FACULDADE EVANGÉLICA DE RUBIATABA
CURSO DE DIREITO
LUIZ FERNANDO BELIZÁRIO MACÊDO

CIBERCRIMES:
A INTERNET COMO FERRAMENTA NA EXECUÇÃO DE CRIMES VIRTUAIS E O COMBATE REALIZADO PELO DIREITO PENAL BRASILEIRO

RUBIATABA/GO
2020

LUIZ FERNANDO BELIZÁRIO MACÊDO

CIBERCRIMES:
A INTERNET COMO FERRAMENTA NA EXECUÇÃO DE CRIMES VIRTUAIS E O COMBATE REALIZADO PELO DIREITO PENAL BRASILEIRO

Monografia apresentada como requisito parcial à conclusão do curso de Direito da Faculdade Evangélica de Rubiataba, sob orientação do professor Mestre em Ciências Ambientais Pedro Henrique Dutra

RUBIATABA/GO
2020

LUIZ FERNANDO BELIZÁRIO MACÊDO

CIBERCRIMES:
A INTERNET COMO FERRAMENTA NA EXECUÇÃO DE CRIMES VIRTUAIS E O COMBATE REALIZADO PELO DIREITO PENAL BRASILEIRO

Monografia apresentada como requisito parcial à conclusão do curso de Direito da Faculdade Evangélica de Rubiataba, sob orientação do professor Mestre em Ciências Ambientais Pedro Henrique Dutra

MONOGRAFIA APROVADA PELA BANCA EXAMINADORA EM __ / ___ / ____

Mestre Pedro Henrique Dutra
Orientador
Professor da Faculdade Evangélica de Rubiataba

Especialista Gláucio Batista da Silveira
Examinador
Professor da Faculdade Evangélica de Rubiataba

Especialista Fernando Hebert de Oliveira Geraldino
Examinador
Professor da Faculdade Evangélica de Rubiataba

Primeiramente agradeço ao nosso Senhor e bondoso Deus, em seguida aos meus pais e família por me proporcionar este sonho.

AGRADECIMENTOS

Em primeiro lugar eu agradeço a Deus por ter me dado esta oportunidade, privilégio, sustentação.

Aos meus pais que me apoiaram em todo período, sem eles este sonho não poderia ser concretizado.

Ao meu orientador, Dr. Pedro Henrique Dutra, pelo suporte afetivo e profissional no auxílio das atividades, principalmente sobre o andamento e normatização deste Trabalho de Conclusão de Curso, aonde obteve partilha de seus conhecimentos.

Aos professores da faculdade que inapelavelmente foram corresponsáveis pelo nosso crescimento intelectual.

Agradeço aos colegas de classe pela espontaneidade e alegria na troca de conhecimentos, ao qual guardarei para sempre em meu coração.

Por fim, agradeço a todos aqueles que, de alguma forma, fizeram-se especialmente presentes na minha vida ou que contribuíram para a minha formação ao longo dos últimos anos.

E finalmente minha caminhada só está começando, e é com muito esforço e dedicação que venha minha aprovação para Agente de Polícia Federal.

RESUMO

O objetivo desta monografia é de identificar o trabalho do Direito Penal em relação a atualização da legislação para o combate de crimes virtuais. Para atingir este objetivo o autor desenvolveu o estudo qualitativo com método dedutivo, expondo as principais leis que interagem com uso de equipamentos informáticos, e como algumas leis são atualizadas para aderir ao amparo de crimes cibernéticos, porém, ao mesmo tempo, destacou-se como o Direito Penal ainda caminha devagar sobre a atualização das leis. Foi possível identificar que a internet ainda é palco da maioria dos crimes envolvendo estelionato, fraudes, golpes, humilhação, violência, dentre outros, e mesmo tendo isso em mente, a velocidade pela qual uma lei se adequa e permite o amparo social sobre determinado crime informático ainda é pequeno, sendo necessário maior conscientização dos legisladores sobre a necessidade de manter esse tipo de atividade sempre atualizado, principalmente pelo fato do Brasil ser um dos países que mais são acometidos por golpes informáticos, e na maioria das vezes, pouco amparados sobre como recorrer.

Palavras-chave: Cibercrime. Direito Penal. Internet.

ABSTRACT (SE O RESUMO FOR EM LÍNGUA INGLESA)

The objective of this monograph is to identify the work of Criminal Law in relation to updating legislation to combat virtual crimes. To achieve this objective, the author developed the qualitative study with a deductive method, exposing the main laws that interact with the use of computer equipment, and how some laws are updated to adhere to the protection of cybercrimes, however, at the same time, stood out as Criminal Law still walks slowly on updating laws. It was possible to identify that the internet is still the scene of most crimes involving fraud, swindles, humiliation, and violence. Even keeping this in mind, the speed by which a law is adequate and allows social protection over a certain crime information technology is still small, requiring greater awareness of legislators about the need to keep this type of activity always up to date. Mainly Brazil because is one of the countries that are most affected by computer scams, and in most cases, little supported on how to resort

Keywords: Cybercrime. Criminal Law. Internet.
Traduzido por Eliane Clemente da Silva.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Cibercrimes são crimes realizados em meios informáticos, de preferência recorrendo a internet como principal ferramenta para aplicação. No Brasil, demandam enorme perigo para a população, principalmente no período de pandemia onde as pessoas acessam mais computadores, celulares, tablets, etc. Para se ter uma ideia, somente entre os períodos de janeiro a julho de 2020, mais de dez milhões de pessoas foram atingidas pelo golpe digital *phishing*, que se trata num meio de aplicar golpes, clonagem de cartão, dentre outros crimes (GARRETT, 2020).

Como consistem em crimes considerados silenciosos, por não ameaçarem diretamente a vítima como acontecem nos crimes tradicionais, a legislação para inibi-los tende a ser diferenciada, necessitando a descrição e adaptação das leis para punir e aumentar a segurança da população.

Nessa mesma premissa, por se tratar de novos crimes de contexto social, o Direito tem como trabalho identificar essas novas situações que ferem os princípios da liberdade, segurança e que ferem a cidadania dos indivíduos. Além disso, pode-se considerar como dificuldade a velocidade dos avanços tecnológicos em comparação ao desenvolvimento de legislações, por isso, escolheu-se como problemática: como o Direito Penal se aplica e se atualiza para assegurar os direitos das pessoas que sofrem cibercrimes?

O objetivo geral é de identificar o trabalho do Direito Penal em relação a atualização da legislação para o combate de crimes virtuais. Para isso, deve-se entender primeiramente em relação aos objetivos específicos: descrever as características do cibercrime e os principais crimes virtuais acometidos aos brasileiros; identificar as atuais leis para a proteção e o amparo dos indivíduos que sofrem crimes virtuais; e avaliar os desafios do combate aos crimes virtuais.

O tema vai se destinar ao uso da internet para realização dos crimes virtuais mais cometidos no Brasil entre os anos de 2013 a 2019, e como existe o trabalho penal para o combate a estes crimes. Porque destaca-se a hipótese de que criminosos veem na internet uma “terra sem lei” para cometer crimes. A lei n. 12.737/2012 que dispõe sobre tipificação criminal de delitos informáticos foi o primeiro passo para coibir o considerado cibercrime, porém, passados sete anos da criação dessa lei o Brasil ainda necessita de equipes destinadas a área de atualização de leis relacionadas a informática, com legislações mais específicas e punitivas aos crimes virtuais.

A pesquisa terá metodologia de revisão de literatura com abordagem qualitativa. Os dados são organizados por um levantamento bibliográfico e organizados segundo o método dedutivo. Assim, é possível realizar a explicação de um tema geral e alterando para o foco do documento. Os arquivos lidos foram encontrados nas bases de dado *Google Scholar* e *Scielo* onde foram selecionados artigos e livros, com língua portuguesa, com ano de publicação entre 2000 a 2017, sendo utilizados como descritores: cibercrimes, direito penal do cibercrime.

O tema escolhido é relevante porque o brasileiro é o povo que mais sofre com ataques de cibercriminosos na América Latina e a sétima posição no ranking mundial (KAPERSKY, 2019). Os crimes geram diversas desavenças as pessoas, como estelionato, clonagem de cartão, ameaças, falsidade ideológica, dentre outros. Entender que este é um tema de preocupação nacional, e que as pessoas não sabem o que fazer quando sofrem deste mal, por isso, relatar o amparo que o Direito estabelece para combater estes crimes é importante para possibilitar as pessoas de receber seus direitos e proteção.

Com isso, o trabalho apresenta no capítulo 2 as principais informações sobre o cibercrime, suas definições e como ocorre no Brasil. No capítulo 3 foi descrito as como consistem as leis de proteção na internet, verificando o amparo por direito e a opinião de doutrinadores sobre o tema. E o capítulo 4 destaca os principais desafios do combate ao cibercrime pelo Direito Penal, destacando a necessidade de atualizações para o direito, como ainda é uma vantagem para ação criminosa, e o que pode ser sugerido para diminuir as ocorrências.

2 A INTERNET NOS CRIMES VIRTUAIS

O primeiro passo para entender como o Direito Penal se atualiza para assegurar os direitos das pessoas que sofrem os chamados cibercrimes necessita do entendimento dos profissionais desta área sobre como a internet funciona, mais especificadamente dentro da prática de cibercrime. Dessa forma é possível estabelecer medidas para que a legislação possa ser atualizada a intervir sobre estes casos.

Por isso, como capítulo inicial, são discutidas as principais questões que esclarecem a importância da internet para a globalização e como esse tipo de ambiente se tornou propicio a criminalidade, motivado principalmente pelo anonimato. Para ter uma ideia, hoje a internet é parte da vida humana, sendo muito complicada a vida sem internet, ou dispositivos tecnológicos.

Computadores, celulares, tablets, sites, dentre outros recursos tecnológicos possuem os dados pessoais da maioria das pessoas, e, sabendo disso, os criminosos recorrem a estratégias e ao desenvolvimento de programas que possam roubar os dados das pessoas, assegurando possível assedio, falsidade ideológica, chantagem, dentre outros crimes que competem a difícil identificação do criminoso ou do que fazer após passar por uma situação dessas.

Sendo assim, pode-se explicar de forma mais detalhada todas essas informações a seguir.

2.1 INTERNET NA GLOBALIZAÇÃO E NA PRÁTICA DE CIBERCRIMES

Quando foi criada a Internet na década de 60, mais concretamente em 1969, pelo governo norte-americano para fins militares, nada fazia prever a escala global e as capacidades que esta viria a alcançar. Foi graças à *World Wide Web* que a Internet se tornou no fenómeno que é atualmente e adquiriu a maioria das suas capacidades. Atualmente a Internet permite: armazenar e partilhar ficheiros com computadores e pessoas de todo o mundo; obter informação em formato digital, de forma rápida, simples e acessível a todos, em qualquer parte; localizar de forma rápida e simples qualquer pessoa ou serviço; entre outros (SANTOS, 2015).

Em meio à Era da Informação, que se iniciou ao final do século XX motivado pelo constante desenvolvimento tecnológico no mundo, a sociedade tornou-se, transformou-se em

uma sociedade global, proporcionando meios positivos, oportunidades para o indivíduo. No entanto, com a evolução da tecnologia informacional, também apresentou riscos a partir de sujeitos que as utilizam em condutas ilícitas, as quais passaram a serem praticadas nesse novo ambiente. Esta conduta ilícita passou a ser denominada como cibercrime (ALEXANDRE JÚNIOR, 2019).

> O primeiro registro de delito com o uso de computador data de 1958, no qual um empregado do Banco de Minneapolis, nos Estados Unidos da América, havia alterado os programas de computador do banco, de modo a depositar para si as frações de centavos resultantes de milhões de movimentações financeiras. A primeira condenação por uma corte federal norte-americana deu-se em 1966, por alteração de dados bancários (SILVA, 2012, p. 28).

Desde que, em 1984, quando William Gibson utilizou pela primeira vez a palavra Ciberespaço na sua obra de ficção científica Neuromancer, surgiram várias expressões derivadas e com o mesmo prefixo daquela. Entre elas, ciberdireito e Cibercrime. Não obstante as várias alusões à palavra Cibercrime, a verdade é que não está doutrinariamente definido o seu conceito, ou seja, não existe nenhum dispositivo legal que use, refira ou defina este conceito. Do ponto de vista doutrinário ainda não existem teorizações nem delimitações metodológicas (VERDELHO, 2003).

A Convenção sobre Cibercrime do Conselho da Europa é o primeiro trabalho internacional de fundo sobre crime no ciberespaço. Foi elaborado por um comité de peritos nacionais, congregados no Conselho da Europa e consiste num documento de direito internacional público. Embora tenha na sua origem, sobretudo, países membros do Conselho da Europa, tem vocação universal. Na sua elaboração participaram vários outros países (Estados Unidos da América, Canadá, Japão e África do Sul) e pretende-se que venha a ser aceite pela generalidade dos países do globo (VERDELHO et al., 2003).

Dessa forma, a internet se tornando uma tecnologia que contribuiu gradativamente com a evolução da humanidade, também se torna um ambiente para a prática de crimes, sendo os chamados cibercriminosos responsáveis por intervir em todo tipo de situação para o acometimento de crimes, como demonstrado no exemplo de 1958, um caso de mais de 60 anos onde esse tipo de delito já podia ocorrer.

2.1.1 PRINCIPAIS CRIMES

A partir do entendimento de que a prática de crimes na internet se tornou possível, agora o Direito Penal precisa entender quais são os principais crimes cometidos no século XXI, a partir disso, é possível estabelecer as medidas preventivas e leis que possam amparar as pessoas que caem nesses crimes.

A internet é um dos meios tecnológicos utilizados pelos cibercriminosos para violarem os dados pessoais na internet utilizando de meios refinados para atacar os direitos humanos e ofender os direitos humanos por meio da injuria, calunia e da difamação. Eles não utilizam das armas convencionais, tais como arma de fogo, agressão física, intimidação, mas sim da ausência física. O que dificulta ao Estado brasileiro decifrar esta fenomenologia, que nem sempre a vítima sofre dano verificável no momento (LIMA; XAVIER, 2015).

> Com o avanço da tecnologia, conectar-se à rede mundial de computadores ficou cada vez mais acessível, ainda mais com a popularização dos smartphones, aparelhos celulares, que possuem recursos que possibilitam tal acesso, ou seja, "o que há pouco era meramente um telefone evoluiu para um pequeno computador de propósito geral que cabe na palma da mão''. Os celulares evoluíram a tal ponto que além de serem utilizados com a finalidade de possibilitarem a comunicação via telefonia móvel, eles equiparam-se a pequenos computares, repletos de aplicativos que possuem uma diversidade de funções, como destaca (BROOKSHEAR, 2013, p. 10).

Os ataques dos Cibercriminosos às suas vítimas são silenciosos, a arma utilizada geralmente é um computador, tablet, smartphone ou outro meio tecnológico de ponta. Os danos causados a imagem de uma pessoa agredida por esse tipo de criminoso são imensuráveis (LIMA; XAVIER, 2015).

A definição de cibercrime difere em alguns pontos de autor para autor, mas praticamente todos terminam com o mesmo posicionamento em relação ao vínculo com a internet. Para a advogada militante na área de Direito Digital, Pinheiro, "O cirbercriminoso deveria ser responsabilizado e punido pelo crime, mas ainda é difícil reunir provas técnicas que identifiquem o bandido ou a quadrilha" (CASSANTI, 2014).

Para outros, denominados de leigos, os quais não se aprofundam no mundo virtual, falar em cibercrimes quer dizer falar em crimes cometidos no âmbito virtual, como a pedofilia virtual, a invasão de hacker e crackers, a publicação da vida íntima de terceiros, a invasão em sites de bancos, lavagem de dinheiro, perseguição on-line e outros delitos cometidos via

internet, tais muitas vezes desconhecidos pela população, tornando-a frágil e vulnerável de ser atacada (SAVEGNAGO; WOLTMANN, 2015).

Além destes, possuem sistemas e estratégias que são muito ligadas a cibercrimes, onde mesmo com o investimento e a constante evolução na área da tecnologia, muitos ataques ainda ocorrem e são efetivos, principalmente por causa da engenharia social, na qual induz o usuário (diretamente ou indiretamente) a instalar, sem perceber, programas que serão perigosos ao computador e que podem coletar os dados das pessoas, quebrando os princípios da segurança da informação. Alguns desses ataques estão descritos como exemplos: o *Malware*, o *Spyware* e o *Ransonware*

Os *malwares* são programas maliciosos que podem possuir inúmeras funções, de acordo com a programação e tipos de serviços desejados. Eles podem conter spywares de *keyloggers*, por exemplo. Uma das atividades mais comuns desse tipo de ataque, consiste na criação de máquinas zumbis, uma botnet. As botnets são máquinas que executam tarefas a qual são comandadas remotamente pelo seu criador, na maioria das vezes são utilizadas para executar ataques em larga escala, onde vários computadores podem derrubar computadores e servidores governamentais e de sites, também conhecimentos como ataque DDOS (ataque de negação de serviço). Eles trabalham em conjunto com o *phishing*, induzindo vítimas a acessarem sites clonados sem seu conhecimento e passando informações pessoais (OLIVO, 2010).

O *spyware* é o tipo de ataque que consiste na instalação de um software espião, na maioria dos casos sem que a vítima perceba, permitindo monitorar seu computador. Através da conexão feita P2P (ponto a ponto), ou seja, seu computador diretamente conectado no computador do cibercriminoso, todos os documentos, fotos, vídeo, webcam podem ser compartilhados entre ambos. Com isso o atacante pode instalar mais softwares maliciosos, ou ameaçar e chantagear a vítima quando toma posse de algum documento ou foto (PEREIRA; MARTINS, 2014).

E o *ransonware*, que consiste no sequestro do computador, ou seja, quando ele é executado na máquina vítima, seu código malicioso codifica todas as informações do computador, em seguida apresenta uma tela com os procedimentos que devem ser seguidos para a recuperação dos arquivos. Na maioria dos casos, costuma se pedir dinheiro para recuperação do computador, onde a vítima recebe a senha remove a criptografia executada, permitindo o acesso novamente aos arquivos (CABRAL, 2015).

O caso mais recente deste tipo de ataque ocorreu em 2017 com o ransomware WannaCry, que infectou mais de 230 mil computadores com Windows em mais de 150 países,

muitos deles em agências do governo e hospitais, sendo considerado o maior ataque de um ransomware na história (AVAST, 2017).

Figura 1 – Tela do Ransonware WannaCry
Fonte: Avast (2017).

Na Figura 1, observa-se a tela que aparecia quando o computador era criptografado, dessa forma era pedido uma quantia de trezentos dólares para recuperação dos arquivos. Caso não fosse confirmado o pagamento após 72 horas, o valor dobrava. E após sete dias, todos os dados seriam excluídos, causando pânico em diversos locais, uma vez que era o sequestro de dados extremamente importantes em qualquer local afetado.

Como observado, de modo geral no mundo, inúmeros tipos de golpes podem ser aplicados, golpes, espionagem, estelionato, chantagem, este são os principais tipos de situações que podem ocorrer com as vítimas desses ataques, e que por sinal existem leis próprias para estes casos, mas quando o assunto é relacionado a práticas informáticas as leis realmente estão atualizadas?

2.2 O CIBERCRIME NO BRASIL

No Brasil, conforme apresentado, todos esses ataques também ocorrem, porém, existe um que é mais comum e que tornou o país o mais afetado do mundo, que remete aos ataques de *phishing* (KAPERSKY, 2018). Como esse é o ataque mais comum, as leis podem ser atualizadas mediante o combate a esse tipo de crime em especifico, e mostrando que o Direito Penal precisa estar sempre estudando a nível mundial quais as prática criminosas estão sendo realizadas pela internet para atualizar com maior velocidade e tornar possível o amparo ao usuário, mesmo que determinado ataque ainda não tenha chegado ao país.

O termo *phishing* vem da palavra *fishing*, que em inglês significa pescar, ou seja, ocorre quando uma mensagem falsa é jogada como isca para diversas pessoas, na qual o atacante espera alguém fisgar ela e passar suas informações pessoais. Ela é uma fraude eletrônica e grave ataque, pois quem pratica o golpe obtém desde senhas, dados financeiros, cartões de créditos, dentre outras informações da vítima (MORGENSTERN; TISSOT, 2015).

Dentre os métodos de *phishing* o *scam* é o mais utilizado. Ele ocorre no recebimento de e-mails fraudulentos de empresas conhecidas pelo público, tentando convencer na mensagem de que o acesso é de suma importância, levando-o à uma página clonada com as informações a serem colocadas, na maioria dos casos, confidenciais como o número da conta, senha de acesso, senha do cartão, entre outras (JORGE, 2007).

Pereira e Martins (2014) descrevem que além do *phishing* por e-mail, outro tipo em constante expansão é o *phishing* em sites de relacionamentos, para muitos considerado o meio favorito, consistindo no envio de mensagem para serem compartilhadas, afetando todos aqueles que acessam ao mesmo tempo que facilita a contaminação, visto que um conhecido compartilha o arquivo de *phishing* do outro.

Constata-se que atualmente este tipo de ataque tem aumentado consideravelmente o número de vítimas no mundo todo. Ameaça, estelionato, chantagem, roubo de identidade, perseguição, clonagem de cartões, são apenas alguns das ameaças representadas atualmente por esse tipo de ataque. Estima-se que ao longo dos anos, este meio se tornou o favorito para garimpar informações, crescendo mais de 60% a taxa de uso entre quem prática isso (CORTELA, 2013).

Um tipo de ataque muito comum refere-se ao uso do nome de empresas conhecidas, na qual são criadas páginas falsas e e-mails para inúmeras pessoas aleatórias. Essa prática pode ser vista nas figuras a seguir: na Figura 2 observa-se no topo da imagem o link

"www.internetbanking.caixa.gov.br" que é o do site original do *Internet Banking* da Caixa, enquanto na Figura 3 apresenta link "www.caixaassistenciia.websiteseguro.com" nome tendencioso para que pessoas menos preocupadas não percebam que o site é fraudulento (JORGE, 2007).

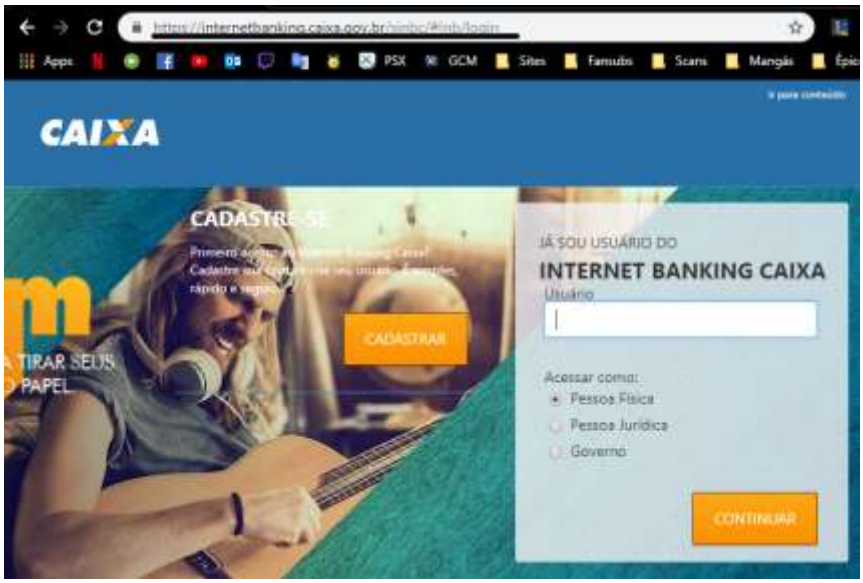

Figura 2 – Site original do Internet Banking Caixa
Fonte: Caixa (2018).

Figura 3 – Site com prática de Phishing do Internet Banking Caixa
Fonte: NoliCorp (2015).

Não apenas utilizando-se de mensagens aleatórias torcendo para que alguém caia neste ataque, os criminosos que praticam *phishing* combinam técnicas de engenharia social e de manipulação de informação e clonagem de páginas para enganar diversos perfis de usuários. Permitindo que o manipule indiretamente para considerar tudo isso legítimo, conseguindo os roubar dados pessoais das vítimas. Dessa forma, o uso de nomes de bancos, lojas e empresas famosas é o básico na prática desse ataque, criando réplicas quase perfeitas para mascarar qualquer possibilidade de identificação (LAS-CASAS et al., 2016).

A Kaspersky (2018), em pesquisa realizada em 2018, destaca que o Brasil ocupa a primeira posição no mundo em ataques de *phishing*. A posição estava garantida ano passado quando constatou que quase 30% dos internautas no país já sofreram ao menos uma tentativa de golpe. Neste ano o índice caiu para 23%, mas não foi o suficiente para tirar o brasil desta posição, confirmando o *phishing* pelo WhatsApp a prática mais comum efetuada atualmente, como apresentado na Figura 4.

Figura 4 – Exemplo de *Phishing* utilizando o WhatsApp
Fonte: TechTudo (2018).

Além do erro humano e a falta de se preocupar em quebrar vulnerabilidades de sistema, a prática de *phishing* é relativamente simples e barata. Basta cadastrar um domínio, seja gratuito ou com preço acessível, depois adquirir um certificado digital para o site ser considerado confiável e disparar e-mails em massa a espera de alguma vítima (KAPERSKY, 2018).

Assim como as tecnologias se tornam cada vez mais seguras e eficientes para a humanidade, o crime cibernético também evolui seus métodos de aplicar golpes via *phishing*, o que antes era feito totalmente através do e-mail, hoje consegue alcançar proporções maiores e mais rápidas graças as redes sociais, anúncios e aplicativos *mobile*.

Pode parecer difícil a relação do crime com as estratégias, porém, como observado, a estratégia que o criminoso é a ponte para um crime maior, seja o roubo de informações pessoais, fotos intimas, clonagem de cartão, informações sigilosas de empresa, dentre outros tipos de dados que se pode dizer em tonar uma “bola de neve” na vida do indivíduo.

Por isso, ao conhecer os principais conceitos sobre os cibercrimes e os principais crimes cometidos no Brasil e no mundo, agora pode-se apresentar o que o indivíduo pode fazer para se assegurar, descrevendo no capítulo seguinte quais as legislações para a internet já existentes no país, para ter um paradigma se já existe certa atualização das leis para o amparo a quem cai nesse tipo de crime.

3 LEGISLAÇÕES PARA A INTERNET

Neste capítulo foram apresentadas as principais informações sobre as atualizações do Direito Penal em relação as práticas de crimes informáticos, descrevendo o histórico e os principais marcos realizados pelo país. Para isso, assegura-se como fundamental a discussão das duas principais leis que abordam completamente a questão informática, sendo elas a Lei Caroline Dieckmann, diretamente relacionada a um ciber crime, e o Marco Civil, que tem como objetivo principal a regulamentação da segurança pessoal da internet.

Junto a essas discussões, pode-se observar que o Brasil ainda não possui uma legislação totalmente focada aos crimes informáticos, porém, realiza atualizações mediante a necessidade e a verificação daquilo que se torna mais necessário à população, e, pode-se ressaltar também que a mídia colabora para que maiores legislações sejam desenvolvidas, como também remetem as duas principais leis criadas no país.

3.1 LEI CAROLINE DIECKMANN (LEI N. 12.737/12)

No Brasil, não existiam leis para o combate a cibercrimes até o ano de 2012, quando uma lei foi sancionada, demonstrando o primeiro sinal da movimentação do Direito Penal para amparar a população sobre crimes cibernéticos. A Lei nº 12.737/12, conhecida por Lei Caroline Dieckmann ocorreu graças a um projeto de autoria do Deputado Federal Paulo Teixeira (PT-SP), que buscou a regulamentação de crimes cometidos em ambientes cibernéticos, que até então era uma lacuna legislativa.

O motivo do nome de “Carolina Dieckmann” se deu devido ao envolvimento da atriz na época em um cibercrime, onde teve suas fotografias íntimas invadidas e expostas na internet o que teve muita repercussão na mídia e nas redes sociais. Para ter uma ideia da repercussão deste caso ocorrido no dia 04 de maio de 2012, foram divulgadas 36 imagens da atriz com cunho íntimo. As fotos rapidamente se tornaram assunto na internet, sendo o assunto mais comentado pelo Twitter na época, e conforme dados da ONG Safernet, em apenas 5 dias as imagens tiveram mais de 8 milhões de acessos únicos (ROMANI, 2012).

Esse evento agilizou a lei para entrar em vigor, onde ela foi sancionada em dezembro de 2012 e entrou em vigor no dia 3 de abril de 2013. De modo geral a lei adiciona ao

Código Penal, os artigos 154-A e 154-B. O motivo da adição no artigo 154 refere-se a sua descrição, relacionada a crimes de violação do segredo profissional, que apresenta:

> Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:
> Pena - detenção, de três meses a um ano, ou multa de um conto a dez contos de réis. (Vide Lei nº 7.209, de 1984)
> Parágrafo único - Somente se procede mediante representação (BRASIL, 1940).

E dessa forma, sendo complementado pelo artigo 154-A:

> Art. 154-A. 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:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (BRASIL, 2012).

Segundo Capez (2014), a lei permitiu a devida classificação sobre o que pode ser considerado crime, pois nela, qualquer pessoa pode ser um sujeito ativo, referente a crime comum. O sujeito passivo é qualquer possuidor do dispositivo informático. Os dados ao bem jurídico tutelado são relativos ao que se define como nível do crime de perigo, ou seja, do qual importante são os documentos expostos. Nesse tópico cabe a ressalva pois, entendemos ser o tipo penal condizente com a classificação de crime de perigo. Dessa forma, sua abordagem pode ser caracterizada como crime formal, devido ao acesso, modificação ou destruição de dados e informações importantes. E finalmente, impactando no principal perigo abstrato ao bem jurídico tutelado que é a privacidade.

Entender que o bem jurídico tutelado é a liberdade individual do usuário do dispositivo informático é fundamental porque este é primeiro impacto sofrido em qualquer tipo de crime cibernético. A liberdade é um dos direitos e garantias fundamentais impostos no artigo 5 da Constituição Federal de 1988, dessa forma, no âmbito Penal, dispõe os crimes que acometem ela.

Criou-se o tipo penal “invasão de dispositivo informático”, conforme art. 154-A e sua respectiva modalidade de ação penal, prevista no art. 154-B.

> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal

> ou Municípios ou contra empresas concessionárias de serviços públicos." (BRASIL, 2012)

Com o artigo 154-B, torna os crimes cometidos nos 154-A de ação penal pública condicionada à representação da vítima, uma vez que sua intimidade e vida privada foram os bens disponíveis violados. Dessa forma, a vítima também tem o direito de ponderar se deseja evitar o processo judicial, sendo no formato de ação pública incondicionada. A ação direta do Ministério Público neste tipo de crime só ocorre nos casos onde o crime foi praticado contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos (PAGANOTTI, 2013).

Sendo assim, mostra como o ocorrido com a atriz Carolina Dieckmann, aumentou a vulnerabilidade da população sobre a internet, estando com medo de algo semelhante ocorrer com eles. Um dos motivos do medo e de maior velocidade na aprovação das leis ocorreu com a mídia, que repercutiu bastante o caso, ressaltando a falta de uma legislação penal pertinente ao tema e sendo direta sobre os perigos da exposição na rede. Com isso não foi apenas os políticos envolvidos, mas também todo um clamor popular em prol de uma legislação que tratasse dos crimes cibernéticos (GRANATO, 2015).

Isso demonstra que para resolver um problema de um crime ainda não legislado, as vezes, torna necessário a ação popular para que determinada lei seja atualizada, demonstrando que apenas a ação legislativa pode ser demorada para realizar a atualização, conforme o projeto de lei for tramitado no congresso, algo que pode demorar até anos, como ocorreu com o Marco Civil da Internet que será descrito a seguir.

3.2 MARCO CIVIL DA INTERNET (LEI N. 12.965/14)

O Marco Civil da Internet foi uma lei que esteve em conversas e tramitações desde 2007, sendo realizada a partir de inúmeras consultas e debate públicos, e seguido de um período de incertezas e inação após seu encaminhamento à Câmara dos Deputados. Quando inúmeros crimes internacionais foram divulgados referente a vigilância em massa e não autorizada por parte da agência norte-americana de segurança nacional, o projeto de lei voltou ao centro de atenções e foi objeto de intenso debate, na qual finalmente foi votado e aprovado nas duas casas legislativas, sendo sancionado (GARCIA, 2016).

Souza e Lemos (2016) descrevem que o Marco Civil da Internet (Lei nº 12.965/2014) foi a primeira iniciativa do Poder Executivo brasileiro destinada totalmente a especificação e eventos ocorridos na rede. Foi um processo gradual, porém, se não fosse os casos internacionais sobre a segurança na internet, este projeto poderia ter sido esquecido no Senado. Dessa forma, o escândalo serviu como catalisador, acelerando a tramitação que vinha apenas arrastando-se, mostrando novamente que uma atualização das leis referentes a informática só ocorreu devido a propagação da mídia.

Tomasevicius Filho (2016), em leitura ao Marco Civil, estaca as críticas de que se poderia restaurar a censura no país, por estar sendo legislado um ambiente que até então, era totalmente "livre". Porém, em seu artigo 2º, caput, afirma-se que o uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão. E o artigo 19 declara que:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário (BRASIL, 2014).

Com esse artigo, os provedores de internet estariam amparados de serem culpados pela ação de terceiros que utilizam seus serviços, evitando assim, denúncias ou cobranças que ferem a liberdade. Liberdade que prevê o princípio da Constituição Federal sob a "garantia da liberdade de expressão, comunicação e manifestação do pensamento, nos termos da Constituição Federal" (TOMASEVICIUS FILHO, 2016).

Preservar os direitos fundamentais e garantir que o desenvolvimento tecnológico é fundamental, pois a legislação deve ter como base as melhores condições a população, tornando o Marco Civil numa ferramenta que aprimore o desenvolvimento das condições econômicas e sociais dos indivíduos e coletividades, e não o contrário.

Considerado pela mídia como a "Constituição da Internet", esta lei buscou disciplinar toda a matéria existente sobre o uso da rede no território nacional a partir de princípios como da neutralidade, privacidade e liberdade de expressão, dessa forma, foram desenvolvidos 32 artigos que abordam os princípios do uso da internet, os direitos e garantias dos usuários, a provisão da conexão e de aplicações da internet, a atuação do Poder Público e as disposições finais.

O usuário da rede tem garantia de que sua vida privada não será violada, a qualidade da conexão estará em linha com o contratado e que seus dados só serão repassados a terceiros segundo seu consentimento ou em casos judiciais. Nesse sentido, a lei regula o monitoramento, filtro, análise e fiscalização de conteúdo para garantir o direito à privacidade

Especial atenção deu-se ao direito à privacidade, entendido aqui, sob o ponto de vista do direito civil, como o direito de isolar-se do contato com outras pessoas, bem como o direito de impedir que terceiros tenham acesso a informações acerca de sua pessoa (Amaral, 2008, p.306). Isso está previsto nos incisos I, II, III, VII e VIII do art.7º, ao elencarem-se como direitos dos usuários de internet a inviolabilidade da intimidade e da vida privada, a preservação do sigilo das comunicações privadas pela rede, transmitidas ou armazenadas; o não fornecimento de dados pessoais coletados pela internet a terceiros sem prévio consentimento do usuário, além de estabelecer o dever de informar os usuários acerca da coleta de dados sobre si, quando houver justificativa para tal fato.

Também descrito no seu art. 10 estabelece a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet devem ser realizadas com respeito a intimidade, vida privada, honra e imagem das pessoas direta ou indiretamente envolvidas. Dessa forma, possibilitou que os provedores de internet e de serviços somente serão obrigados a fornecer informações dos usuários se receberem ordem judicial. No caso dos registros de conexão, os dados devem ser armazenados por, pelo menos, um ano, enquanto os registros de acesso a aplicações por seis meses (MPSP, 2018).

Essa atribuição é complementar ao art. 14, na qual os provedores de conexão à internet não podem guardar registros de acesso a aplicações da internet sem prévio consentimento do usuário, nem os dados pessoais desnecessários à finalidade. Isso foi o chamado neutralidade da rede, também vedando às operadoras a venda de pacotes de internet pelo tipo de uso, ou seja, não é permitido que, visando a um benefício econômico, criem-se barreiras para determinado tipo de conteúdo. Dessa forma, o tráfego de qualquer dado deve ser feito com a mesma qualidade e velocidade, sem qualquer discriminação (MPSP, 2018).

O Marco Civil da Internet foi um marco para a legislação informática, mostrando que o Direito pode se atualizar nessa questão, e que uma constituição direcionada as práticas penais nesta área também pode ser criado com estudos e estabelecimento de objetivos diretos para o amparo ao usuário.

3.3 COMBATE AO CIBERCRIME

Quando se fala em cibercrimes, a privacidade é o primeiro ponto destacado, tanto que na literatura o primeiro tipo de lei para amparar o usuário ocorreu em 2012, porém, antes desse ano outras leis já haviam sido criadas para aumentar a segurança sobre outros tipos de crimes, que se expandiram com a internet.

A Lei nº 9.296/1996 disciplinou a interceptação de comunicação telemática ou informática, descrito em seu artigo 10: "constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei" (BRASIL, 1996).

A Lei nº 9.609/1998, que trata da proteção da propriedade intelectual do programa de computadores. Dessa forma, esta lei regulamentou a propriedade dos códigos de um programa ao seu desenvolvedor, conciliando a lei de direito autoral, cuja violação pode gerar pena de seis meses a dois anos ou multa, conforme artigo 12. Neste artigo também se ressalta a venda pirata de um produto (BRASIL, 1998).

No ano de 2008, foi sancionada a Lei nº 11.829/2008, que atualiza o Estatuto da Criança e do Adolescente no combate a pornografia infantil na internet. Com isso, foram adicionados os artigos 241-A, 241-B, 241-C, 241-D e 241-E. No artigo 241-A fica registrado qualquer troca, disponibilidade, transição ou distribuição, por qualquer meio, inclusive por meio de sistema de informática ou telemático, arquivos (fotos, vídeos ou outros) que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente (BRASIL, 2008).

Dessa forma, não apenas aqueles que realizam o ato criminoso contra menor de idade é punido, como também aquele que armazena, comercializa ou divulga documentos com pornografia infantil. Com a expansão da internet e o acesso de crianças e adolescentes a todo tipo de site e rede social, a lei também ampara os casos de aliciamento, assedio, ou constrangimento da criança, com o fim de com ela praticar ato libidinoso, conforme artigo 241-D (BRASIL, 2008).

Outro ponto importante foi a lei nº 13.185, de 6 de novembro de 2015 que institui o Programa de Combate à Intimidação Sistemática (*Bullying*). A nível informático, ele combate o chamado *cyberbullying* (artigo 2, parágrafo único), cujo tipo de intimidação sistemática pode ser qualquer um dos descrito no artigo 3, porém, uma das descrições foi totalmente destinada as ameaças virtuais: "VIII - virtual: depreciar, enviar mensagens intrusivas da intimidade, enviar ou adulterar fotos e dados pessoais que resultem em sofrimento ou com o intuito de criar meios de constrangimento psicológico e social" (BRASIL, 2015).

A lei mais recente em relação a internet entrou em vigor em agosto de 2020, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), já conhecida como LGPD. Sua criação teve como objetivo reduzir os riscos associados ao uso impróprio e/ou indevido do processamento de dados pessoais e, ao mesmo tempo, permitir que novos negócios e tecnologias se desenvolvam em um ambiente legalmente seguro. A aplicação da LGPD não afetará apenas os negócios das empresas brasileiras, mas também todos os países ou empresas estrangeiras ou locais de residência que forneçam produtos e/ou serviços para o mercado brasileiro ou monitorem o comportamento dos proprietários de dados no Brasil, independentemente de sua nacionalidade.

Com essa lei foi definido informações sobre o que é considerado um dado pessoal, um dado sensível e um dado anonimizados, que representam as informações pessoais pessoa física (CPF, RG, endereço IP, etc.), dados relacionados a saúde, vida sexual, orientação política, etc., e os que não permitem a identificação, direta ou indireta, de seu titular, respectivamente.

Dessa forma, a lei tem como objetivo gerir o tratamento de dados das pessoas que acessam a internet, tratamento esse que pode ser referente a "coleta, produção, recepção, classificação, utilização, o acesso, a reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, ou extração de dados pessoais" (DANIEL IP, 2019).

Como observado, mesmo que inúmeras leis relacionadas a internet foram desenvolvidas antes de 2012, porque elas não são consideradas as primeiras para resolução de crimes informáticos? Porque foi uma questão de mídia, onde o caso em específico tornou a lei Caroline Dickmann num marco para leis de combates a cibercrimes. Interceptação de dados, combate a pedofilia e direitos autorais já existiam, porém foram atualizados para combater aqueles que praticam o mesmo crime na internet.

Enquanto isso, o crime cometido pela atriz foi uma novidade, no país ainda não tinha sido feito uma exposição que surtiu em tamanha repercussão, totalmente no âmbito online, pois os documentos roubados era as fotos do celular da vítima, que foi invadido. Dessa forma, mostra os dois pontos da atualização do Direito Penal, na qual ele visa a mudança de leis existentes, adicionando como deve ser o combate relacionado ao uso informático. E na estratégia de crimes totalmente virtuais.

4 DESAFIOS DO COMBATE AO CIBERCRIME

Neste capítulo foram descritos os principais pontos ressaltados da dificuldade do combate aos cibercrimes, o que torna o cibercrime tão eficiente e quais as práticas podem ser realizadas para melhorar a segurança dos usuários. Entende-se que existe a dificuldade da atualização penal visto a tramitação das leis no Senado e a velocidade que os cibe criminosos se atualizam para dificultar sua identificação.

Outro ponto a ressaltar é devido ao fato de que apenas uma estratégia atinge mais de 10 milhões de brasileiros, o que mostra a importância do Direito Penal em assegurar o amparo dessa população, ao mesmo tempo que é necessário a conscientização para que diminua a probabilidade de a população cair nesses golpes, que abusam principalmente da inocência e falta de conhecimento da vítima.

Assim, pode-se finalizar com clareza o funcionamento dos crimes, o porque são tão chamativos para os criminosos, o trabalho do Direito Penal para atualização penal e, principalmente, como a população pode ser amparada pela legislação e conhecimento desses tipos de eventos.

4.1 ATUALIZAÇÃO PENAL

O Marco Civil da Internet trouxe grande regulamentação sobre como os dados na internet devem ser administrados, porém, a nível de combate a crimes, mas ainda existe ausência de legislação bem elaborada e específica, algo fundamental para o amparo dos usuários acometidos pelas condutas atípicas que não podem ser punidas em decorrência do princípio da reserva legal (BORTOT, 2017).

Um crime muito comum e relevante que ocorre é o chamado Ataque Distribuído de Negação de Serviço (DDoS), que consiste numa técnica maliciosa pela qual o agente utiliza equipamentos conectados à rede, de forma coordenada e distribuída, parar deixar um serviço, computador ou rede, inoperante. Esse tipo de ataque não tem objetivo de invadir e nem de coletar informações, e sim de exaurir recursos e causar indisponibilidade ao alvo (CERT.BR, 2016).

Além dos servidores, os principais impactados são os usuários desses recursos, que ficam impossibilitados de acessar ou realizar as operações desejadas. Esse ataque também é

difícil de ser identificado, devido ao fato de que os acessos legítimos dos maliciosos se misturam na sobrecarga (CERT.BR, 2016).

Neste caso, entende-se a dificuldade de atualização penal, uma vez que um ataque desse tamanho parte de inúmeros computadores que podem estar infectados, sendo necessários meios de identificar o computador responsável pela ativação do ataque para verificar se é mesmo o responsável.

No caso da A Lei Dieckmann, mesmo apresentado em seu art. 3, que incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, é um dispositivo insuficiente, devido à falta de elementos normativos como “Serviço telemático e informação de utilidade pública”. Esse tipo de lei pode não se aplicar a ataques a sites, devido a definição não ser semelhante a esta (BORTOT, 2017).

Outro ponto reflete que seja necessário o rompimento de um mecanismo de segurança (como antivírus, firewall, senhas, etc.) para que realmente aconteça o crime de invasão de dispositivo informático. Ou seja, se um dispositivo é invadido sem a violação de alguma barreira de segurança (por exemplo, se o computador da vítima não tem antivírus), a conduta será atípica. E na lei sobre a regulamentação de autoria sobre programa de computador, não são apresentados os processos penais nas atividades de comercialização de *cracking codes* (decodificadores de acesso) e de engenharia reversa de software, por meio das quais inúmeros danos e prejuízos podem ser gerados aos usuários (SÃO PAULO, 2017).

No caso de ataques de *Ransomware*, o anonimato torna difícil a identificação do infrator, que prática o sequestro de dados e estelionato com ameaça sobre os dados que foram presos. Neste caso, existe um trabalho conjunto para identificação dos métodos de resolver o ataque, pois o pagamento do valor pedido não impede que um próximo ataque seja realizado, sendo necessário acionar a polícia se algo assim ocorrer (BORTOT, 2017).

Por isso, se deve realizar o estudo continuo de como as leis podem ser atualizadas para amparar os usuários dos crimes informáticos, observando também como os outros países agem para o combate delas. Apenas na leitura desta monografia já é possível identificar inúmeros pontos que deveriam ser atualizados pelo Direito Penal, mas que até o momento não tem previsão de mudanças.

4.2 VANTAGENS DA INTERNET PARA O CIBERCRIME

Como demonstrado, os principais passos para atualização Penal referente a crimes informáticos remetem ao entendimento de como são esses crimes, e como eles são aplicados, porém, mesmo com as inúmeras atualizações existentes, ainda existem inúmeros desafios a serem enfrentados.

Um dos principais meios da criminalidade ocorre devido as zonas obscuras da rede mundial de computadores, a chamada “deep web”. Ela é a camada da internet que não está indexada nos buscadores tradicionais de busca, como Google, Bing, etc. Muitos exemplos representam a deep web no formato de iceberg, onde a parte visível seria a representação normal da internet e o fundo abaixo da água a internet da zona obscura. Devido ao sigilo que ela apresenta, a dificuldade para encontrar os servidores dos infratores é mais complicado do que seria nos casos de cyberbullying nas redes sociais, onde a prestadora dos serviços online pode ceder, sob solicitação judicial, o IP e endereço do computador que está cometendo este delito (CARDOSO et al., 2018).

A grande dificuldade encontrada para punir os infratores dos crimes praticados na internet conforme já foi mencionada não ocorre pela falta de norma que caracteriza os crimes e os classifica em uma ordem. O real problema se presencia em detalhes como a falta de tecnologia e de mão de obra especializada para o combate aos cibercrimes. Desde 1988, quando a rede mundial de computadores passou a ser implementada no Brasil, não houve preparos e investimentos para combater os crimes que já vinham sendo praticados nos países que originaram a internet, de modo que ficou mais fácil a pratica de crimes na rede (CRUZ; RODRIGUES, 2018).

Outro problema encontrado para as investigações serem mais precisas é que o nosso ordenamento jurídico a sanção penal só pode ser aplicada, quando houver a certeza da prática do crime, sendo fundamentais a comprovação da autoria e da materialidade, ou a existência de fortes indícios de que o sujeito praticou o crime. Caso não consiga ser comprovada a materialidade e autoria o juiz poderá absolver o réu, conforme traz o artigo 386 do Código de Processo Penal (CPP) (CRUZ; RODRIGUES, 2018).

> Art. 386. O juiz absolverá o réu, mencionando a causa na parte dispositiva, desde que reconheça: I - Estar provada a inexistência do fato; II - Não haver prova da existência do fato; III - Não constituir o fato infração penal;IV - Estar provado que o réu não concorreu para a infração (...) V - Não existir prova de ter o réu concorrido para a infração penal;

Além do tramite demorado, evidenciasse um outro problema que é as empresas de informação, se recusarem a prestar auxílio a polícia e ao judiciário, a título de exemplo o WhatsApp, que mesmo com a autorização da justiça se recusou prestar informações quanto a usuários investigados, que gerou decisão de bloqueio da referida rede social, por tempo limitado. Há a falta de pessoas especializadas para agilizar nas investigações, empresas como o WhatsApp que não colaboram com o judiciário, leis fundamentais que atrasam as investigações e o pior com a globalização, aumenta o número de crimes praticados por estrangeiros no Brasil, e a facilidade de compra de hospedagens de IP localizada fora do País, causando um conflito de competência acerca de que órgão deve julgar os crimes cibernéticos. (CRUZ; RODRIGUES, 2018).

4.3 METODOLOGIAS DE AUMENTO DA SEGURANÇA VIRTUAL

Quanto a prevenção de ataques, na maioria dos casos os métodos para se prevenir de um ataque funcionam para todos, dessa forma, seguindo estas dicas, além de evitar o *phishing*, também pode evitar os demais como os citados *malware*, *spyware* e *ransomware*.

A Cartilha de Segurança para Internet (CERT.br, 2012) apresenta dez precauções que devem ser tomadas pelos usuários quando estiverem navegando na internet.

Tabela 1 – 10 dicas para prevenção de ataques *phishing*

Dicas de prevenção ao *phishing*
Ficar em alerta com mensagens com nome de alguma instituição, principalmente se estiver pedindo informações ou instalação de programas;
Questionar-se por que a instituição da mensagem está mandando mensagem para você e se realmente possui relação com ela (por exemplo, se um banco que você não possui conta manda recadastrar);
Fique atento a mensagens que chamam muito a atenção ou ameace caso não cumpra o que está escrito;
Não considere uma mensagem confiante por que conhece o remetente, inúmeros atacantes usam contas invadidas ou manipuladas;
Seja cuidadoso ao acessar links, sempre analisando se o endereço está correto mesmo, antes de digitar dados pessoais;
Caso não suspeitar do link visualmente, passe o mouse por cima, caso houver técnica de ofuscar, ao posicionar o mouse sobre o link o endereço real da página falsa aparece;

Utilize mecanismos de segurança, como *antimalware*, *firewall* pessoal e filtros *antiphishing*;
Verifique se a página utiliza conexão segura;
Verifique as informações mostradas no certificado;
Acesse a página da instituição que supostamente enviou a mensagem e procure por informações (a maioria não adiciona páginas como suporte, sobre, etc.)

Fonte: CERT.br (2012, p. 11)

Junto a essas dicas, o uso de navegadores Web atualizados são essenciais, pois muitos possuem mecanismos de *antiphishing* nativos que identificam possíveis páginas fraudulentas, apresentando mensagem de segurança (SILVA et al., 2017).

Na Figura 6 observa-se uma das funções do mecanismo, ao tentar acessar o site "www.fakebook.com", que é um site fraudulento, o navegador apresenta a mensagem que podem ser invasores, impedindo que caia nesse golpe.

Figura 5 – Página de proteção contra golpes cibernéticos do navegador Google Chrome
Fonte: Google (2018)

Silva et al. (2017) ainda apresenta que os navegadores listam essas mensagens de proteção por gerar listas negras com diversos *urls* de sites potencialmente perigosos, onde ao receber a solicitação verifica em seu repositório, se conter exibe a mensagem de alerta, porém, se for um novo site de golpes, pode acabar exibindo a página ao usuário, como apresentado na Figura 6.

Figura 6 – Exemplo do mecanismo de proteção dos navegadores contra *phishing*
Fonte: SILVA et al. (2017, p. 375)

Cabral (2015) destaca também a importância de manter o Firewall sempre ativo, pois ele previne que atacantes externos acessem a rede do computador. Não apenas o computador, mas o roteador também possui firewall, trabalhando em conjunto para bloquear qualquer tipo de pacote malicioso que venha tentar acessar o dispositivo do usuário.

O uso de antivírus é imprescindível, principalmente para usuários leigos em informática, pois ele permite detectar e neutralizar vírus e ameaças ao computador. Esses programas podem ser executados em tempo real para que sempre identifique qualquer software malicioso antes mesmo dele executar qualquer tipo de ação na máquina (ARAUJO; ARAUJO, 2013).

Um antivírus confiável e sempre atualizado evita inúmeros tipos de ataques de sistemas da informação, e não faltam escolhas no mercado, como o Avast, Kaspersky, McAfee, Avira, dentre diversos outros (JORGE, 2007).

Se mesmo seguindo as dicas da Tabela 2, ocorreu o clique na página e verificou o que um arquivo foi baixado, nunca execute ou abra qualquer arquivo de origem desconhecida, principalmente nos formatos “exe”, “pif”, “bat”, “com” e “scr”. Outra função importante é a configuração do e-mail e dos aplicativos mobile para não executar anexos imediatamente, evitando que um ataque de *phishing*, vírus e *spywares* seja instalado sem que o usuário perceba (JORGE, 2007).

Os criminosos cibernéticos fazem de tudo para aplicar golpes abusando da boa-fé e inocência das pessoas, a falta de conhecimento também ajuda na efetivação de um ataque malicioso, dessa forma, a conscientização e o estudo sobre os perigos enfrentados na internet e como evita-los, assim como explicados neste capitulo, permitem tornar capaz qualquer pessoa apta a se defender contra a prática de *phishing* e demais ataques que ferem os sistemas de segurança gerenciais.

5 CONSIDERAÇÕES FINAIS

Como observado, o principal motivo para a atualização do Direito Penal sobre as leis com amparo a segurança à cibercrimes ocorre principalmente em casos de repercussões na mídia, seja nacional ou internacional, sendo as duas principais alterações realizadas a Lei Caroline Dickmann e o Marco Civil da Internet.

Porém, o Marco Civil não regulamenta o lado Penal devidamente, sendo essa questão pouco elaborada, e com algumas leis dentro de outros contextos para a regulamentação, sem uma "Constituição" voltada para essa área. Como foi possível identificar as principais características do método de ataque *phishing*, que é o ataque mais comum no país para aplicação de golpes, ao adquirir dados sigilosos das pessoas.

Deve-se ler, compreender, aplicar e testar no cotidiano os métodos de prevenção à ataques é essencial para diminuir cada vez mais a taxa de casos de ataques no Brasil. As pessoas devem se conscientizar e não serem inocentes quando abrirem determinado site ou aplicação, seja pelo computador ou celular.

Isso ocorre porque os golpes podem ocorrer em qualquer hora, local e equipamento, seja através do *hardware*, *software* ou pelo ser humano, por isso, saber que esses problemas e possíveis com qualquer pessoa representa o necessário para aprender a combater estes males, tornando a internet do país um local mais seguro para todos.

E mesmo assim, as leis ainda pecam em atualização, sendo necessário o trabalho mais preciso do Direito Penal para realmente estabelecer o devido amparo ao usuário, não apenas trazendo meios de prevenção, mas realmente métodos para efetivar a Segurança da Informação, como por exemplo, uma evolução do Marco Civil da internet voltado apenas para a segurança e tipificando todos os crimes informáticos, trazendo uma organização mais precisa e direcionada sobre o que já foi regulamentado, permitindo entender melhor quais as novas leis devem ser analisadas e legisladas.

REFERÊNCIAS

ALEXANDRE JÚNIOR, J. C. Cibercrime: um estudo acerca do conceito de crimes informáticos. **Revista Eletrônica da Faculdade de Direito de Franca**, v. 14, n. 1, jun. 2019.

AVAST. ***WannaCry***. 2017. Disponível em: <https://www.avast.com/pt-br/c-wannacry>. Acesso em: 10 nov. 2019.

BARRETO, A. G.; KUFA, K.; SILVA, M. M. **Cibercrimes e seus reflexos no direito brasileiro**. Salvador: JusPODIVM, 2019

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. **Diário Oficial [da] União**, Brasília, 30 nov. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 10 out. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial [da] União**, Brasília, 14 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 10 out. 2020.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial [da] União**, Brasília, 23 abr. 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 out. 2020.

BROOKSHEAR, J. Glenn. **Ciência da Computação:** Uma visão abrangente. Porto Alegre: Bookman, 2013.

BORTOT, Jessica Fagundes. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. **VirtuaJus**, Belo Horizonte, v. 2, n. 2, p. 338-362, 2017.

CABRAL, I. **Segurança da informação em bibliotecas universitárias federais:** um levantamento sobre ferramentas e técnicas utilizadas. 2015. 80f. Trabalho de Conclusão do Curso (Bacharel em Biblioteconomia) – Universidade Federal de Santa Catarina, Florianópolis. 2015. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/133969/TCC%20APROVADO%20ISMAEL%20CABRAL%20UFSC%202015.pdf?sequence=1>. Acesso em: 10 nov. 2019.

CARDOSO, L. de H. M.; FRACASSO, C. R.; MARIN, M. M. A. **O direito na era digital:** o Cibercrime no Ordenamento Jurídico Brasileiro. 2018. Disponível em: < https://cepein.femanet.com.br/BDigital/arqPics/1611400792P734.pdf >. Acesso em: 05 mai. 2020.

CAPEZ, Fernando**. Curso de Direito Penal – Parte Gera**l – Vol. 1 – 18ªed. São Paulo: Saraiva, 2014;

CAIXA. ***Internet Banking*** **Caixa**. 2018. Disponível em: <https://internetbanking.caixa.gov.br/sinbc/#!nb/login>. Acesso em: 10 nov. 2019.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro; Brasport, 2014.

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança No Brasil. **Cartilha de Segurança para Internet**: Ransomware. Disponível em: <http://cartilha.cert.br/ransomware/>. Acesso em: 05 mai. 2020.

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança No Brasil. **Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)**. Disponível em: <http://www.cert.br/docs/whitepapers/ddos/>. Acesso em: 05 mai. 2020.

CORTELA, J. J. C. **Engenharia social no Facebook**. 2013. 44f. Trabalho de Conclusão de Curso (Bacharel em Ciência da Computação) – Universidade Estadual de Londrina, Londrina. 2013. Disponível em: <http://www.uel.br/cce/dc/wp-content/uploads/ProjetoTCC-JoaoCortela.pdf>. Acesso em: 10 nov. 2019.

CRUZ, D.; RODRIGUES, J. Crimes cibernéticos e a falsa sensação de impunidade. **Revista Científica Eletrônica do Curso de Direito**, v. 13, jan. 2018.

DANIEL IP. Conhecendo a Lei Geral De Proteção De Dados Do Brasil LGPD. 2019. Disponível em: <https://www.daniel-ip.com/wp-content/uploads/2019/02/Daniel_Cartilha_LGPD_atual_fev2019.pdf>. Acesso em: 10 out. 2020.

GARRETT, Filipe. **Golpes bancários crescem em 2020 e atingem mais de dez milhões no Brasil**. 2020. Disponível em: <https://www.techtudo.com.br/noticias/2020/07/golpes-bancarios-crescem-em-2020-e-atingem-mais-de-dez-milhoes-no-brasil.ghtml>. Acesso em: 20 ago. 2020.

GRANATO, F. R. de P. **A influência do discurso midiático e do clamor popular na recente produção legislativa penal brasileira:** os delitos eletrônicos e a Lei 12.737/12 (Lei Carolina Dieckmann). 2015. 56f. Trabalho de Conclusão de Curso (Bacharel em Direito) – Universidade Federal de Juiz de Fora, Juiz de Fora, 2015.

JORGE, P. G. **Fraudes na Internet**: Uma proposta de identificação e prevenção. 2007. 79f. Trabalho de Conclusão de Curso (Bacharel em Ciência da Computação) – Faculdade Santa Maria, Recife. 2007. Disponível em: <http://www.nogueira.eti.br/profmarcio/obras/Paulo%20-%20Fraudes%20na%20Internet.pdf>. Acesso em: 10 nov. 2019.

KASPERSKY. **Brasileiros são maiores vítimas de golpes phishing no mundo**. 2018. Disponível em: <https://www.kaspersky.com.br/blog/phishing-klsec-brasil-assolini/10642/?utm_source=newsletter&utm_medium=Email&utm_campaign=kd%20weekly%20digest>. Acesso em: 10 nov. 2019.

LAS-CASAS, P. H. B. et al. Uma metodologia para identificação adaptativa e caracterização de phishing. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 34., 2016. **Anais...** Salvador: UFBA.

LIMA, P. R. M. de; XAVIER, L. de O. O fenômeno do cybercrime sob a perspectiva do direito a privacidade. **Revista Eletrônica de Relações Internacionais do Centro Universitário Unieuro**, n. 16, p. 4-21. 2015.

MORGENSTERN, G. G.; TISSOT, T. R. G. Crimes cibernéticos: phishing – privacidade ameaçada. In: SEMINÁRIO DE INICIAÇÃO CIENTÍFICA, 23., 2015. **Anais...** Santa Rosa: FEMA.

NOLICORP. **Site Caixa *Phishing***. Disponível em: <https://noli.com.br/falso-e-mail-da-caixa-economica-federal/site-caixa-phishing/>. Acesso em: 10 nov. 2019.

OLIVO, C. K. **Avaliação de característica para detecção de phishing de e-mail**. 2010. 81f. Dissertação (Mestre em Informática) – Pontifícia Universidade Católica do Paraná, Curitiba. 2010. Disponível em: <https://www.ppgia.pucpr.br/pt/arquivos/mestrado/dissertacoes/2010/cleber_kiel_olivo_-_final.pdf>. Acesso em: 10 nov. 2019.

PAGANOTTI, Ivan. Pressão virtual e regulamentação digital brasileira: análise comparativa entre o Marco Civil da Internet e a Lei Azeredo. **Eptic Online**, v. 16, n. 2. 2014.

PEREIRA, L. de D.; MARTINS, D. M. S. Engenharia social: segurança da informação aplicada à gestão de pessoas – estudo de caso. **Caderno de Estudos em Sistemas de Informação**, v. 1, n. 2. 2014. Disponível em: 10 nov. 2019

ROMANI, Bruno. Fotos de Dieckmann nua tiveram 8 milhões de acessos; saiba como proteger as suas. **Folha de S. Paulo**, São Paulo, 14 maio 2012. Disponível em: <http://www1.folha.uol.com.br/tec/2012/05/1089392-fotos-de-dieckmann-nua-tiveram-8-milhoes-de-acessos-saiba-como-proteger-as-suas.shtml>. Acesso em: 05 mai. 2020.

SANTOS, A. F. C. **O cibercrime: desafios e respostas do direito**. Dissertação (Mestre em Direito) – Universidade Autónoma de Lisboa, Lisboa. 2015

SÃO PAULO. Ministério Público do Estado de São Paulo. **Visão geral sobre a lei nº 12.737/2012 ("Lei Carolina Dieckmann")**. São Paulo: MPSP.

SAVEGNAGO, J. U.; WOLTMANN, A. A regulamentação dos cibercrimes no brasil: uma análise jurídica dos "três pilares" norteadores do marco civil da internet. In: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 3., 2015. Santa Maria: RS. **Anais...** Rio Grande do Sul: UFSM. 2015.

SILVA, Marcelo Mesquita. **Ação internacional no combate ao cibercrime e sua inflência no ordenamento jurídico brasileiro**. 2012. 107f. Dissertação (Mestre em Direito) – Universidade Católica de Brasília, Brasília. 2012.

VERDELHO, P.; BRAVO, R.; ROCHA, M. L. (Orgs.). **Leis do Cibercrime**. Lisboa: Centro Atlantico, 2003

VERDELHO, P. **Cibercrime, in Direito da Sociedade da Informação**. Lisboa: Coimbra Editora, 2003.

TECHTUDO. **Os dez tipos de *phishing* mais comuns**. 2018. Disponível em: <https://www.techtudo.com.br/listas/2018/06/os-dez-tipos-de-phishing-mais-comuns.ghtml>. Acesso em: 10 nov. 2019.

TOMASEVICIUS FILHO, E. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, n. 86. 2016

ANEXO A – DECLARAÇÃO DE REVISÃO ORTOGRÁFICA

Eu, ELIANE CLEMENTE DA SILVA, graduada do curso de Licenciatura em Letras pela Faculdade Metodista de São Paulo, devidamente registrado no Ministério da Educação, declaro para a Faculdade Evangélica de Rubiataba, para todos os fins que foi realizado o ABSTRACT do trabalho de conclusão de curso de Graduação em Direito, intitulado: **CIBERCRIMES:** A INTERNET COMO FERRAMENTA NA EXECUÇÃO DE CRIMES VIRTUAIS E O COMBATE REALIZADO PELO DIREITO PENAL BRASILEIRO, do acadêmico **LUIZ FERNANDO BELIZÁRIO MACÊDO**.

Carmo do Rio Verde, 28 de agosto de 2020

Eliane Clemente da Silva

Eliane Clemente da Silva

ANEXO B – DECLARAÇÃO DE REVISÃO ORTOGRÁFICA, GRAMATICAL E DE NORMALIZAÇÃO TÉCNICA

Eu, ELIANE CLEMENTE DA SILVA, graduada do curso de Licenciatura em Letras pela Faculdade Metodista de São Paulo, devidamente registrado no Ministério da Educação, declaro para a Faculdade Evangélica de Rubiataba que revisei o trabalho de conclusão de curso de Graduação em Direito, intitulado: **CIBERCRIMES:** A INTERNET COMO FERRAMENTA NA EXECUÇÃO DE CRIMES VIRTUAIS E O COMBATE REALIZADO PELO DIREITO PENAL BRASILEIRO, do acadêmico **LUIZ FERNANDO BELIZÁRIO MACÊDO**. Consistente na correção ortográfica e gramatical, bem como na adequação das normas técnicas estipuladas pela Associação Brasileira de Normas Técnicas (ABNT).

Carmo do Rio Verde, 28 de agosto de 2020

Eliane Clemente da Silva

Eliane Clemente da Silva