O COMBATE AOS CRIMES VIRTUAIS

Caio César Fonseca de Souza[1]

RESUMO

O presente trabalho tem por objetivo mostrar a eficácia do Estado ao combate a crimes virtuais através de uma análise da sua atuação em diferentes níveis e da verificação de algumas informações relevantes sobre os crimes virtuais em si. Com o propósito de saber se o Estado brasileiro cumpre essa função de forma correta, e no caso de não cumprir, verificar o que o Estado faz de errado ou deixa de fazer, desse modo assim compreendendo o problema e através disso criar um debate que leve a uma possível solução, assim será possível dar mais segurança aos usuários de computadores e mostrando aos infratores que o Brasil não é o pais da impunidade. O trabalho será organizado de forma a se estudar três aspectos, os métodos de investigação da polícia, a incidência dos crimes virtuais e por fim como as leis auxiliam no combate, com essas informações poderemos saber como acontece o combate a crimes virtuais realizado pela polícia e pela legislação, além saber pelo dados obtidos pela incidência, se realmente a repressão desse crime pelo Estado tem efeito, sabendo assim quais são os desafios a serem enfrentados, e desse modo chegando a uma conclusão.

PALAVRAS-CHAVE:
Crimes virtuais. Investigação. Legislação.

ABSTRACT

This paper aims to show the effectiveness of the State in combating cyber crimes through an analysis of its performance at different levels and the verification of some relevant information about the virtual crimes themselves. With the purpose of knowing if the Brazilian State fulfills this function in a correct way, and in the case of not complying, verifying what the State does wrong or fails to do, thereby understanding the problem and thereby creating a debate that leads to a possible solution, so it will be possible to give more security to computer users and to show offenders that Brazil is not the country of impunity. The work will be organized in order to study three aspects, the methods of investigation of the police, the incidence of virtual crimes and finally how the laws assist in the combat, with this information we can know how happens the fight against virtual crimes by the police and by the legislation, besides knowing by the data obtained by the incidence, if indeed the repression of this crime by the State has effect, knowing thus what are the challenges to be faced, and thus reaching a conclusion.

---

[1] Aluno do curso de Direito, matriculado na disciplina TCC, orientados pelo Prof. Me. Francisco Joaquim Branco de Souza Filho.

KEY WORDS:
Virtual Crimes. Investigation. Legislation.

1 INTRODUÇÃO

Com a popularização da internet surgiu novos meios de emprego, de se informar, de adquirir conhecimento, de fazer amigos e de se divertir, mas como tudo não são flores, surgiram também novos meios de se cometer crimes como roubo de contas bancarias, divulgação de fotos ou vídeos íntimos de terceiros, a disseminação da pornografia infantil e vários outros tipos de males.

Embora os crimes de informática já existam desde a década de sessenta, eles só foram adquirir relevância na década de oitenta, quando houve maior propagação desses crimes. Com isso os governos começaram a criar formas de combater esse tipo de crime, nos Estado Unidos houve uma caçada ao hacker Kevin Mitnick, já no Brasil só se falou nisso com a Constituição Federal de 1988 na parte de leis relativas à competência do Estado sobre questões de informática.

Dentro desse contexto, questiona-se: O Brasil como país subdesenvolvido e com a sua máquina pública falha, da conta de combater esses crimes?; será que a nossa lei está apta para lidar com esse tipo de situação?; A polícia está preparada em termo de equipamentos ou conhecimento para achar e prender esses criminosos?

Desse modo esse Trabalho tem como objetivo geral: a) analisar a eficácia com que o Estado brasileiro com que o Estado brasileiro combate os crimes virtuais; para se atingir a esse proposito tem-se como objetivos específicos: b) verificar a eficiência dos métodos de investigação que a polícia emprega nesses crimes, c) identificar qual é o grau de reincidência dos autores de crimes virtuais, d) observar como o Direito combate os crimes relacionados a informática.

A justificativa dessa pesquisa é que segundo a matéria do Uol: “De acordo com um relatório da Norton Cyber Security, em 2017 o Brasil passou a ser o segundo país com maior número de casos de crimes cibernéticos, afetando cerca de 62 milhões de pessoas e causando um prejuízo de US$ 22 bilhões. No ano anterior, o Brasil era o quarto colocado na lista, mas agora fica atrás apenas da china, que em 2017 teve um prejuízo de US$ 66,3 milhões. ”

Segundo a matéria acima uns dos fatores deste aumento é a disseminação de smartphones, mas outros países têm uma disseminação maior de smartphones e não ficaram em quarto e agora em segundo lugar, então onde entra o Estado brasileiro para evitar esses crimes.

Segundo Patrícia Peck Pinheiro que é advogada em direito digital, o combate aos crimes cibernéticos deve ser mais ostensivo sendo necessário atualizações nas legislações quanto à capacidade de comprovação de autoria e quanto à tipificação dos crimes cibernéticos e a qualificação técnica das autoridades, ela ainda diz:

"Em alguns tipos de crimes, que vão da ameaça terrorista a fraude eletrônica, muito praticada com aplicativos falsos, que são os golpes da internet, se você não tiver uma ação imediata, em questão de horas desaparece toda a quadrilha e você não consegue pegar quem fez, fica só a vítima e resta a impunidade", ela disse isso defendendo a possibilidade do Ministério Público de julgar ações imediatas ou mais conhecidas como flagrante online.

O trabalho vai ter a finalidade básica estratégica e seu objetivo será descritivo, quanto a abordagem será usada a qualitativa, com relação ao método vai ser o indutivo e finalmente o procedimento será tanto bibliográfico com documental.

2. MÉTODOS INVESTIGAÇÃO, NOÇÕES DE INFORMATICA E DESAFIOS NA INVESTIGAÇÃO.

Como se sabe todos os crimes deixam rastros, no caso dos crimes virtuais esses rastos são mais voláteis sendo facilmente apagados ou modificados por isso é essencial a preservação dessas informações.

Outro detalhe a ser observado é que esses crimes podem ser praticados em qualquer lugar do mundo onde houver conexão com a internet, em outras palavras o criminoso pode do outro lado do mundo cometer um crime contra um cidadão brasileiro isso dificulta muito o trabalho da polícia tornando a revelação do autor do crime e a sua punição muito difícil de acontecer.

2.1 O Endereço IP e os Logs

O endereço IP (Internet Protocol) é a identificação das conexões de computadores ou redes locais com a internet, o IP é fornecido pelo provedor (empresa que fornece o serviço de internet), quando o usuário está online, quando ele está off-line esse endereço é cedido a outra pessoa, ou seja, não é uma coisa fixa variando conforme a data e horário em que o usuário está acessando a internet, exemplo: uma pessoa pode ter um endereço em um dia em determinada hora, quando essa pessoa sai da internet e vai fazer outra coisa e depois volta em outra hora no mesmo dia o provedor pode acabar fornecendo outro IP.

O endereço IP é de grande utilidade na investigação pois com ele é possível localizar o local onde o criminoso cometeu o ato ilícito, outra informação importante são os logs ou registros de acesso que basicamente gravam as ações do usuário durante a navegação na internet, logs são gravados em servidores (supercomputadores que controlam o acesso à internet dos usuários) das empresas que fornece o serviço de internet aos usuários.

É possível saber o IP de alguém através de um e-mail que ela enviou a uma pessoa, pelo gerenciador de e-mails que mostra o IP do remente da mensagem ou através de sites que registram o IP dos visitantes.

2.2 Evidências e métodos de investigações

Como foi dito acima quando se acessa ou compartilha alguma coisa ou simplesmente realiza qualquer ação em um site se cria um registro dessa ação, esses registros ficam guardados nos servidores do provedor, quando se recebe uma queixa de crime virtual e se inicia a investigação a primeira coisa a se saber é qual o endereço IP do infrator no dia, na hora e no fuso horário do sistema quando ocorreu a conexão no estante em que ocorreu o crime, depois devesse saber a qual provedor ele pertence, para isso deve se digitar o IP nos sites registo.com ou whois.sc.

Quando se obtiver o endereço IP na hora do crime e o provedor ao qual ele pertence o próximo passo é pedir a empresa que forneceu o IP a quebra do sigilo dos dados telemáticos através de autorização judicial.

Realizando todos os procedimentos acima citado ainda não será possível saber quem é o responsável pelo ato ilícito nem qual dispositivo ele usou para isso, só é possível saber quem é o dono da linha e os dados de acesso fornecidos pelo

provedor, é aí que entra a parte de busca e apreensão na residência apreendendo celulares e computadores ou qualquer coisa coma qual seja possível acessar a internet, por último devesse procurar as evidencias e as provas nos dispositivos de acesso à internet como por exemplo: arquivos digitais, registros de servidores, cookies (arquivos gravados no computador do internauta, que registram os sites que ele visitou), o histórico de navegadores, fotos ou vídeos, e-mails e registros de conversas on-line.

O advogado especialista em crimes virtuais Daniel Allan Burg, sócio do escritório de Direito Criminal Burg Advogados Associados, confirma essa informação sobre o procedimento supracitado:

> "Vamos supor que o Google seja o responsável por manter os dados cadastrais do autor da ofensa. Nós temos que enviar um ofício à empresa solicitando os dados. O Google apresenta os dados cadastrais, mas, com base no Marco Civil da Internet, se recusa a fornecer o IP (internet protocol) e outros dados que necessitam de autorização judicial para se obter. Em regra, até o Google responder isso, a autoridade policial remeter o inquérito para o fórum e ter a representação judicial, um considerável tempo já se passou. É preciso ser bastante claro com o cliente que procura um advogado com esse tipo de caso de que é possível que o resultado almejado pode não ser alcançado por causa desses entraves. Além disso, nós que atuamos nessa área precisamos ficar atentos e cobrar celeridade nesse processo. De certa forma a internet criou a impunidade para a prática de alguns crimes. "

O endereço MAC é o número que identifica a placa de rede do dispositivo computacional, com ele é possível que os peritos identifiquem o dispositivo específico usado na pratica do crime, o site da receita federal possui softwares que rasteiam o endereço MAC, com isso basta pedir a receita federal esse endereço.
O programa HTTrack Website Copier pode fazer cópias completas de sites para um diretório local do computador do investigador. Assim é possível fazer uma navegação completa pelo site copiado sem levantar as suspeitas do dono da página caso ele esteja cometendo crime, dessa forma evitando que ele faça modificações na página apagando provas importantes.

Outra ferramenta importante na investigação é o programa MD5summer que verifica a integridade dos arquivos, gerando assinaturas digitais (hashes) nesses

arquivos, sendo assim possível ver se um arquivo é original ou foi modificado (WENDT e JORGE,2013), os dados dentro do documento do site podem achar o e-mail do criminoso (Brasil, 2013).

2.3 Dificuldades Materiais

Existem vários obstáculos a serem superado um deles é a dificuldade de se obter a origem de um evento na internet, um exemplo são os meios de burlar o IP através de proxies, redes wifi abertas, os cyber cafés, lan houses.

Os proxies são serviços que ocultam o verdadeiro IP utilizado em um evento de internet, já as redes wireless ou wifi abertos permitem o uso de pessoas não identificadas, no caso das lan houses e cyber cafés há uma falta de registro dos usuários o que torna possível que o criminoso possa usar falso e-mails ou qualquer outra coisa que permita o anonimato do crime.

O conhecimento que se deve ter de terminologias quanto de conhecimento em si é muito grande e muitos policiais e investigadores não possuem esse conhecimento, isso causa um grande problema já que mais da metade não é capaz de investigar esse tipo de crime, e como esse tipo de crime já é mais fácil de sair impune pois não se precisa estar no local do crime e não há muitos agentes investigando para uma modalidade de crime cujo o Brasil está em segundo em incidência então fica mais difícil para o Estado brasileiro punir os crimes cibernéticos. Daniel Burg fala sobre a facilidade que a internet deu aos criminosos para praticar crimes:

> “Facilitou é uma boa definição. Os crimes continuam os mesmos, mas se aumenta a gama da forma como eles podem ser praticados. Antigamente o sujeito que queria obter R$ 200 mil ia pegar uma arma e assaltar um banco. Hoje, se ele tem um conhecimento virtual um pouco mais avançado, consegue por detrás do computador, sabendo da dificuldade que as autoridades têm de identificar autoria, entrar numa conta e surrupiar esses valores. Então, facilita a prática de um crime e até cria uma nova tendência, sobretudo dos crimes patrimoniais. Não só dos crimes contra a honra, mas também de crimes patrimoniais. ”

Nos crimes praticados por e-mails há a dificuldade que certos provedores não possuem registros apropriados, o que pode resultar em um equívoco durante o processo, recaindo a autoria do crime sobre um usuário que de fato não praticou o delito (Brasil, 2013).

Outro problema é a utilização de esteganografia por internautas, que é um meio de mandar mensagens privadas e por essa causa cria muita dificuldade para os investigadores. As técnicas variam muito de um software para outro, por isso, o investigador deve ter conhecimento sobre os programas e técnicas mais comuns empregados nesse sistema de códigos, para que seja possível operar efetivamente em diferentes casos (Brasil ,2013).

Por fim existe o problema que é o cloud computing ou computação em nuvem, que permite a disponibilidade de um computador para que seja acessado pelo usuário via internet, ficando todo o conteúdo salvo em servidores brasileiros ou estrangeiros. Se os dados do crime estiverem em servidor estrangeiro isso dificultará, demorando ou até mesmo não sendo possível conseguir as informações para a investigação, considerando que o Brasil não é signatário da convenção de Budapeste, também conhecida como convenção sobre cibercrime, que trata da cooperação internacional para a persecução de crimes virtuais (WENDT e JORGE, 2013).

2.4 Criptografia

A criptografia é técnica que embaralha a mensagem para torna-la incompreensível, essa técnica foi muito usada antigamente na espionagem, na internet se usa a criptografia para se, manter a privacidade na conversa entre duas pessoas no whatsapp, ou proteger transações bancarias ou qual quer informação que se requer sigilo.

A criptografia na internet embaralha a mensagem e depois a transforma em números e a envia para o destinatário que depois e decodificada, isso permite que apenas o destinatário e o remetente possam ter acesso a mensagem decodificada. O problema é como apenas o destinatário e o remetente tem acesso a informação decodificada faz com que os provedores não possam fornecer qualquer informação para a autoridade legal, o que torna mais complicado concluir a investigação de crimes na internet.

Ouve uma briga entre a Apple e o FBI na justiça, pelo fato da apreensão de um iPhone 5c, que era de um dos envolvidos no massacre em San Bernadinho. A polícia americana não era capaz de acessar os dados do iPhone, pois a Apple passou a criptografar todo o conteúdo de seus equipamentos e somente a senha poderia dar acesso aos dados. A técnica da força bruta (Técnica que gera todas as combinações de senha possíveis para tentar acesso a um sistema) não foi suficiente para resolver o problema, pois o equipamento poderia apagar todo o conteúdo se fizessem onze tentativas erradas. O FBI informou que consegui a senha sem a ajuda da Apple, sem explicar como.

2.5 Bitcoins uma forma eficiente de lavar dinheiro

Os bitcoins são moedas virtuais as quais se permitem fazer transações na internet, é possível compra-los com dinheiro comum, através dos bitcoins é possível fazer transações pela internet em vários países do mundo através de sites, muitas dessas transações podem ser ilícitas como explica ULRICH (2014):

> "Bitcoin é uma moeda digital descentralizada, que permite efetuar transações financeiras sem intermediários, sem taxas, em qualquer parte do planeta, sem criar limites ou requisitos atrelados ao possuidor da moeda. "

Ao contrário da lavagem de dinheiro tradicional, que deixa rastros os quais a polícia pode seguir até chegar os criminosos, os bitcoins não deixa rastros, já que sites de cambio transforma dinheiro ilícito em legal, por que os bitcoins não possuem meios de fiscalização ou supervisão por qualquer órgão regulamentador, com isso o dinheiro pode ser usado em transações legais sem se saber qual é sua origem.

Na deep web que é uma rede sem supervisão onde se pode fazer todo tipo de coisa como vender ilícitos, é possível fazer compra de armas ou drogas através dos bitcoins, sem saber tanto quem comprou ou vendeu.

2.6 Deep web

Vamos supor que a rede de internet é um grande iceberg, como se sabe o iceberg tem uma pequena parte que fica fora da agua, a maior parte fica submerso. A surface web como é conhecida é a web comum que nós conhecemos que onde a maioria dos usuários acessão, ou seja, sites como youtube, facebook e etc; fazem parte dessa surface web, já parte submersa do iceberg seria a deep web onde poucas pessoas tem acesso dado o fato que é mais difícil de acessar.

A surface web corresponde a apenas 4% da rede, todo o restante pertence a deep web, mais o que é essa deep web? A deep web é a parte da internet que não é indexada pelos mecanismos de busca, como o google por exemplo, ficando oculta para a maior parte das pessoas.

Na deep web é possível navegar de forma anônima por isso nela é que se guardam dados que são cruciais para a manutenção da rede, que não pode ser acessado por qualquer usuário como por exemplo bancos de dados acadêmicos, registros médicos, informações confidenciais de segurança nacional, registros financeiros, artigos científicos, repositórios de algumas ONGs e etc.

Existem várias formas de se acessar a deep web pois ela é composta de várias redes separadas, que não se comunicam entre si, uma dessas formas é pelo tor que é um software que possui o código aberto, com isso é possível navegar pela deep web de forma anônima. Uma das páginas que é possível na deep web é o silk road que nada mais é um site de venda de drogas ilícitas.

Existe uma parte mais profunda da deep web e essa seria a dark web. A dark web faz parte da deep web porem na dark web os domínios (endereços dos sites como por exemplo https://www.youtube.com/) são compostos por strings de letras e números sem o menor sentido, e apenas quem possui os domínios e credenciais completos é autorizado a entrar nesses sites. A dark web é usada na pratica de crimes como por exemplo o silk road que já foi citado.

Quanto as atividades ilegais que podem ser praticadas na dark web um exemplo delas além do tráfico de drogas é a venda de armas ilegais, trafico de órgão humanos, serviços de assassinos de aluguel, pornografia infantil, venda de escravas sexuais e alguns boatos falam das salas vermelhas que supostamente seriam espaços onde uma pessoa é torturada por outras e sendo assistida por várias onde elas pagariam para que a tortura continuasse ou para que os torturadores matassem a vítima. A moeda de troca dessas atividades ilegais é o bitcoin pois como já foi dito o bitcoin garante o anonimato.

O 4chan são fórum de conversas onde não é necessário cadastro para participar ou seja não precisa se identificar para colocar mensagens, o problema é o que o 4chan da dark web a conversa é mais obscura, lá rola assuntos racista, a favor de violência contra mulher já que em certos grupos se reúnem homens que não conseguem arranjar parceiras sexuais, em outros são grupos formados por garotos que sofrem bully e por isso quando um pensa em se suicidar os outro não só o encorajam como também o aconselham a levar outras pessoas no processo, é nisso que acontece esse atentados nas escolas como no caso de Suzano, também fica mais fácil organizar atentados terroristas e ação de quadrilha.

3. A INCIDENCIA DE CRIMES VIRTUAIS NO BRASIL

Segundo uma matéria do UOL os crimes virtuais têm uma média de 38% no mundo enquanto que no Brasil a média é de 274% entre 2014 e 2015, de acordo com a consultoria PwC, a matéria continua: " O usuário comum é peça chave nessa equação. A última pesquisa do IBGE focada na posse, uso e acesso da população a tecnologias, de 2015, mostrou que 58% dos brasileiros (102 milhões de pessoas) acessavam a internet. Dados coletados no mesmo período pela Avast-procuradora de softwares antivírus. "

O jornal o globo diz que a companhia holandesa de segurança digital Gemalto divulgou um relatório afirmando que houve mais de 1.500 vazamentos de dados por hackers em 2014 que gerou um comprometimento de mais de mais de um bilhão de informações durante o ano 78% maior que 2013, a matéria também cita que a impunidade é um atrativo para os hackers.

> "Devido ao problema carcerário do país, nosso Judiciário tende a optar por penas alternativas. Em geral, esses crimes cibernéticos não são praticados com grave ameaça ou violência, o que fez com que a pessoa, num primeiro momento, não fique presa",

Diz o delegado da P.F Stênio Santos e continua:

> ” quando o crime é de fraude bancária e de pornografia infantil, temos percebido a reincidência. Muitos criminosos sentem ser mais vantajoso praticar o ilícito, ser preso, sair e voltar a praticar o cyber crime do que buscar um emprego formal. “

O Norton Cyber Security diz que o Brasil passou da quarta posição em 2017 para a segunda posição em 2018 em caso de crimes virtuais.

4. A LEI COMO INSTRUMENTO DE COMBATE

Antes a legislação era muito fraca pois não havia uma legislação especifica para os crimes virtuais, com o tempo esses crimes foram se tornando mais graves e sua incidência foi se tornando relevante o que fez com que o Estado brasileiro tivesse que prestar mais atenção a esse tipo de crime.

Um dos casos que repercutiu na mídia e fez com que o Estado tivesse que dar uma resposta a população foi o caso da atriz global Carolina Dieckmann que teve suas fotos intimas divulgadas pela internet.

Existem outros casos posteriores que também repercutiu na mídia como o caso da cantora Preta Gil que sofreu ataques de racismo na internet e muitos outros artistas que sofreram racismo ou qualquer outro tipo de crime cometido pela internet.

O grande problema com os crimes virtuais é que não existia antes do marco civil e da lei Carolina Dieckmann legislação especifica, ou seja, quando alguém invadia o computador de outra pessoa, o invasor só podia ser criminalizado por outro crime que já existia anteriormente e não precisava necessariamente de um computador com por exemplo o próprio crime cometido contra atriz Carolina Dieckmann em que os hackers obtiveram suas fotos e depois pediram dinheiro, nesse caso o crime cometido seria a extorsão ou seja se caso não houvesse a extorsão não haveria crime, pois não era crime simplesmente invadir o computador alheio e bisbilhotar a privacidade ou obter fotos intimas.

4.1 A lei Caroline Dieckmann e o marco civil da internet

A lei 12.737/2012 mais conhecida como lei Caroline Dieckmann criou algumas alterações no código penal, a principal delas é a criação do artigo 154-A e

154-B, esses artigos são específicos para os crimes virtuais já que antes dessa lei não havia tipo penal especifico para crimes virtuais, vejamos essas modificações:

> 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: (Incluído pela Lei nº 12.737, de 2012)
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (Incluído pela Lei nº 12.737, de 2012)
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (Incluído pela Lei nº 12.737, de 2012)
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. (Incluído pela Lei nº 12.737, de 2012)
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012)
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (Incluído pela Lei nº 12.737, de 2012)
>
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. (Incluído pela Lei nº 12.737, de 2012)
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012)
>
> I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012)
>
> II - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012)
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou (Incluído pela Lei nº 12.737, de 2012)
>
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012)
>
> 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. (Incluído pela Lei nº 12.737, de 2012) Vigência

A lei com o intuito de combater os crimes virtuais tem algumas falhas como por exemplo no artigo 154-A a pena é muito fraca sendo de apenas três meses a um ano, além de pouco tempo a pena prescreve em três anos. O artigo também fala que a mera invasão do dispositivo informático de terceiro não é crime, pois o crime deve ter como finalidade especifica de obter, adulterar ou destruir dados e informações. Além disso tem o fato que para haver o cometimento do crime é necessário a invasão do mecanismo de segurança, ou seja, se o dispositivo invadido não tiver firewall, antivírus ou senha, a conduta será atípica, e ainda o mecanismo de segurança deve ser indevidamente violado, e qual o problema disso vejamos um exemplo (BERETTA, 2014):

> "A e B são amigos e cada um está com o seu computador (conectado ou não à rede de computadores). A solicita a B seu notebook emprestado, pois o dispositivo informático de A está acabando a bateria. B autoriza o acesso de seu amigo. A, no entanto, sabia que seu amigo, B, estava tendo relações com sua namorada. Assim, com o fim de obter, adulterar ou destruir dados ou informações, ao utilizar o computador de B, A verifica que existem diversas fotos de B com sua namorada em momentos íntimos. Este, por sua vez, ingressa no sistema de fotos do computador de B e obtém, altera-as e apaga todas as fotos para posterior publicação na Internet. " (BERETTA, 2014)

> "Afinal, pergunta-se: "A" praticou o crime descrito no artigo 154-A do Código Penal? Não, pois, além de não utilizar-se de nenhum mecanismo de violação para o acesso ao dispositivo, a autorização existiu tacitamente, e como sabemos, o dolo é a vontade livre e consciente de realizar todos os elementos descritos no tipo penal. " (BERETTA, 2014)

A lei número 12.965/14 (marco civil da internet) regula vários pontos sobre a internet, mas o que nos interessa é a obrigação das empresas que fornece internet

de guardar logs (registro de dados sobre data, horário e duração de acesso à internet) no prazo de um ano para fins de investigação previsto no artigo 10:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> § 1o O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7o.
> § 2o O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7o.
> § 3o O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
> § 4o As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Outro aspecto importante é o direito à privacidade a internet dado pela lei no artigo 7:

> Art. 7o O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

Com isso a invasão de privacidade do computador pode ser punida, algo que não acontecia no artigo 154-A.

O advogado Daniel Burg responde quando questionado sobre a eficácia da lei Carolina Dieckmann e do Marco Civil da internet no combate a crimes virtuais:

> "A Lei Carolina Dieckmann não é. Apenas trouxe um novo dispositivo, inclusive redigido de forma bastante confusa, também com prazo prescricional de pena bastante baixa. Eu não ouvi falar de nenhuma denúncia recebida envolvendo esse tipo de crime. E o Marco Civil da Internet, por enquanto, para manter no exemplo que eu dei ao falar que o IP e outros dados que somente podem ser fornecidos com representação judicial, prejudica o ofendido. Como iniciativa, pelo menos dá para ver, existe alguma intenção do Legislativo em trazer ao mundo das leis alguns dispositivos para tratar do tema, mas como conteúdo ainda é muito pouco. Se o legislador pegasse uma coletânea de situações, decisões e artigos jurídicos do que vem acontecendo no dia a dia dos crimes virtuais com certeza veria que tem muita coisa para melhorar. "

5. CONSIDERAÇÕES FINAIS

Nesse trabalho podemos concluir que o Brasil precisa evoluir muito tanto em legislação como no preparo da polícia, pois não existem muitas leis específicas para o caso de crimes virtuais o que deixa brechas (como vimos nesse trabalho) para que os criminosos se aproveitem da situação não é à toa que o Brasil está em segundo lugar em incidência de crimes virtuais.

A reincidência é um grande fator de impunidade já que é uma espécie de crime complexo de ser investigado e nos casos de crimes com menores penas como os crimes contra a honra em que há um grande risco de haver prescrição e caso não haja ainda tem o fato de que é uma pena muito pequena no caso de extorsão ou roubo de informações, além de que é muito mais difícil se ser pego já que existem várias formas de se garantir o anonimato como no caso da Deep Web.

Quanto à polícia que não possui um preparo para boa parte dos seus agentes fazendo com que não tenham condições de participar de uma investigação de crimes virtuais, além do fato de que existem os meios de se cobrir os rastos do crime como a Dark Web e outros meios citados no artigo, tornado assim o trabalho mais difícil e necessitando de um preparo ainda maior.

Enquanto não a polícia não tiver os melhores cursos de preparo para a investigação de crimes virtuais e o governo criar uma legislação especifica que preencha as lacunas na lei e facilite o combate aos crimes na internet, então os índices desses crimes continuaram autos.

REFERÊNCIAS

CAVALCANTE, W.F. **Crimes Cibernéticos**: Noções Básicas de Investigações e Ameaças na Internet.

LESSA, I.M.B.; VIEIRA, T.V. **Crimes Virtuais:** Análise do Processo Investigatório e Desafios Enfrentados.

MATSUURA, Sérgio. JANSEN, Thiago. **Onda de crimes praticados por hackers cresceu 197% no Brasil em um ano**. Disponível em: https://oglobo.globo.com/economia/onda-de-crimes-praticados-por-hackers-cresceu-197-no-brasil-em-um-ano-17197361

MUNDO DOS HACKERS. **Como conseguir o IP de alguém.** Disponível em: http://www.mundodoshackers.com.br/como-conseguir-o-ip-de-alguem

HARADA, Eduardo. **Tecmundo Explica: o que é essa tal de "Deep Web"?** Disponível em: https://www.tecmundo.com.br/tecmundo-explica/74998-tecmundo-explica-tal-deep-web.htm

HIGA, Paulo. **Como entrar na Deep Web utilizando o Tor**. Disponível em: https://tecnoblog.net/189897/como-acessar-deep-web-links/

GORGONI, Ronaldo. **Deep Web e Dark Web: qual a diferença?** Disponível em: https://tecnoblog.net/282436/deep-web-e-dark-web-qual-a-diferenca/

BERETTA, Pedro. **Sem meios eficazes, Lei Carolina Dieckmann até atrapalha**. Disponível em: https://www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha

CONJUR. **"Internet facilita crimes e dificulta investigação, estimulando a impunidade"**. Disponível em: https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais

SHIMABUKURO, A. **Cibercrime**: quando a tecnologia é aliada da lei.

JORNAL DO COMERCIO. **Crimes virtuais disparam no Brasil**. Disponível em: https://jconlineinteratividade.ne10.uol.com.br/canal/economia/nacional/noticia/2017/08/29/crimes-virtuais-disparam-no-brasil-303855.php

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos:** Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.