
**CRIMES CIBERNÉTICOS:
SEUS EFEITOS REVOLUCIONÁRIOS DIANTE DE UMA LEGISLAÇÃO EM
CONSTANTE EVOLUÇÃO**

*Erika Fernanda Tangerino Hernandez¹
Nathália Karina Abucci de Toledo²*

RESUMO

O presente artigo tem como objetivo a reflexão acerca dos efeitos notáveis que o avanço tecnológico trouxe no mundo do Direito, em especial, na legislação brasileira. Sabemos que, o Direito acompanha as transformações e evoluções sociais no decorrer do tempo e da história assim, visando tais evoluções, na medida em que a sociedade tecnologia evolui, concomitantemente, crescem as diversas formas de condutas delituosas através de meios eletrônicos, portanto o Direito Penal vem, em seu caráter repressivo e punitivo alcançando a passos largos, as modalidades trazidas por esse “admirável mundo novo” que é o ambiente virtual, conduzindo importantes e significativas mudanças legislativas, as quais possuem por si só efeitos revolucionários no que tange a tipificação e investigação dos crimes cibernéticos, os quais são cada vez mais comuns e crescentes na sociedade hodierna.

Palavras-chave: Crimes cibernéticos. Direito. Evolução social. Legislação.

72

ABSTRACT

This article aims to reflect on the remarkable effects that technological advancement has brought in the world of law, especially in Brazilian legislation. We know that the law follows the social transformations and evolutions over time and history, thus, aiming at such evolutions, as society evolves technology, concomitantly grows the various forms of criminal conduct using electronic media, so the Criminal Law comes, in its repressive and punitive character reaching in stride, the modalities brought by this "brave new world" which is the virtual environment, leading important and significant legislative changes, which have by themselves revolutionary effects, regarding the typification and investigation of cybercrimes, which are increasingly common and growing in society today.

Keywords: Cyber crimes. Law. Legislation. Social evolution.

¹ Mestre em Geografia, Meio Ambiente e Desenvolvimento pela Universidade Estadual de Londrina (UEL); Especialista em Educação à Distância pela Faculdade Arthur Thomas (FAAT); Especialista em Direito e Processo Penal pela Universidade Estadual de Londrina (UEL); Graduada em Direito pela Universidade Estadual de Londrina (UEL). Docente em Cursos de Graduação e de Pós-Graduação da Universidade Filadélfia de Londrina –UNIFIL; Advogada. E-mail: erika.hernandez@unifil.br.

² Acadêmica em Direito e Pós-graduanda em Perícias Judiciais pela Universidade Filadélfia de Londrina- UNIFIL; Estagiária na Representação Jurídica da Caixa Econômica Federal de Londrina- REJUR/LD; E-mail: nathalia.toledo@edu.unifil.br



SUMÁRIO

1. INTRODUÇÃO. 2. O DIREITO E A INTERNET. 3. O SURGIMENTO DA FIGURA DO CIBERCRIMINOSO. 4. DOS CRIMES VIRTUAIS EM ESPÉCIE. 5. DA INVESTIGAÇÃO E COMBATE AOS CRIMES VIRTUAIS. 6. CONSIDERAÇÕES FINAIS.

INTRODUÇÃO

É notável o avanço da tecnologia no decorrer da história, bem como, as benesses que ela proporciona até os dias atuais. O mundo virtual trouxe inúmeras facilidades para a sociedade como um todo, como por exemplo, acesso ilimitado a informações, a possibilidade de comunicação imediata, a simplificação das relações de consumo, e também relações de trabalho, entre outros. Ocorre que, juntamente com os benefícios, é de praxe que tal evolução, também ocorra em contrapartida de forma negativa.

De forma infeliz, essa facilidade também recaiu em condutas delituosas, sendo aberto um mundo de novas possibilidades para a prática de infrações penais no ambiente virtual, vez que pessoas podem utilizar-se da tecnologia para realizar diferentes crimes. Sucessivamente foi necessária, em contrapartida, uma reação do Direito, em especial do Direito Penal, o qual vem munido de preocupação em combater e reprimir os crimes informáticos com suas mais variáveis espécies.

Esse combate contra os crimes cibernéticos vem de anos atrás, se tornando uma preocupação mundial, sendo munido de um grande escopo histórico e de suma importância nos dias que se decorreram, no entanto, na medida em que tais crimes avançam, o Direito também segue tais transformações, caminhando em passos largos no intuito de investigar e aplicar sanções de forma eficiente para cibercriminosos.

2. O DIREITO E A INTERNET

O Direito como ciência social, nasce da relação entre pessoas, podemos dizer que ele é o meio que interliga o homem e a sociedade, com a finalidade de regulamentar as relações coletivas, visando manter a ordem através das leis impostas pelo Estado, e seus conjuntos de normas, obrigações, direitos e deveres os quais devem ser prestigiados e cumpridos



objetivando o bem-estar social. Assim, da mesma forma em que a sociedade está em constante transformação e evolução, o Direito se relaciona com o tempo e o contexto social, podendo ser político ou moral. É válido ressaltar que a moral em si não tem caráter jurídico, portanto, em matéria de Direito, o mesmo segue a evolução de acordo a complexidade e transformações de relações no âmbito coletivo.

Conforme a teoria Darwinista das normas jurídicas, as evoluções que a sociedade traz consigo, induz às futuras alterações no entendimento jurídico, pode se dizer então que, tal teoria amolda-se dentro do mundo do Direito, pois, observado a contínua evolução da sociedade juntamente com os seus regimentos normativos, tal processo de transformação é constante no decorrer da história. Temer (2000, p.204) cita que:

O Direito, por sua vez, tem por uma de suas principais características o hiato temporal existente entre o conhecimento das mudanças sociais, sua compreensão, as tentativas iniciais de trata-las á luz de conceitos tradicionais e finalmente, a adoção de princípios para regular as relações que delas resultam.

Assim posto, sobrevém a amplitude da internet nos dias atuais. É oportuna uma breve contextualização de onde surgiu a ferramenta da internet. A palavra em si significa “rede internacional” - advindo da união dos termos em inglês Inter (internacional) e net (rede), e teve seu surgimento no fim século XX, como ferramenta para as comunicações internas em casos de guerra e para estudar as relações entre ser humano e máquinas, com seu uso estritamente limitado, apenas a militares e cientistas da época.

Somente na década de 1990 o uso da internet como ferramenta se torna de fácil uso para todos, juntamente com as suas mais diversas utilidades. Por conseguinte, é presente cada vez mais a evolução da tecnologia, e a sua incrível facilidade de substituir atos físicos pelos atos virtuais. Com toda essa acessibilidade e inovação, simultaneamente houve múltiplas benesses, assim como problemáticas, tendo em vista o enfoque na esfera jurídica, um dos problemas, por exemplo, é a criminalidade virtual, a qual se tornou um grande desafio para área jurídica nos mais variados aspectos, uma vez que, regulamentar as relações sociais ocorridas no âmbito da tecnologia é desafiador, devido a celeridade em que tal área avança juntamente com suas inúmeras modalidades. Diniz (2000, p.19), aduz que:

74



Com o advento da informática, no alvorecer do novo milênio, surge o Direito da Internet, como um grande desafio para a ciência jurídica, por descortinar, como diz Huxley em sua obra “um admirável mundo novo”, diante do enorme clamor provocado ao levantar questões polêmicas como: “[...] Como evitar ou como punir os infocrimes, as atividades delituosas praticadas na internet por crackers e invasão dos hackers nos arquivos de dados confidenciais? [...]” Essa problemática gerada pelo Direito na internet tem grande relevância na atualidade, não só por sua complexidade, como também pela riqueza de seu conteúdo teórico-científico e pelo fato de não estar, normativa, jurisprudencial e doutrinariamente bem estruturada.

Portanto, de fato a internet é um mecanismo que trouxe muitas mudanças significativas, por que não dizer extremas! Tanto na sociedade como em um todo, quanto na individualidade de cada cidadão, devido a todo acesso à informação que ela traz a esse mundo novo.

3 O SURGIMENTO DA FIGURA DO CIBERCRIMINOSO

Em uma época totalmente informatizada, o Direito, como já pontuamos, busca acompanhar a realidade fática da sociedade, principalmente tratando-se de regulamentar as condutas humanas, portanto, na era digital são presentes os mais variados obstáculos, por ser algo tão atual e sendo tão notória a transformação social advinda com seu crescimento.

Importa-se frisar, a rapidez em que a ferramenta eletrônica se tornou alvo do interesse público mundial, portanto, sendo de se esperar que nela desenvolvam-se as mais variáveis condutas, entre elas a criminosa, já que, infelizmente no mundo atual tem se por corriqueiro que uma parte mínima da sociedade se volte para condutas tendenciosas e ilícitas. “A internet é um paraíso de informações, e, pelo fato de essas serem riqueza, inevitavelmente atraem o crime. Onde há riqueza, há crime.” (CORREA, 2000, p. 42).

A internet traz consigo uma riqueza inovadora, através de suas mais variadas formas de comunicação, de todo alcance de informações e conhecimentos que dispõe, juntamente com a facilidade em seu acesso. Fato esse, que certamente não escapou e não escapa de olhares criminosos, se tornando “palco” da maior parte de crimes digitais, pois nessa modalidade é oferecida aos mesmos certa vantagem que é difícil obter em crimes “palpáveis”, que se dá então pelo possível “anonimato”, e por ser um sistema virtual que está em constante transformação, sendo tirado ainda o proveito de suas imperfeições.



Surge, assim, diante desse novo cenário, a figura do cibecriminoso, a qual vem munida de uma conduta progressiva na medida em que se avançam as normas regulamentares para o mundo virtual, e a ascensão tecnológica através do tempo.

Muitas atividades desenvolvidas no âmbito cibernético, dão margem a uma série de violações e princípios e normas jurídicas, assim, é indispensável partir da premissa que o Direito é a única forma de controle capaz de conter o crescimento da criminalidade nesse “mundo novo”, já que se reveste de coercitividade, sancionando condutas ilícitas, principalmente sob o escopo do Direito penal e processual Penal. De acordo com Daoun (2000. p. 129), a informática aliada ao Direito nos faz concluir que falar hoje sobre o é estar em constante mutabilidade pessoal em princípios, conceitos e ideias.

Podemos dizer que, a partir das transformações da sociedade e das relações pessoais, os comportamentos socialmente danosos também se adaptaram a essa nova era virtual. Boiteux (2010, p. 947) aduz que:

O crime é um fato social, portanto, é perfeitamente natural que também se transformasse com as alterações da sociedade em que se insere”. É notável que hoje as consequências de determinado ato delituoso praticado com o uso de computadores na esfera local, ou via internet, podem ser bem mais amplas e perigosas do que antes, já que não há restrição de fronteiras ou limitações geográficas no chamado ciberespaço.

76

O Direito penal informático nasce então da necessidade de lidar com a melhor maneira possível com novos tipos de condutas delituosas, sendo de suma importância levar em consideração que, quando qualquer fato social novo se aproxima do Direito, são elencados novos desafios e o surgimento de novas realidades, especialmente no âmbito do Direito penal, como atuante em forma de controle social, sofre ainda mais pressões e cobranças.

A Criminalidade com o uso de computadores trouxe uma preocupação em equilibrar a forma repressiva penal com as condutas mais graves, garantindo os Direitos a respeito dos Direitos fundamentais em junção com os Direitos humanos, ainda mais visando um mundo de tão livre espaço de comunicação mundial, porque não dizer democrático, que é a internet.

Assim, o Direito Penal vem, não somente com sua força punitiva mais também preventiva acerca de tais delitos, sempre munido com as suas evoluções de acordo com o lapso temporal social e se preocupando com o bem estar social, dando grandes passos a cada evolução.



No geral, para a configuração de um crime virtual, necessariamente ele deve ocorrer por meio da internet, portanto, qualquer um que possua acesso pode cometer uma prática delitiva no âmbito virtual, além de que, nesse meio é oferecida uma ferramenta única: a possibilidade de anonimato, no entanto, diante do cenário atual no combate a essa modalidade de crime, tal possibilidade vem sendo cada vez menor.

Dentro do mundo virtual, atualmente existem as mais diversas classificações de cibercriminosos, sendo as mais comuns os “*Hackers*”, o qual é o termo em que mais temos familiaridade, vem do verbo em inglês “to hack”, o que significa fuçar/bisbilhotar, as ações dos hackers se dão por procurar vulnerabilidades em sistemas computacionais, os “*Crackers*”, o qual nomenclatura também vem do verbo em inglês “to Crack”, o que significa quebrar, sendo aqueles que usam claramente os meios digitais sempre com o intuito de obter vantagem.

Além do mais, existe de forma não menos importante e mais corriqueira aqueles chamados “comuns” os quais não possuem o conhecimento técnico como os outros, e que acabam utilizando a ferramenta virtual para cometer crimes “corriqueiros”, como ameaça, compartilhamento de conteúdo ilícito, pedofilia, crimes contra a honra entre outros.

77

Observamos que, conforme crescem os crimes virtuais, também crescem quem o número dos cibercriminosos dentro dessas variáveis classificações.

Outro assim importa ressaltar que, na medida dos avanços desses crimes, bem como, o aumento de quem os pratica, o Direito brasileiro avança a passos largos, já que, muitas dessas ações se descobertas, já são criminalizadas e podem gerar consequências, tais como sanções penais ou civis.

4 DOS CRIMES VIRTUAIS EM ESPÉCIE

Conforme a teoria tripartida do conceito analítico de crime, conceitua-se o crime como um fato típico, antijurídico e culpável, sendo o primeiro elemento de identificação do mesmo consistente na conduta humana voluntária produzindo um resultado que se amolda formalmente e materialmente ao tipo penal previsto em lei, a segunda denominação se dá pelo fato de que, não basta a conduta estar apenas prevista na Lei, para configurar crime é preciso que o fato seja contrário ao previsto, de forma que viole os bens jurídicos tutelados pelas



normas, por fim, se preenchido os requisitos de tipicidade e antijuricidade, recai sobre a conduta delituosa do indivíduo uma sanção, conforme determinado na Lei penal.

O crime sempre esteve presente na sociedade, contudo, com o advento da internet no decorrer no tempo, como já contextualizamos anteriormente, surge uma nova maneira de praticar as condutas delituosas usando a ferramenta da internet. Essa modalidade vem de duas formas, existem os crimes cometidos através do meio virtual, ou seja, aqueles que usam a internet como meio para chegar então ao resultado pretendido, e existem os crimes que visando determinado ambiente virtual, ou seja, utilizam a internet, com o objetivo de obter o resultado no próprio meio virtual.

O conceito de crime informático pela Organization for Economic Cooperation and Development (OECD), da ONU (Organização das Nações Unidas), foi definido no ano de 1986, a qual conclui ser: “[...] qualquer comportamento ilegal, aéctico ou não autorizado envolvendo processamento automático de dados ou informações, a falsificação de programas, o acesso e/ou uso não autorizado de computadores e redes”

De acordo com a classificação dos crimes cibernéticos, os mesmos podem ser classificados como próprios, impróprios, mistos e indiretos. Os crimes cibernéticos próprios são aqueles onde o bem jurídico violado é a própria tecnologia da informação, os impróprios são aqueles onde a tecnologia atua como um meio para o cometimento do delito, portanto, os bens jurídicos já tutelados pelo Código penal são atingidos com o auxílio virtual, os mistos ocorrem quando há ofensa a mais de um tipo penal, e por fim, o indireto são aqueles chamados “crimes-meio”, onde a conduta delituosa é iniciada através do meio informático, visando à consumação de um crime não virtual.

Conforme relatório da Norton Cyber Security referências, em 2017 o Brasil passou ser o segundo país com maior número de crimes cibernéticos, afetando cerca de 62 milhões de pessoas, e causando um prejuízo de R\$ 66,3 bilhões (UOL, 2018). Atualmente conforme pesquisas o Brasil é o quarto país do mundo onde os cibercrimes mais crescem e esse número tende a aumentar cada vez mais.

Outro assim, devido a termos a visão de Direito a qual acompanha a sociedade, cada vez mais nosso ordenamento jurídico tem acompanhado esse fenômeno, observando a necessidade de haver Leis específicas em sua tratativa, o que vem acontecendo, cada vez ficando longe a possibilidade de usar a analogia nas práticas descritas no Código Penal.



Um grande avanço normativo brasileiro foi a promulgação do Marco Civil da Internet, o qual foi considerado no Brasil, um texto pioneiro a fundar direitos, deveres e regras acerca do mundo digital, o qual ainda tramitou mais de dez anos, sendo oficialmente chamado de Lei 12.965, sancionado em 23/04/2014 pela então presidente da época Dilma Roussef, considerado como uma "Constituição da Internet", pois veio regulando princípios, garantias, Direitos e deveres de quem usa a rede, bem como da determinação e diretrizes para a atuação do Estado.

Posteriormente, foram promulgadas a Lei Azeredo (Lei 12.735/12, e a Lei Carolina Dieckmann (Lei 12737/2012) as quais regem especificadamente sobre crimes no âmbito virtual. O surgimento das referidas Leis, foi algo revolucionário no que tange a crimes virtuais no Brasil.

A Lei 12.735/12- Lei Azeredo- teve inicialmente seu projeto proposto em 1999, por Luiz Piauhyllino, visando à punição para crimes virtuais, porém, somente 4 anos depois foi aprovada pela Câmara, tendo o seu texto alterado pelo então Senador Eduardo Azeredo. Tal projeto foi debatido por mais de uma década no Congresso Nacional, aprovado pela Câmara em 2003 e enviado ao Senado, onde tramitou até 2008 e ainda passou pelas mais diversas discussões.

De seu conteúdo original, o qual inicialmente continha 23 artigos, desses foram sancionados apenas 4, referidos artigos, são os que trazem de fato, mudanças à legislação penal, contudo, ainda 02 destes foram vetados pela então Presidente Dilma Rousseff, restando apenas 2 artigos na lei sancionada em 3 de dezembro de 2012.

Com o veto, a Lei instituiu que órgãos de polícia judiciária deverão formar setores e equipes especializadas no combate à ação delituosa em rede de computadores, e também promoveu alteração no inciso II do § 3o do art. 20 da Lei 7.716/89, a então Lei de Crimes Raciais, que define os crimes resultantes de preconceito de raça ou de cor.

Muito se discutiu acerca de violação aos Direitos constitucionais que o projeto de Lei em si trazia consigo, discutindo-se até sobre possível inconstitucionalidade de seu conteúdo. Foi dito até projeto de lei do senador Eduardo Azeredo, criminaliza de forma generalizada, tipificando, inclusive a conduta culposa, extrapolando os limites da razoabilidade e da proporcionalidade, por trazer em seu texto a permissão do juiz, de antes mesmo do inquérito policial, determine a cessação das transmissões de símbolos ou similares cujos objetivos sejam divulgações que incitem a discriminação ou o preconceito.



A Lei 12737/2012 - intitulada pela imprensa de “Lei Carolina Dieckmann” -foi aprovada na época em que a atriz foi vítima da divulgação de suas fotos íntimas conseguidas através da invasão de seu computador, dispondo sobre a tipificação criminal de delitos informáticos, acrescentando ao Código Penal os artigos 154-A e 154-B e também alterando os artigos 266 e 298 do mesmo.

O art.154-A traz a tipificação da invasão do dispositivo eletrônico, visando a proteção da privacidade e da intimidade, bem como informações sensíveis ao proprietário ou usuário do dispositivo, informações essas que não deveriam ser de conhecimento público ou de terceiros. O artigo em comento foi recentemente alterado pela Lei nº 14.155/2021, sendo majorada a pena, que passou a ser de reclusão de 1 (um) a 4 (quatro) anos e multa, para quem invadir dispositivo eletrônico de uso alheio, com o fim de obter, adulterar ou destruir dados sem autorização do usuário ou até mesmo instalar vulnerabilidades para obter vantagem ilícita, bem como, é aumentado a pena de 1/3 (um terço) a 2/3 (dois terços), se da invasão resultar em prejuízo econômico, e se caso a invasão resultar em obtenção de informações sigilosas, ou controle remoto não autorizado do dispositivo invadido, a pena será de 2 (dois) a 5 (cinco) anos de reclusão e multa.

O art. 154-B, acrescentado pelo referida Lei prevê que a ação penal do Estado ficará vinculada à representação da vítima, salvo se o ilícito for praticado contra entidade administrativa pública direta ou indireta, e ainda a alteração do art. 266, trouxe consigo a proteção contínua disponibilidade dos serviços de informação e de comunicação de dados de utilidade pública, ainda a alteração do art.298, equipara o cartão de crédito e débito a documento particular, no intuito de evitar o uso indevido e criminoso das informações pessoais de terceiros para a prática de fraudes eletrônicas.

Há quem defenda a não criação de leis próprias para tratamento de crimes cibernéticos, ocorre que, a vasta gama de inovações tecnológicas que devem ter uma interpretação extensiva, pois seus significados trazem consigo uma complexidade alinhada a contemporaneidade, devendo ter regramento próprio, pois a simples analogia as tipificações penais anteriormente vigentes, não possuem caráter para efetivamente enquadrar, muito menos repelir as práticas cometidas nesse novo mundo.

Recentemente, houve a promulgação da Lei 14.132/21, a qual inclui no Código Penal Brasileiro a tipificação do crime do termo em inglês “Stalking”, o qual significa “perseguição”, tal ato ocorre principalmente através de computadores, o mesmo traz em seu



texto que” perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade”. Mediante denúncia pela vítima, o autor do crime poderá ser condenado à pena de reclusão, de 6 meses a 2 anos, e multa, causando aumento de pena pela metade se for cometido contra criança, adolescente ou idoso; contra mulher por razões da condição de gênero; se praticado por duas ou mais pessoas; se cometido com emprego de arma.

Outra inovação legislativa foi a recente promulgação da Lei 14.155/21 a qual trouxe mudanças mais que necessárias, trazendo penalidades mais severas a crimes de furto, fraude e estelionato praticados através de ferramentas tecnológicas, com a reclusão, de um a quatro anos, e multa, aumentando-se a pena de um terço a dois terços se a invasão resultar em prejuízo econômico. Antes, a pena aplicável era de detenção de três meses a um ano e multa.

Ainda, a Lei acrescentou ao Código Penal a agravante do furto qualificado por meio eletrônico, trazendo a pena será de reclusão de quatro a oito anos e multa, e se o crime for praticado contra idoso ou vulnerável, a pena aumenta de um terço ao dobro. E, se for praticado com o uso de servidor de informática mantido fora do país, o aumento da pena pode ir de um terço a dois terços, e também incluiu no texto normativo que a pena do estelionato será de reclusão de quatro a oito anos e multa quando a vítima for enganada e fornecer informações por meio de redes sociais. (AGÊNCIA SENADO, 2021)

Através da Lei nº 13.964/19, foi inserida uma significativa mudança nos crimes contra a honra, no art.141 §2 do CP, na onde foi determinado que, se tais crimes forem cometidos através de meio virtual, será aumentado a pena em triplo.

Além do que, entre os crimes cada vez mais corriqueiros, os quais são o “bulling”, a pedofilia, o “phissing” mais conhecido como grampo eletrônico, a injúria, a calúnia e a difamação virtual, entre inúmeros outros, todas essas condutas, se reconhecidas, podem ser penalizadas de acordo com o Código Penal, Civil e ECA.

Assim, referidas Leis trouxeram significativas mudanças, possibilitando o aprofundamento punitivo e repressivo dos agentes delituosos, possibilitando ainda o uso da própria ferramenta como combate a fatos típicos, trazendo então ainda mais o fortalecimento da justiça nos dias atuais.



5 DA INVESTIGAÇÃO E COMBATE AOS CRIMES VIRTUAIS

A investigação referente a esse tipo de crime tem o início semelhante a qualquer outra investigação, primeiramente é necessária a constatação do crime ou incidência cibernética, devendo ser observado se a conduta praticada se enquadra dentro do rol taxativo das Leis que tangem sobre tal matéria, para assim, ser possível a verificação de que se trata de prática punível.

Inclusive, já existe previsão legal de instituição de delegacias estaduais especializadas em crimes virtuais, bem como, canais de atendimento on line para atendimentos e registros de ocorrências. De acordo com o Safernet (2021) já existem delegacias especializadas nos seguintes Estados: Bahia, Espírito Santo, Mato Grosso, Maranhão, Minas Gerais, Pará, Paraná, Pernambuco, Piauí, Rio Grande do Sul, São Paulo, Sergipe, Rio de Janeiro, Tocantins e Distrito Federal.

Há também canais de atendimento ao cidadão no âmbito federal, através do Ministério Público e a Polícia Federal via SAC (Sala de Atendimento ao Cidadão), instituída pela Portaria PGR/MPF Nº 412/2013 (BRASIL, 2013) onde é recebida as denúncias e então as mesmas são encaminhadas ao setor responsável.

Havendo a constatação de crime, inicia-se a investigação, onde primeiro é incumbido aos investigadores oficiarem os provedores para se possível a preservação das evidências, solicitando, assim a busca e apreensão dos equipamentos eletrônicos envolvidos os quais serão devidamente periciados.

Quando presente a impossibilidade de busca e apreensão, é possível requerer ao juízo que o mesmo oficie os provedores de aplicação que informem os dados cadastrais e de registros, os quais possibilitam a localização do suspeito.

Outro assim, instaurada a fase investigativa, a mesma pode promover o desencadeamento da Ação Penal para a então responsabilização dos agentes pela prática delitiva cometida.

CONSIDERAÇÕES FINAIS

Considera-se fascinante o desenvolvimento tecnológico, pois o mesmo resultou para a humanidade, a denominada “Era da Informação”, logo, se fazem necessárias atualizações



legislativas, o que já faz parte do mundo dos operadores do Direito, assim como, dos legisladores, como já demonstrado neste trabalho.

O mundo cibernético se mostra totalmente dinâmico e de características únicas, portanto, no ramo normativo, não há espaço para apegos tradicionais de pensamento. Essa é a beleza do Direito, ter por sua força a característica de se amoldar de acordo com as evoluções sociais que decorrem ao infinito tempo, e nos proporcionar fonte inesgotável de informações e conhecimento que também vão passando por transformações ao decorrer da história, tornando-se o que ele é, assim como deve ser uma ciência puramente social, imperado pela adaptação as convicções de justiça.

Diante de inúmeras transformações, estamos diante de um cenário cada vez mais eficiente no que tange a investigação e combate aos crimes cibernéticos no Brasil, já que, tem sido crescente a consciência de que é possível identificar e punir tais criminosos, bem como, a decretação de regimento próprio para tal, outro assim, se tratando não somente de grandes avanços normativos, mas também um significativo avanço social.

REFERÊNCIAS

83

AGÊNCIA SENADO. Disponível em :
<https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contracrimenes-ciberneticos-e-sancionada>. Acesso em: 28 maio 2021.

BOITEUX, Luciana. **Crimes informáticos**: reflexões sobre política criminal inseridas no contexto internacional atual. Doutrinas Essenciais de Direito Penal. São Paulo: Editora RT, 2010.

BRASIL. **Lei nº 12.737 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 de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, [2012]. Disponível em :
http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm . Acesso em: 15 jun. 2021.

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. Brasília, DF: Presidência da República, [2012]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112735.htm. Acesso em: 15 jun. 2021.



BRASIL. **Lei nº 14.155 de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 27 jul. 2021.

BRASIL. Ministério Público Federal. Procuradoria Geral da República. **Portaria nº 412 de 05 de julho de 2013**. Disponível em: <http://bibliotecadigital.mpf.mp.br/bdmpf/bitstream/handle/11549/20096/PORTARIA%20PGR%20N%C2%BA%20412-2013.pdf?sequence=4&isAllowed=y>. Acesso em: 15 jul. 2021.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 2000.

DAOUN Alexandre; DINIZ, Maria Helena; TEMER Michael. **Direito & Internet- Aspectos Jurídicos relevantes**. Bauru: Edipro.2000.

OECD. Organization for Economic Cooperation and Development. Disponível em: <https://www.cybercrimelaw.net/OECD.html> Acesso em: 07 jul. 2021.

SAFERNET. Disponível em: <https://new.safernet.org.br/content/delegacias-ciber Crimes>. Acesso em: 07 jul. 2021.

UOL. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes->. Acesso em: 25 jun. 2021.

