFIOS ENFRENTADOS PELA PERÍCIA

Existem diversas dificuldades enfrentadas pelos peritos durante o processo de investigação, são elas a quantidade de arquivos, existência de senhas, criptografia, a esteganografia e muitos outros empecilhos que surgem no processo de investigação e dificultam ainda mais a realização dos exames necessários para obtenção de provas. Sobre isso, Gustavo Testa Corrêa (2010, p. 79) discorre:

> O grande problema relacionado aos “crimes” digitais é a quase ausência de evidências que provem contra o autor, a inexistência da arma no local do crime. Uma gloriosa invasão a sistema alheio não deixaria nenhum vestígio, arquivos seriam alterados e copiados, e nenhum dano seria prontamente identificado. Um crime perfeito, sem traços, e, portanto, sem evidências. Justamente por essa qualidade da perfeição há a dificuldade em presumir o provável número desses “crimes.

A quantidade de arquivos é uma grande complicação para o perito, com o aumento da capacidade de memória nos dispositivos também gerou um aumento na quantidade de arquivos, o que dificulta ao perito encontrar evidências.

As senhas são formas bem comuns de proteger arquivos e também são usadas para ocultar provas, ocasionando em um trabalho ainda mais árduo para a perícia, que são obrigadas a usar programas para quebra desta barreira. Já a criptografia é uma técnica ainda mais complicada, os criminosos utilizam uma escrita na forma original e ilegível, formando códigos para tornar um arquivo codificado e ainda é provável que aliem esta técnica a esteganografia, que é a ocultação de um arquivo dentro de outro. Por isso se faz necessário que o perito tenha conhecimentos avançados, para que possa obter as informações necessárias para que seja possível rastrear e punir o *cibercriminoso*.

Quando se trata da vida real, os problemas causados à vítima por algum crime são quase imediatos, já no meio virtual é possível que a vítima leve meses até perceber que seu computador ou smartphone foi invadido, infectado ou seus dados foram roubados. Deste modo, é bem provável que grande parte das evidências seja perdida já que os provedores de acesso têm a obrigação de guardar as informações como IP, data e hora de acesso por apenas 6 (seis) meses. Caso os dados sejam solicitados após esse período, o servidor não possui a obrigatoriedade de dispor esses dados, deixando a investigação ainda mais difícil.

As grandes empresas e corporações também dificultam o trabalho da polícia, não acionando a justiça quando uma conta de um cliente é invadida, por exemplo. Elas se valem do receio de quebrar a confiança de seus clientes e futuros clientes, sendo as invasões uma mancha na reputação da empresa.

Em entrevista concedida a Isadora Marina C. de Almeida Pagzonni em 1 de novembro de 2017 o advogado especializado em crimes digitais, Dr. Fernando Peres, ao ser questionado sobre quais seriam as dificuldades na aquisição de provas nos crimes cibernéticos, ele discorre que:

> O grande problema se encontra na produção de provas e na identificação do agente. A produção de provas em si, depende muito mais da sua existência e disponibilidade. Por exemplo, se alguém faz um comentário na internet, ou publica um site falso, se este ainda estiver no ar eu posso facilmente produzir a prova, por meio de print screens, impressões ou até mesmo por meio de prova testemunhal. Agora, quanto a identificação do agente, [...] cada aparelho registra as informações de acesso, que corresponde a conexão daquele momento [...] e a partir dessas informações

> vamos pedir a quebra de sigilo no processo judicial e ir até a operadora de internet, e lá, com o número de IP, data e hora, obrigatoriamente, eles devem fornecer os dados cadastrais do responsável por aquela conexão. Mas, por exemplo, se o sujeito está na casa de outra pessoa, será identificado o nome dessa outra pessoa, nesse caso na investigação policial ou cível, pode ser realizado uma busca e apreensão de equipamento para que se faça uma perícia. Essa é uma situação padrão, mas não quer dizer que seja a mais fácil. [...] Outro problema é quanto aos procedimentos tomados pela vítima, visto que muitas vezes ela demora muito na produção de provas. Por exemplo, o Marco Civil da Internet prevê que os provedores de aplicação devem guardar os registros de IP com data e hora pelo período de 6 meses. Assim, se a vítima demora muito a descobrir o crime ou a solicitar a informação, eles não serão obrigados a fornecer. [...] Falta muitas vezes conhecimento do próprio juiz, promotores e advogados na produção da própria técnica, como por exemplo, compreender que é obrigatória a informação não só do IP como da data e hora, para que essa prova não seja inútil, o que acaba dificultando na obtenção dessas informações.

A lei será sempre a maior ferramenta para inibir a ocorrências dos crimes virtuais e isso reforça a ideia de capacitação dos agentes de investigação, afinal, para a efetivação de uma investigação completa e eficaz são necessárias pessoas especializadas capazes de quebrar todas as barreiras colocadas pelos criminosos para dificultar a obtenção das provas.

É necessário considerar que a sociedade a cada dia que passa fica mais informatizada, o que reforça a ideia de maior conscientização por parte desses usuários, sendo os crimes virtuais um ônus da modernidade e dos avanços tecnológicos. Muitos usuários ainda se colocam em situação de risco quanto a esses crimes, insistindo em navegar sem a proteção de antivírus ou aqueles que clicam em qualquer site e abrem qualquer conteúdo que recebem em seu e-mail. Com isso, favorecem o crescimento desenfreado dos delitos virtuais e sobrecarregam os órgãos responsáveis em deter os cibercrimes.

Para diminuir os desafios dos peritos e dos profissionais especializados nessa área, é preciso pensar em que maneira é possível educar os usuários dos computadores e ferramentas tecnológicas, para que assim haja uma diminuição de oportunidades das quais o *cibercriminoso* toma proveito para efetuação do *cibercrime.* Também excluindo a responsabilidade penal do usuário/vítima em se pôr em situações de risco.

É notável, diante de pequenas ou grandes pesquisas, que existem muitas propostas de inovação. Contudo, o amadurecimento dessas ideias é lento em comparação a velocidade que os crimes virtuais se multiplicam. É importante que haja uma melhoria e adaptações perante a redação dos tipos penais e da imposição

de obrigações aos servidores de acesso para que haja, de fato, uma melhoria e facilitação no trabalho dos peritos e profissionais que atuam para coibir esses crimes.

3. CONCLUSÃO

Quando falamos de crimes virtuais, muitos associam a imagem daquela pessoa que faz do crime sua profissão, agindo por trás da tela de um computador com o objetivo de conseguir roubar dinheiro. Quando, na verdade, o crime virtual pode ser cometido por uma pessoa comum quando ultrapassa o limite da própria liberdade, violando o direito de privacidade do outro. É aí que a questão se torna muito mais complexa.

Por meio deste artigo foi possível notar a relevância do tema, posto que a evolução tecnológica é gradativamente crescente e, com ela, as modalidades de crimes do meio virtual cresce conjuntamente. Uma vez que a tecnologia se tornou parte do dia a dia das pessoas, se torna necessário uma avaliação para criação de normas que regulamentem a ação humana e projetos que conscientizem o usuário dos riscos e os eduquem para que melhor se previnam contra a ação desses meliantes.

É notório, diante da pesquisa realizada, que o Direito Penal brasileiro ainda não está completamente apto para lidar com as novas realidades que envolvem a criminalidade cibernética, por faltar a ele tipificações de condutas mais específicas. Constam, também, as grandes dificuldades e empecilhos no processo de investigação pela falta de profissionais especializados na área.

É de extrema importância que haja uma criação de penas mais severas e leis específicas para punir o *cibercriminoso*. Assim como estimular as pessoas a denunciar quando forem vítimas dessas condutas criminosas obrigarem as grandes empresas a relatarem invasões de contas de seus clientes, criarem mais delegacias especializadas nesta área para que assim a população se sinta mais segura.

REFERÊNCIAS

BARRETO, Alessandro Gonçalves. **Investigação Digital em fontes abertas**. Rio de Janeiro. Brasport, 2017.

BRASIL, Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF, Senado, 1988.

BRASIL. LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012 altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. **Diário Oficial da República Federativa do Brasil**, Brasília, 30 de novembro de 2012.

BRASIL. **Lei Federal Nº 13.709, de 14 de agosto de 2018.** Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>

COLLI, Maciel. **Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos**. Curitiba: Juruá Editora, 2010.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 5 ed. São Paulo, Saraiva, 2010

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais.** São Paulo: Saraiva, 2011.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a Computação Forence**. São Paulo: Novatec Editora, 2011GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet**. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

G1. **Lei 'Carolina Dieckman', que pune invasão de Pcs, entra em vigor.** Publicado em 2013. Disponível em: <http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html>. Acesso em 09 de Abril de 2020.

JÚNIOR, Antonio Rulli; NETO, Antonio Rulli. **DIREITO AO ESQUECIMENTO E O SUPERINFORMACIONISMO: APONTAMENTOS NO DIREITO BRASILEIRO DENTRO DO CONTEXTO DE SOCIEDADE DA INFORMAÇÃO**. Publicado pela Revista Esmat, em 2013. Disponível em: <http://esmat.tjto.jus.br/publicacoes/index.php/revista_esmat/article/view/57/63> . Acesso em 02 de Abril de 2020.

PAESANI, Liliana Minardi. D**ireito e Internet: liberdade de informação, privacidade e responsabilidade civil**. 1ª ed. São Paulo, Atlas: 2000.

PINHEIRO, **Patricia Peck. Proteção de Dados Pessoais**. Comentários à Lei n. 13.709/2018. Ed. 1. Vol. Único. São Paulo: Saraivajur, 2018.

ROHRMAN, Carlos Alberto. **Curso de Direito Virtual**. 1ª ed. Belo Horizonte: Del Rey, 2005.

STJ. **Justiça usa Código Penal Para Combater Crime Virtual**. Publicado em 2008. Disponível em: <https://stj.jusbrasil.com.br/noticias/234770/justica-usa-codigo-penal-para-combater-crime-virtual> . Acesso em 05 de Março de 2020.

SAJ ADV. **Direito Digital: Lei Geral de Proteção de Dados Pessoais**. Publicado em: 2018. Disponível em: <https://blog.sajadv.com.br/direito-digital-lei-de-protecao-de-dados/>. Acesso em 06 de Setembro de 2020.

VIANA, Marco Túlio. **Fundamento de direito penal informático. Do acesso não autorizado a sistemas computacionais**. Rio de Janeiro: Forense, 2003.