CENTRO DE EDUCAÇÃO SUPERIOR REINALDO RAMOS - CESREI
FACULDADE REINALDO RAMOS - FARR
CURSO DE BACHARELADO EM DIREITO

BRUNO CÉSAR DE BRITO

CYBERCRIMES: OS CRIMES NA ERA DA INFORMÁTICA: UMA ANÁLISE APROFUNDADA DOS DELITOS CYBERNÉTICOS OU DE INFORMÁTICA E SUA CONGRUÊNCIA COM O ATUAL ORDENAMENTO JURÍDICO BRASILEIRO

CAMPINA GRANDE – PB
2019

BRUNO CÉSAR DE BRITO

CYBERCRIMES: OS CRIMES NA ERA DA INFORMÁTICA: UMA ANÁLISE APROFUNDADA DOS DELITOS CYBERNÉTICOS OU DE INFORMÁTICA E SUA CONGRUÊNCIA COM O ATUAL ORDENAMENTO JURÍDICO BRASILEIRO

Monografia apresentada como pré-requisito para a obtenção do título de Bacharel em Direito pelo Centro de Educação Superior Reinaldo Ramos/CESREI.

Orientador: Prof. Ms. Rodrigo Araújo Reul.

CAMPINA GRANDE – PB
2019

B862c Brito, Bruno César de.
Cybercrimes: os crimes na era da informática: uma análise aprofundada dos delitos cybernéticos ou de informática e sua congruência com o atual ordenamento jurídico brasileiro / Bruno César de Brito. – Campina Grande, 2019.
95 f.

Monografia (Bacharelado em Direito – Faculdade Reinaldo Ramos-FAAR, Centro de Educação Superior Reinaldo Ramos-CESREI, 2019.
"Orientação: Prof. Me. Rodrigo Araújo Reul".

1. Crimes na Internet. 2. Cybercrime. 3. Cyberespaço. 4. Crimes Virtuais 5. Legislação Vigente. I. Reul, Rodrigo Araújo. II. Título.

343.6:004.738.5 (043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

BRUNO CESAR DE BRITO

CYBERCRIMES: OS CRIMES NA ERA DA INFORMÁTICA E SUA CONGRUÊNCIA COM O ATUAL ORDENAMENTO JURÍDICO BRASILEIRO

Aprovada em: 12 de JUNHO de 2019.

BANCA EXAMINADORA

Prof. Ms. Rodrigo Araújo Reul

Faculdade Reinaldo Ramos FARR/ CESREI

(Orientador)

Profa. Ms. Vyrna Lopes Torres de Farias Bem

Faculdade Reinaldo Ramos FARR/ CESREI

(1º Examinador)

Profa. Esp. Ana Caroline Câmara Bezerra

Faculdade Reinaldo Ramos FARR/ CESREI

(2º Examinador)

Aos que não estão aqui,
mas ainda assim,
fazem parte de mim.
Para vocês, meus dois Luiz.

AGRADECIMENTOS

Um trabalho de conclusão de curso é o resultado do empenho de quem o constrói, do auxílio de quem o orienta e da colaboração de todos os que durante o seu desenvolvimento são partícipes, sendo essencial o agradecimento.

Agradeço e dedico essa conquista primeiramente a Deus, por me permitir que tudo isso que hoje estou vivendo pudesse acontecer. Foi difícil. E é a plena realização de um sonho. De verdade. Tu, Senhor, és o maior mestre que alguém pode conhecer e pode ter ao lado!

Agradeço às minhas heroínas, vovó Maria Amélia, e minha mãe Lélia Maria, pelo amor, incentivo, apoio incondicional e cada oração. Vocês são meu porto seguro. Não me imagino sem vocês por um minuto. Obrigado por todo o apoio, incentivo nas horas difíceis, de desânimo, cansaço e tristeza. E meu agradecimento se estende a tudo que vocês fizeram por mim por toda a minha vida acadêmica, desde a escola Balão Mágico, passado pelo *Mather Christi*, Colégio Santa Cruz, Alternativo, Colégio Pio XI, Alfredo Dantas. Só nós sabemos o que passamos, não é verdade, minhas "*véinhas*"? Mas a vitória chegou... Ela é nossa!

Dedico*, in memorian*, ao meu vô Luiz Miranda de Brito, por todo o amor e carinho que sempre teve por mim. Exemplo de pai, meu *avohai*, imagem personificada de uma ausência paterna, mas que nunca me deixou faltar nada. Muito menos carinho e cuidado. Lembro com muita alegria das vezes que o senhor ia me buscar na escola, quando pequeno. Quem diria, "*hein"*? Seu neto está formando! Impossível não falar de ti sem as lágrimas correrem em meu rosto. Deus sabe da saudade que sinto de ti. Mas sei que estás presente de alguma forma.

In memorian, ao meu irmão Luiz Neto, por cada momento compartilhado, de uma infância maravilhosa. Lembrar da nossa infância transborda meu coração de amor e alegria. Meu sempre companheiro para "fazer arte". Obrigado por ter-nos apresentado ao Senhor como hoje conhecemos, e plantado a semente do servir. Sinto sua falta e queria muito que estivesses aqui, para eu te dar um abraço e te ajudar a conquistar o mesmo. Para você me ajudar com a nossa casa, com nossa vovó, tão velhinha e frágil, e com nossa mamãe, tão guerreira. Você merecia, meu

irmão. Nós merecíamos te ver alcançando voos altos também. Mas a vontade do Senhor é boa, perfeita e agradável. Como diz a letra daquela canção de Catedral, *“tenho certeza que vou te encontrar, não sei o dia, nem a hora, mas sei bem o lugar; sei que você está bem, mesmo assim, isso não me impede de chorar...”*

Agradeço ao meu pai, por ter plantado, lá em 2008, a sementinha em meu coração, de concluir um curso superior, mais precisamente o curso de Bacharelado em Direito, reacendendo uma vontade e um sonho de infância.

Agradeço, também, aos meus orientadores, Lamartine Lacerda e Rodrigo Reul, por todos os ensinamentos a mim transmitidos, pela paciência e pelo aceite do convite para encararem esse desafio de abordar um tema tão recente comigo, mas tão pertinente e relevante na nossa atualidade, mesmo sem termos atualmente uma base sólida construída dentro do ordenamento jurídico brasileiro. Vocês são exemplos, referências para mim, como profissionais, como cidadãos, sobretudo como docentes.

A todos os professores do curso de Direito das instituições em que tive a honra de fazer parte e que contribuíram com seus conhecimentos para o êxito da minha formação profissional, independentemente de onde estejam hoje.

E não poderia esquecer dos meus amigos, pessoas que contribuíram com sua valiosa amizade para conclusão desse trabalho, em especial a Josefa (Bolinha), por cuidar da minha vó enquanto eu corria atrás desse sonho, desse meu objetivo. Esses últimos meses você tem sido nossa melhor companhia, sempre com uma palavra de alento, sempre trazendo um sorriso, uma alegria para nossa casa; obrigado por tudo. A Marcos Vinícius e a Carlos Itamar, dois grandes irmãos que a vida me agraciou, amigos sempre presentes e a quem eu sempre recorria quando precisava de ajuda; Dois incentivadores e motivadores quando eu me via desanimado.

Estendo meus agradecimentos à minha família gaúcha por adoção, em Canela, estado do Rio Grande do Sul, em especial na pessoa de Odeti Michaelsen e Lauro Azevedo, refúgio de carinho e afeto quando eu me encontrava extremamente cansado e decidia descansar dessa loucura que foi minha graduação. Hoje mais ainda tenho ciência que uma família é formada não somente pela relação sanguínea que seus membros possuem, mas pelos laços de amor, de carinho, de respeito e

admiração que se estabelecem entre eles. É inexplicável meu sentimento por vocês, mesmo diante dos 3.800km que nos separam. Vocês de alguma forma também fazem parte dessa minha conquista.

Não existe espaço e nem palavras suficientes para agradecer a todos que de alguma forma contribuíram para que eu alcançasse essa conquista. A todos vocês meu carinho e meu muito obrigado, de coração!

“Por isso não desanimamos. Embora exteriormente estejamos a desgastar-nos, interiormente estamos sendo renovados dia após dia, pois os nossos sofrimentos leves e momentâneos estão produzindo para nós uma glória eterna que pesa mais do que todos eles. “

2 Coríntios 4:16-17

RESUMO

A utilização da internet e da tecnologia por criminosos está incluída na modalidade dos crimes virtuais, constituindo-se um dano realizado via internet ou através de ferramentas ou instrumentos digitais. Na realidade, em face do dinamismo da tecnologia, muitas são as dificuldades encontradas para resolução de tais crimes e poder punir com rapidez e com a severidade que a sociedade já cobra da classe judiciária e política legislativa. Entretanto, a legislação brasileira vem buscando, através das leis já existentes e com novas leis, garantir a punição desses crimes e o cumprimento destas mesmas leis segundo os rigores da justiça, acompanhando os avanços do crime digital e atualizando o ordenamento jurídico para tipificar as condutas e adaptar o crime praticado no ambiente virtual – já tão parte do cotidiano dos cidadãos brasileiros - ao nosso conjunto de normas e regras. Os crimes virtuais encontram-se tipificados de acordo com a legislação especifica, bem como a conduta desta nova modalidade criminal, que tem acarretado danos aos cidadãos e a sociedade. Entende-se que uma intensa discussão no âmbito acadêmico sobre o combate ao cybercrime é de extrema pertinência, a fim de contribuir para uma reflexão sobre a segurança pessoal e empresarial, tanto nacional como internacional. Apesar desta problemática ser recente, surgindo com a explosão tecnológica do final dos anos 80/90 e que trouxe consigo problemáticas novas, se acentuou no século 21, carecendo, isto posto, de uma legislação mais efetiva e própria. A principal função deste trabalho é dirimir dúvidas sobre as ferramentas utilizadas pelos cybercriminosos, fazer uma diferenciação entre eles mediante suas técnicas, entender o campo virtual e cibernético como um meio de se cometer o delito ao mesmo tempo em que é local para o cometimento do ilícito, além de entender a aplicabilidade da legislação e de que forma o judiciário e o legislativo brasileiro vem abarcando esta nova demanda. Ademais, trazer prognose, circunstâncias e discutir formas de diminuir a demanda de crimes cybernéticos, trazidos pelo aumento exacerbado de redes sociais e sites de relacionamento são as égides que movem o presente trabalho.

Palavras-chave: 1. Cybercrime; 2. Cyberespaço; 3. Crimes Virtuais 4. Legislação Vigente

RESUMEN

La utilización de Internet y de la tecnología por criminales está incluida en la modalidad de los crímenes virtuales, constituyéndose un daño realizado vía internet oa través de herramientas o instrumentos digitales. En realidad, frente al dinamismo de la tecnología, muchas son las dificultades encontradas para resolución de tales crímenes y poder castigar con rapidez y con la severidad que la sociedad ya cobra de la clase judicial y política legislativa. Sin embargo, la legislación brasileña viene buscando, a través de las leyes ya existentes y con nuevas leyes, garantizar el castigo de esos crímenes y el cumplimiento de estas mismas leyes según los rigores de la justicia, acompañando los avances del crimen digital y actualizando el ordenamiento jurídico para tipificar las conductas y adaptar el crimen practicado en el ambiente virtual-ya tan parte del cotidiano de los ciudadanos brasileños- a nuestro conjunto de normas y reglas. Los crímenes virtuales se tipifican de acuerdo con la legislación específica, así como la conducta de esta nueva modalidad criminal, que ha acarreado daños a los ciudadanos ya la sociedad. Se entiende que una intensa discusión en el ámbito académico sobre el combate al cybercrime es de extrema pertinencia, a fin de contribuir a una reflexión sobre la seguridad personal y empresarial, tanto nacional como internacional. A pesar de que esta problemática es reciente, surgiendo con la explosión tecnológica de finales de los años 80/90 y que trae consigo problemáticas nuevas, se acentuó en el siglo XXI, careciendo, esto puesto, de una legislación más efectiva y propia. La principal función de este trabajo es dirimir dudas sobre las herramientas utilizadas por los cybercriminantes, hacer una diferenciación entre ellos mediante sus técnicas, entender el campo virtual y cibernético como un medio de cometer el delito al mismo tiempo en que es local para la comisión del ilícito, además de entender la aplicabilidad de la legislación y de qué forma el judicial y el legislativo brasileño vienen abarcando esta nueva demanda. Además, traer pronos, circunstancias y discutir formas de disminuir la demanda de crímenes cybernéticos, traídos por el aumento exacerbado de redes sociales y sitios de relación son las égides que mueven el presente trabajo.

Palabras clave: 1. Cybercrime; 2. Ciberespacio; 3. Crímenes Virtuales 4. Legislación vigente

SUMÁRIO

INTRODUÇÃO

Atualmente, a Internet – de forma incontestável - faz parte da rotina diária da sociedade, seja de uma forma ou de outra, não apenas aqui no Brasil como em todo o mundo, e, de forma totalmente cotidiana, tornou-se uma tecnologia fundamental para as relações sociais e empresariais. A Internet tornou-se imprescindível e fundamental para grande parte da população mundial. É através da internet que conseguimos estudar, realizar transações financeiras, comprar produtos, nos comunicar através das redes sociais, trabalhar remotamente, enviar e receber arquivos, enfim, uma vasta possibilidade de operá-la, de manuseá-la.

Ocorre que, conjuntamente com o todos os privilégios e benesses que a internet nos trouxe, surgiram os chamados cybercrimes, ou, em português, crimes virtuais.

Cybercrimes, Crimes Informáticos, Crimes Digitais, Crimes Virtuais, Crimes Eletrônicos, Crimes Cibernéticos, são apenas alguns dos termos mais usados nos dias de hoje para determinar os delitos - desde dados pessoais até as infrações de conteúdo e de *copyright* - praticados contra ou através de computadores. Neste tipo de crime, podem ser incluídos ações como fraude e acessos proibidos, o *cyberstalking* (assédio pela Internet) e a temida difusão da pornografia infantil. Cabem ainda nesta classificação as ações destrutivas de sistemas computacionais, a interceptação de quaisquer tipos de comunicações, modificações de dados, violações a direitos de autores, incitação ao ódio e quaisquer tipos descriminação, escárnio religioso, *cyberbullying*, terrorismo, entre outros.

Entende-se que a forma tradicional do *cybercrime* caracteriza-se por assumir muitas facetas, podendo inclusive ocorrer a qualquer momento e lugar. Os indivíduos que atuam na prática criminosa das ações especificamente voltadas ao crime cibernético usam inúmeros métodos, possuindo muitos diferentes, e utilizando cada um deles de acordo com cada objetivo desejado. Sendo assim, essas infrações ocorrem quando o sujeito se utiliza das ferramentas do mundo virtual para realização dos crimes intitulados como “crimes cometidos pela informática”.

Não são poucos os casos de vítimas – sejam elas pessoas ou empresas – vítimas dessa variante de crimes, que terminam lesadas com a má disposição de

alguns usuários da rede mundial de computadores. Criminosos têm a utilizado para o cometimento de crimes, com o intuito de adquirir, para si ou para outrem, benefícios dos mais diversos modos, em proveito de outros usuários da rede.

Um dos maiores infortúnios em relação a esses crimes praticados pela internet é ainda a imensa sensação de impunidade que paira, vez que a criminalidade avançou mais rapidamente do que as legislações nacionais e internacionais. Além dessa problematização, a escassez de técnicas necessárias para se identificar a autoria desses delitos também é um fator extremamente preocupante. Como efeito, os crimes virtuais vêm se tornando rotineiros em todo o mundo, e, infelizmente, a dificuldade do poder legislativo em tipificar essas modalidades de crimes vem justamente criando esse clima de “terra sem lei” na Internet, pois os criminosos sabem que sua identificação é difícil.

Se não bastasse a quantidade de crimes que ocorrem na internet diariamente e a falta de um efeito mais específico e sintomático para se evitar tais delitos, ainda surgem zonas dentro do ciberespaço gradativamente mais complicadas de serem vigiadas, como a *Deep Web* (Internet profunda), uma “área” ainda pouco explorada pelo grande público, o que facilita o cometimento de crimes, ante o fato de os endereços e acessos serem mais difíceis de rastrear, ao contrário do que ocorre na Internet convencional chamada de *Surface Web* (Internet de superfície), que requer habilidades para se chegar até o crime e o criminoso, mas que não permite o anonimato total.

Frente a toda essa questão, como fazer para criminalizar tais atos e suas modalidades mais recentes que já não são alcançáveis por nenhuma outra legislação anterior? O que podemos fazer para diminuir o cometimento de crimes no ambiente virtual?

O presente trabalho científico tem como foco principal trazer à tona no meio jurídico e acadêmico um intenso debate onde se envolva as questões jurídicas que são oriundas do resultado livre do uso da internet; resultado este que traz consigo campo fértil para crimes, contravenções e condutas ética e moralmente não aceitas pela sociedade.

Além deste ponto, abordaremos também outras inúmeras novas condutas que surgiram com o advento da revolução digital e a facilidade/acessibilidade ao

universo abstrato *cybernético,* incluindo nesse rol as novas tecnologias que surgiram com o avanço das ciências eletrônicas e seus impactos nesta mesma sociedade que se utiliza desse espaço - que revolucionou a comunicação entre as pessoas, aproximando quem estava longe, ampliou o acesso aos locais mais remotos a produtos e serviços, difundiu informação de todas as formas possíveis e imaginárias, mas que nas mãos de pessoas inidôneas ainda parece ser campo fértil e sem lei para a prática de crimes.

Metodologia

Este trabalho parte de uma intensa revisão bibliográfica, composta por alguns dos principais autores do tema no meio jurídico no Brasil e no mundo, aliados com autores da área de Ciência da Computação e Redes de Computadores, diretamente ligados à segurança de dados. O método de pesquisa utilizado foi o exploratório, com a finalidade de tornar familiar o tema para posterior desenvolvimento ainda mais aprofundado.

Como fonte de pesquisa primária, foram utilizados relatórios técnicos, dissertações e outros artigos sobre o tema; e secundários, livros e manuais técnicos, inclusive em outros idiomas, tendo em vista a ainda pouca oferta de material de relevância desenvolvido sobre este tema em nosso país.

Os resultados foram apresentados de forma qualitativa-quantitativa, e o recurso para a apresentação dos resultados se dá através de pesquisa documental, ou seja, através do estudo e análise de documentos, como normas técnicas, códigos e leis, regulamentos, tratados, convenções internacionais e jurisprudências, além, ainda, de livros, revistas e *websites*.

A pesquisa foi construída em estudos de autores como Julio Fabbrini Mirabette, Jorge R. Valzacchi, Damásio de Jesus, Fernando Capez, entre outros juristas e pensadores que também desenvolveram trabalhos pertinentes e de muita importância ao assunto. Apesar de estes servirem de alicerce para este Trabalho de Conclusão de Curso, é de extrema importância destacar que o apanhado de autores propende a crescer, na medida em que a compreensão e análise for sendo desenvolvida.

CAPÍTULO I

1. DOS CRIMES

1.1. CONCEITO DE CRIME

Antes de qualquer coisa, é de suma importância esclarecer antecipadamente o que é crime, visando uma melhor análise deste trabalho, sendo seu objetivo principal desmistificar o crime virtual, suas peculiaridades e a legislação vigente sobre o assunto.

Mister, ainda, destacar o conceito prático de crime. Desta forma considera-se crime toda ação ou omissão humana que lesa ou expõe ao perigo bem jurídico tutelado pelo Direito Penal. Alguns doutrinadores trazem um conceito bastante similar sobre o assunto.

De acordo com SANTOS (2001), “crime é o comportamento humano positivo ou negativo, provocando, este, um resultado e que segundo o seu conceito formal, é violação culpável da lei penal, constituindo, assim, delito”.

Para CAPEZ (2008), crime pode ser conceituado sob três aspectos diversos, quais sejam: a) material – sob esse enfoque crime é “todo fato humano que, propositada ou descuidadamente, lesa ou expõe a perigo bens jurídicos considerados fundamentais para a existência da coletividade e da paz social”; b) - formal – sob esse enfoque “o crime resulta da mera subsunção da conduta ao tipo legal e, portanto, considera-se infração penal tudo aquilo que o legislador descrever como tal, pouco importando o seu conteúdo”; e c) analítico – nesse enfoque que busca, sob um prisma jurídico, estabelecer os elementos estruturais do crime, o conceito é: “todo fato típico ilícito”.

De acordo com a doutrina majoritária, o conceito analítico de crime o define como um fato típico, antijurídico e culpável, e da noção de que a tipicidade, a conduta, o resultado e o nexo causal, formam o fato típico, excluído qualquer desses elementos não se há de falar em crime.

Já JESUS (2011) é bem sucinto sobre o conceito de crime, trazendo a seguinte explicação: “crime é um fato típico e antijurídico. ”

A lei de introdução ao código penal traz em seu artigo 1º o seguinte conceito:

> *“*Considera-se crime a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas. Alternativa ou cumulativamente. ” (Código Penal Brasileiro, 1940)

Feita esta análise dos conceitos trazidos por alguns doutrinadores, fica fácil o entendimento sobre o assunto, diante do exposto pode-se concluir que crime é resultante de uma ação ou omissão, que irá gerar um fato antijurídico, que colocará em risco o bem jurídico tutelado pelo direito penal.

1.2 CONCEITO DE CRIMES VIRTUAIS E/OU DIGITAIS

Vencido o conceito de crime, carecemos de entranhar no conceito de crime digital, que é o âmago, o centro deste trabalho.

Os crimes cybernéticos adquiriram muitas alcunhas. Por serem uma classe de delitos extremamente nova e de muita inconsistência jurídica, ainda existe bastante desinformação e desconhecimento sobre o assunto.

Muitos entendem o cybercrime de uma forma bem simples, como sendo crimes cometidos por meio da Internet, podendo estes serem enquadrados no Código Penal brasileiro e seus infratores sujeitados às penas previstas na lei.

Não é.

Os crimes virtuais atualmente transcendem os liames e as balizas do nosso Código Penal.

O crime virtual, numa rápida definição, é aquele praticado no meio virtual, podendo ser a internet tanto um ambiente propício para a consumação dos delitos quanto para a execução de seus atos preparatórios.

Com a premissa de abraçar, entender, e, por conseguinte encontrar meios de conter esta nova modalidade de crimes, nasce um novo braço jurídico, extremamente qualificado e necessário para poder alcançar de forma mais precisa esses crimes virtuais - já que nosso Código Penal brasileiro é de 1940, época em

não haviam tais tecnologias - o que torna claro a deficiência em combater tais crimes, devendo-se utilizar além dos princípios gerais do direito penal, a legislação especial para combater tais condutas.

Novas relações sociais passaram a surgir nesta era digital, razão pela qual o direito deve se adaptar a esta nova realidade, visando combater essas infrações penais cometidas no meio virtual.

Apesar disto, podemos afirmar que os crimes cybernéticos são novas modalidades de crimes, diferentes dos crimes tradicionais, justamente por serem cometidos contra sistemas de informática e/ou se utilizando de recurso da tecnologia como ferramenta para o cometimento da conduta criminosa.

CASSANTI (2014) afirma que crime cibernético é:

> "Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cybercrime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital". (CASSANTI, 2014, p.3)

Segundo Mendes e Vieira, crime cybernético é qualquer conduta culpável condenada pelo meio jurídico, ou seja, são condutas típicas, antijurídicas e culpáveis, praticadas utilizando sistemas de informática ou contra eles (MENDES E VIEIRA, 2012).

O crime digital está diretamente ligado ao cybercrime, mas deste mesmo modo, ainda não é algo tão simples de explicar, pois envolve um campo de ação bastante amplo, que vai desde um simples vírus até ações coordenadas, como o roubo dos dados de uma pessoa titular de uma conta bancária, por exemplo.

CASTRO (2001) afirma sobre o tema que:

> "Crime de informática é aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através de computador. Inclui-se nesse conceito os delitos praticados através da Internet, pois pressuposto para acessar a rede é a utilização de um computador". (CASTRO, 2001, p.9)

Entende-se que a forma tradicional do cybercrime caracteriza-se por assumir muitas facetas, podendo, inclusive, ocorrer a qualquer momento e em qualquer

lugar. Os indivíduos que atuam na prática criminosa das ações especificamente voltadas ao crime cybernético usam diferentes métodos e de acordo com cada objetivo desejado. Sendo assim, esse crime ocorre quando o sujeito se utiliza das ferramentas do mundo virtual para realização dos crimes intitulados como “crimes cometidos pela informática”.

Com os pés no chão, quanto ao conceito de crimes digitais, ainda, alguns doutrinadores, legisladores e docentes entendem que a prática de crimes digitais são quaisquer atos ilícitos, sejam omissivos ou comissivos, praticados através de qualquer meio virtual, com a nítida e clara finalidade de prejudicar um ou mais bens tutelados pela Lei. O termo “Crimes virtuais” é somente a expressão usada como referência para elencar toda e qualquer atividade ilícita realizada onde se encontram um meio de acesso (como um *smartphone, desktop, tablet, notebook*, por exemplo) e/ou uma rede de computadores, esta última sendo invadida sem anuência e utilizada como uma ferramenta, uma base de ataque ou como meio para o cometimento de um crime.

> “Podemos conceituar os crimes virtuais como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações os direitos de autor, incitação ao ódio e descriminação, chacota religiosa, transmissão de pornografia infantil, terrorismo, entre diversas outras formas existentes. (PINHEIRO, 2010, p. 46). ”

Já para uma outra leva de entendedores do assunto, os crimes virtuais são vistos e ponderados como “crimes de meio”, aqueles aplicados e manipulados em um ambiente específico, nesse caso, virtualmente; é um crime onde sua espécie só acontece num ambiente virtual, podendo sair deste meio, como em algumas modalidades específicas, ou seja, naquelas que ofereçam a possibilidade do crime poder ser enquadrado num crime de meio real, como alguns diversos tipos de fraudes, estelionato, falsidade ideológica, e outros crimes equiparados a estes, onde exigem um nível técnico maior para o cometimento destas infrações.

Até os dias atuais, sem a tipificação adequada e com a facilidade de acesso à rede mundial de computadores, os crimes tradicionais (previstos em nossa legislação) mas cometidos no ambiente virtual não são suficientes para alcançar os crimes cometidos contra o computador ou por meio dele, frente às novas

modalidades criminosas que surgiram e que merecem ser definidas em lei especial, para garantia da ordem legal.

Atualmente no ramo jurídico alguns doutrinadores se posicionam na busca da conceituação para essa nova modalidade de crimes como PINHEIRO (2009), “O crime virtual é, em princípio, um crime de meio, ou seja, utiliza-se de um meio virtual. ”

REMY GAMA FILHO (2000) define a criminalidade informática como: “Aqueles que tem por instrumento ou por objeto sistema de processamento eletrônico de dados, apresentando-se em múltiplas modalidades de execução e de lesão de bens jurídicos”.

Existem duas correntes doutrinárias que subdividem de maneiras distintas os cybercrimes. FURLANETO NETO, SANTOS E GIMENES (2012) citando PINHEIRO (2001) atestam e defendem essa primeira corrente, que separa tais cometimentos em crimes virtuais puros, mistos e comuns. Vamos conhecer cada um deles desta corrente doutrinária.

1.2.1 *Cybercrimes* Puros

Crimes cybernéticos puros podem ser definidos como toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas.

Damásio de Jesus entende crimes cybernéticos puros como:

> “Crimes eletrônicos puros (...) são aqueles que sejam praticados por computador e se realizem ou se consumam também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado. (DAMÁSIO, 2003).”.

O foco do sujeito ativo é atingir objetivamente o computador, o sistema de informática ou os dados e as informações neles inseridas. Tais dados encontram-se naquele dispositivo, e não em outro ambiente. É aqui que entram boa parte das condutas praticadas por *crackers*, pessoas com amplo conhecimento de informática e programação e que utilizam esse mesmo conhecimento para invadir ou prejudicar

servidores e sistemas, e muitas vezes sem nenhuma razão aparente. Note-se que o alvo são bens jurídicos protegidos pela norma penal, os dados, as informações contidas, cuja sua inviolabilidade é prevista no artigo 10 da lei 9296/96.

Ainda sobre a definição dos cybercrimes próprio:

> Crime virtual puro ou próprio é aquele em que o [...] computador, em seu aspecto físico, ou os dados e programas nele contidos são objetos de uma ação ou omissão antijurídica (PINHEIRO, 2001, apud FURLANETO NETO; SANTOS; GIMENES, 2012, p. 27).

Um clarividente exemplo de *cybercrimes* puros é o caso do vírus Melissa, que no final do século XX (mais precisamente em 1999) causou prejuízos, que, somados, alcançaram a cifra de aproximadamente US$ 80.000.000,00 (oitenta milhões de dólares americanos).

Outro exemplo foi o ocorrido com a *Sony*, em 2011, quando fora furtado os dados pessoais, nomes, endereços e possivelmente detalhes de cartões de crédito de 77 milhões de usuários da *Playstation Network*, plataforma virtual da *Sony* construída para a área de jogos virtuais de sua plataforma.

Três anos depois, a mesma *Sony* sofreu novamente outro ataque, causando prejuízos na casa dos bilhões, quando cinco filmes que não tinham sequer estreado nos cinemas estadunidenses foram furtados e vazados em sites piratas, que disponibilizaram para *download*.

1.2.2 *Cybercrimes* Mistos

Os *Cybercrimes* Mistos são aqueles delitos em que o criminoso utiliza a internet para efetuar o procedimento ilícito, e o objetivo principal não é tão somente o computador pessoal da vítima, mas bens jurídicos de naturezas abundantes. Nas palavras de Reginaldo César Pinheiro, “são aqueles em que o uso da internet ou sistema informático é condição *sine qua non* (em português: “sem ela não”) para a efetivação da conduta, embora o bem jurídico visado seja diverso ao informático” (PINHEIRO, Reginaldo César. Os cybercrimes na esfera jurídica brasileira, não paginado, online).

> O crime virtual misto, por sua vez, caracteriza-se [...] pelo emprego obrigatório de internet no *iter criminis*, embora o bem jurídico a ser lesado seja diverso [...], a exemplo de transferências ilícitas feitas por

> *crackers* que retiram quantias irrisórias de milhares de contas-correntes e transfere tudo para uma conta única, que embora não seja uma quantia insignificante para a vítima, para o criminoso virtual o valor arrecadado torna-se significativo. Outro exemplo é o caso homicídio praticado pela Internet no qual o *cracker* invade o sistema de uma torre de controle de aeroporto e muda a rota de um avião, causando um grave acidente. Tais delitos só se consumariam pelo de um computador conectado à Internet (PINHEIRO, 2001, apud FURLANETO NETO; SANTOS; GIMENES, 2012, p. 27).

O agente ativo da ação delituosa não objetiva o sistema de informática e seus componentes, mas torna a própria informática uma ferramenta, um mecanismo indispensável para o cometimento e execução da ação criminosa. Um bom exemplo são as transferências ilícitas de cifras em uma plataforma de *home banking*.

1.2.3 *Cybercrimes* Comuns

Os *Cybercrimes* Comuns são aqueles cuja Internet é apenas um acessório, um equipamento, um utensílio para o cometimento de um crime já definido e caracterizado e tipificado na lei penal. A Rede Mundial de Computadores torna-se mais um meio para a consumação de determinadas condutas criminosas.

Um bom exemplo é como se dá a pornografia infantil dentro do ambiente virtual: se antes ela apenas era operacionalizada, equiparada por vídeos em fitas VHS, CD'S, DVD'S, fotografias reveladas, pôsteres, atualmente se dá através de sites e de plataformas ilegais exclusivas para esse meio. Transladou-se a maneira, mas a natureza da conduta ilícita continua a mesma.

Além destas subdivisões quanto a classificação dos *cybercrimes*, há outra corrente doutrinária que reconhece uma outra forma, subdividindo os crimes ambientados no virtual como apenas próprios e impróprios, senão vejamos:

1.2.4 *Cybercrimes* Próprios

Os Cybercrimes Próprios são os delitos cujo sistema de *hardwar*e e *softwar*e (sistema operacional) do sujeito passivo é o causador, a ferramenta e também a finalidade do crime. "São aqueles em que o bem jurídico protegido pela norma penal

é a inviolabilidade das informações automatizadas (dados). ” (VIANA, MARCO TÚLIO apud CARNEIRO, ADENEELE GARCIA. 2003).

São os procedimentos executados por *crackers*, com a finalidade de não apenas penetrar o sistema, mas também de modificar, alterar, incluir dados falsos, ou seja, atingir diretamente o software ou hardware do computador. Tais crimes só podem ser materializados e consumados pelo próprio computador e/ou contra ele mesmo e seus periféricos.

1.2.5 Cybercrimes Impróprios (ou impuros)

Os cybercrimes intitulados de impróprios são aqueles que tem por objetivo e alcançam determinado bem jurídico comum, como por exemplo, o patrimônio material do sujeito passivo, e se utilizam dos sistemas eletrônicos e digitais informáticos apenas como um novo meio de efetivação e aplicação do delito.

Assim expõe Damásio de Jesus:

> [...] Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não computacionais ou diversos da informática. (DAMÁSIO, 2003).

Existe uma certa complicação em se identificar e distinguir um crime cibernético impróprio cometidos contra patrimônio, por não haver reconhecimento em tratar informações armazenadas como um bem material, visto que a grande maioria dos tribunais nacionais tratam os dados computacionais como bem imaterial, impassível de apreensão como objeto.

Entretanto, conforme explica RITA DE CÁSSIA LOPES DA SILVA:

> “A informação neste caso, por se tratar de patrimônio, refere-se a bem material, apenas grafado por meio de bits, suscetível, portanto, de subtração. Assim, ações como alteração de dados referentes ao patrimônio, como a supressão de quantia de uma conta bancária, pertencem à esfera dos crimes contra o patrimônio. ” (SILVA, 2003, p. 97).

Portanto, podemos atestar que os cybercrimes impróprios ou impuros carregam em si mesmos um efeito naturalístico, que, por sua vez, afronta o espaço físico, o espaço “real”, atingindo algum ou alguns bens jurídicos, diversos do sistema informático.

Como exemplos de *cybercrimes* impróprios ou impuros podemos citar os três crimes contra a honra, podendo ser todos eles praticados no ambiente virtual, através de redes sociais, como WhatsApp, Facebook, Instagram, Twitter, como também através de salas de chats, e-mails, etc. Por exemplo, uma pessoa que divulga foto íntima de outra, sem autorização em uma rede social, causando assim uma ofensa à honra, é um sujeito ativo de crime cybernético de natureza impróprio.

1.3 SUJEITOS DO CRIME

1.3.1 Sujeito Ativo: Quem são os Cybercriminosos?

O sujeito ativo dos crimes cybernéticos é aquele que comete a infração, o crime, cujo perfil geralmente está correlacionado aos crimes comuns, possuindo alguns níveis de risco iminente. O indivíduo que comete crimes virtuais mostra como perfil ser aparentemente uma pessoa comum, sem muitos conhecimentos técnicos da área de informática (ou até mesmo sem nenhum tipo de discernimento sobre a área de programação e linguagem web); pode ser apenas um curioso digital, tão somente atraído pelo fascínio e a beleza do crime. Mas existem também aqueles criminosos com bastante conhecimento técnico, um *expert* no assunto, com *expertise* extremamente aprofundada na área computacional.

Já alguns crimes cometidos por meio de computadores pedem uma condição mais aprofundada, mais típica do agente, que é o conhecimento técnico aprofundado. Tais crimes podem atingir inúmeros bens jurídicos e de extrema importância.

Entretanto, pelo fato de haver um distanciamento do local afetado pelo crime e o criminoso, onde este muitas vezes está a quilômetros de distância (algo inerente ao ambiente virtual), a responsabilização objetiva da autoria do delito é difícil de ser comprovada, justamente pelo fato de existir a ausência física do autor do fato delitivo. E por ser a *internet* facilmente acessada por qualquer meio e em qualquer

lugar, de forma remota por vezes, isso facilita para que qualquer pessoa possa se conectar à rede, fato que facilita em demasia a utilização de alônimos, a fim de esconder seus legítimos e verdadeiros objetivos.

O Direito Penal encontra muitas dificuldades em adaptar-se diante dessa realidade, como podemos observar:

> O Direito em si não consegue acompanhar o frenético avanço proporcionado pelas novas tecnologias, em especial a Internet, e é justamente neste ambiente livre e totalmente sem fronteiras que se desenvolveu uma nova modalidade de crimes, uma criminalidade virtual, desenvolvida por agentes que se aproveitam da possibilidade de anonimato e da ausência de regras na rede mundial de computadores. (PINHEIRO, 2009 apud DULLIUS, 2012, [n.p.]).

Podemos descrever a aparência do sujeito ativo como a de qualquer outro sujeito que comete um crime qualquer. Independente do cometimento ter sido efetivado no ambiente real ou virtual, o sujeito que comete uma conduta ilícita e culpável pode e deve ser responsabilizado pelo delito (desde que este possua aptidão para isto).

Porém, parece que, ao ingressarmos no ambiente virtual, essa liberdade de uso da rede, muitas vezes dada de forma irrestrita, oferece uma falsa ideia: a de que podemos admitir certas características incondizentes com o que somos na realidade, no ambiente real. E, justamente por este motivo, algumas pessoas optam em assumir uma outra imagem, ficando livres, portanto, para dizer ou não a verdade enquanto se utilizam deste ambiente factível e virtual.

E é justamente por esta complexidade – a falta de identificação na internet, ou seja, a de se poder identificar os usuários e correlacioná-los a quem de fato são no meio físico, sobrevieram algumas determinadas designações, a fim de possibilitar o reconhecimento destes sujeitos. Foi aí que surgiram algumas denominações. As principais nomenclaturas são: *hacker's* (ou *White-Hats*), *cracker's* (ou *Black-Hats*), *coder's, carder's, phreaker's, warez, defacer's, Virii's, lamer's*. Entenda onde cada um atua:

a) Hacker's (ou White-Hats): Os *hacker*s (também conhecidos como *White-hats*) são indivíduos que apresentam conhecimentos técnicos bastante aprofundados e nem sempre utilizam tais conhecimentos para a prática de condutas ilegais. O *hacke*r não tem por finalidade primária cometer crimes, mas utilizam de seu conhecimento para se auto desafiarem. A grande maioria desses indivíduos somente querem invadir um sistema e expor, revelar o quão vulnerável se encontra tal sistema.

Os *hackers* conseguem acessar sistemas e computadores de maneira muito fácil ao encontrarem a vulnerabilidade na segurança da máquina, assim como os *crackers*. Porém, os *hackers* não empreendem práticas negativas. Eles não alteram, não modificam em absolutamente nada, ou seja, não possuem como finalidade praticar uma determinada conduta criminosa.

O *hacker*, no popular, não passa de um *nerd* da internet que tem como objetivo fazer o bem, ajudar no combate a pedófilos, venda de drogas pela internet, explicitar erros de sistemas bancários e atuam contra os *crackers*; este sim, possuem por finalidade principal utilizar a internet para o cometimento de crimes.

Numa analogia mais clara de ser entendida, o *hacker* é aquele cara que observa de longe você saindo de casa em seu veículo, e após a sua partida, atravessa a rua em direção a sua casa e roda a maçaneta da porta a fim de verificar se você trancou sua residência. Se ele perceber que você não trancou, te liga e te comunica.

Porém, apesar dos *hackers* não procurarem de forma consistente prejudicar e causar danos a terceiros, não significa que estes estejam imunes a cometer crimes. A prática de invadir um sistema qualquer sem autorização, ainda que não altere ou danifique nada, pode ser qualificado como crime. Voltando a analogia acima, se ele percebe a maçaneta sem tranca e entra em sua residência, mesmo que não deixe rastros ou subtraia nenhum bem seu, ele já cometeu um crime.

b) Cracker's (ou Black-Hats): Os *crackers* ou *Black-hats* (em inglês: hacker do mal ou chapéu negro ou aqueles que quebram sistemas) possuem um vasto conhecimento em programação (assim como os *hackers*), porém estes indivíduos

fazem uso deste conhecimento ímpar para encontrarem lacunas, fendimentos em sistemas e causarem danos à terceiros, obtendo informações sigilosas.

O termo *cracker* surgiu no ano de 1985, criado por profissionais da área de Tecnologia da Informação que não concordavam com o termo utilizado pela imprensa da época, que comumente os associavam numa mesma terminação os *hackers* e os *crackers*, justamente pelo fato de que ambas as espécies possuem amplo conhecimento técnico, sem se importarem com a finalidade que suas práticas resultam, que são completamente distintas.

A finalidade do *cracker* não é simplesmente encontrar a vulnerabilidade e tentar sanar ou avisar o responsável (como os *hackers*), e sim roubar senhas de acessos, documentos importantes de diversos formatos, realizar espionagem, dentre outras.

Utilizando a mesma analogia do tópico anterior, o *cracker*, ao contrário do *hacker*, vai perceber a tranca da sua casa aberta, vai adentrar em sua residência e subtrair bens, pichar paredes, quebrar aquilo que não conseguir furtar.

Habitualmente, o cracker possui seus alvos bem definidos e pode passar dias e dias tentando conseguir acesso ao sistema que deseja atacar, podendo passar semanas e até meses para alcançar seu objetivo, caso este sistema seja melhor protegido.

1.3.1.1 A confusão entre os dois termos e o surgimento do "*hacker* ético"

Apesar de ter surgido em meados de 1984, a confusão entre *hackers* e *crackers* ganhou na década seguinte um fardo depreciativo muito forte. Ainda hoje é frequente a baralhada confusão entre os dois termos, sendo ainda muito corriqueiro empregar a expressão *hacker* para associar o *cracker*, e vice-versa.

A expressão "*hacker*" tinha como significado principal para a mídia rotular qualquer indivíduo com exímia habilidade ou apreço na área de computação, sem considerar a finalidade do sujeito ativo. Esta mesma mídia nunca considerou a divergência de sentidos entre ambas as palavras, por não conseguirem entender a diferenciação que ambas carregam entre si.

Desde que surgiu de forma mais concisa nos meios de comunicação atuais (sobretudo ganhando força na virada do século 20 para o século 21, mais precisamente em 1999, com o famoso "*bug* do milênio"), o termo *hacker* amplamente ficou reconhecido perante a sociedade com um significado errôneo, tendo como conceito público "os piratas eletrônicos ligados a crimes que se cometem utilizando computadores". O vocábulo já possuía desde a década de 80 uma carga descreditada em seu real sentido, o que fez, naquele momento, o surgimento deste termo.

Apesar de ter suas raízes nos anos 50 e 60 de forma muito embrionária (com alguns princípios surgindo no Instituto de Tecnologia de Massachusetts, nos EUA), foi em 1984, através do jornalista norte-americano Steven Levy que surgiu o termo "Ética *Hacker*" pela primeira vez, onde ele expôs que o ponto principal da ética *hacker* é o livre acesso à informação e que suas condutas no meio virtual possam sempre realizar melhorias para a sociedade e trazer mais qualidade de vida para as pessoas.

A Ética *Hacker* foi exposta como um "novo estilo de vida" entre os *White-Hats*, e quem não a seguia, passava a compor o grupo de *Crackers*. Tais conceitos fizeram surgir o movimento do *software livre*, cuja programação é de código aberto, permitindo que outros *hackers* acessem o código-fonte de determinados *softwares*, dando a possibilidade de que este "*soft"* seja melhorado e reutilizado para outros propósitos brancos.

Na década de 80 o uso de computadores era ainda muito restrito, geralmente a ambientes acadêmicos, empresas governamentais, bibliotecas públicas e uma parcela menos abastada da sociedade, tendo em vista o alto preço de um computador. Entretanto, esse panorama se modificou na década posterior, trazendo uma nova leva de piratas do mundo virtual que sequer tinham conhecimento da figura do *Hacker* Ético, que horas cometiam crimes, horas ajudavam as pessoas.

Foi aí que no início dos anos 2000 programadores de grandes empresas de serviços de segurança divulgaram aqueles valores morais e filosóficos de outrora, nascidos dentro da comunidade *hacker*, tornando pública a "Ética *Hacker*" e dando embasamento para a figura do "*hacker* ético", justamente a fim de minimizar o impacto que o termo *hacker* ainda causava no mercado de segurança cybernética, fazendo ela toda a diferença no meio da segurança virtual.

c) Coder's: Os *Coders* (ou codificadores) são pessoas que possuem notáveis conhecimentos em programação, geralmente em mais de duas ou três linguagens de programação distintas. São eles que constroem as ferramentas de invasão e segurança, geralmente sob medida praquela determinada invasão. Um codificador é um tipo de programador curioso, uma pessoa disposta a passar incalculáveis horas tentando construir algo de pouco ou nenhum valor prático, apenas pelo único intuito de querer descobrir ou desenvolver uma nova ferramenta, podendo esta ser utilizada para invadir sistemas ou não.

Os *Coders* conseguem "escrever" *exploits* e programas de forma a identificar a vulnerabilidade de programas-fontes que possam ser explorados. O sentido de sua atuação não é fazer a invasão, mas desenvolver toda a técnica para uma possível invasão.

Um *hacker* ou um *cracker* pode ser um *Coder* de forma simultânea.

d) Carder's: Os *Carder's* tanto podem ser uma derivação, como podem ser uma modalidade dos *crackers*. Seu principal objetivo encontra-se em conseguir dados e informações de cartões de crédito e/ou débito, assim como informações de contas-correntes e/ou poupança, além de vulnerabilidades em sites bancários, o chamado "*carding*".

Os *carders* tem por finalidade realizarem fraudes online. Geralmente se utilizam dessas informações para benefício próprio, ou de parentes e amigos, seja utilizando-as para comprar produtos e fazer transações financeiras sem o consentimento do titular da conta/crédito, seja vendendo a preços altíssimos (através de repasse, para que outros cometam atos ilícitos) os dados obtidos.

Os *carders* são facilmente encontrados em salas de *chat* com diretórios ocultos, ou se utilizam do IRC (*Internet Relay Chat*), uma plataforma muito usada e difundida nos anos 90.

Ao conseguirem utilizar os dados bancários e de crédito furtados e realizarem alguma compra online, os criminosos utilizam laranjas, também conhecidos como

DROP ou Drops, para receberem os produtos. Muitas vezes os DROPS não têm ciência de que o produto recebido é oriundo de conduta ilícita.

e) Phreaker's: Os *phreakers* (origem etimológica: *Phone* + *freak* ou *Phreak*) é a nomenclatura utilizada para designar os *crackers* da telefonia. Estes criminosos do mundo virtual são especializados em lesar sistemas de telecomunicações, sejam elas fixas ou móveis.

No passado, os *phreakers* empregavam gravadores de fita e outros dispositivos para produzir sinais de controle e enganar o sistema de telefonia. Conforme as companhias telefônicas foram reforçando a segurança, as técnicas tornaram-se mais complexas. Hoje, o *phreaking* – nome dado à prática dos *phreakers* - é uma atividade extremamente elaborada, que poucos hackers dominam (ULBRICH, VALE, 2010).

Alguns exemplos de crimes praticados pelos *phreakers* estão a clonagem de celulares (muito comum no final da década de 90), alteração do sistema de cobranças dos telefones, fazer escutas telefônicas sem autorização, dentre outras.

f) Warez: A palavra *warez* é diretamente derivada da língua inglesa, sendo esta, portanto, a segunda metade da palavra *software* no plural (soft-ware, então *warez*), e é o termo utilizado para se referir aos piratas de software, ou seja, àqueles que praticam pirataria.

A ênfase inicial foi dada para designar o comércio ilegal de softwares protegidos por direitos autorais. Com o passar do tempo, o termo também alcançou os indivíduos que por vezes e de forma ingênua disponibilizam - através de grupos organizados na web – materiais com propriedade intelectual registrada, não sendo mais necessária caracterizar o comércio, auferir lucros.

Outros abarcados pelo termo foram aqueles que colecionam programas ou materiais piratas.

Como exemplo de algumas ferramentas utilizadas pelos *wares* estão os:

- *Patchs* (um tipo de programa que possui dentro de si mesmo uma cópia já alterada daquele software e tem por finalidade substituir trechos do software original pelo modificado);
- *KeyGens* (um programa que funciona como gerador de números seriais, foi especialmente desenvolvido com a finalidade de criar estes números dentro do algoritmo que lhe rege a fim de destravar programas que usam este tipo de validação);
- *KeyMaker* (software que consiste na fusão de *KeyGen, Crack* e do cavalo de Tróia);
- *Seriais* (conjunto de letras e/ou números construídos através de uma fórmula lógica computacional com a finalidade de destravar determinado software - este tipo de warez é híbrido, se divide entre legalidade e pirataria, uma vez que é utilizado por cybercriminosos e produtores de material autoral), e os
- *Cracks* (Uma versão modificada do programa original, que roda uma cópia como se fosse completa. Ou um arquivo que executa tal processo, conhecido como *patching* (ou *"patchear"*, em português).

Lembro ainda que tais tipos de *warez* podem vir a serem utilizados e disponibilizados em quaisquer tipos de mídia física, tais como *CD's, DVD's, BluRay*, *pendrives*, assim como implementados/utilizados em todos os tipos de arquivos e formatos, como jogos (de todas as plataformas), *softwares* (para quaisquer sistemas operacionais), filmes, séries e musicais, mp3, etc.

g) Defacers: Os *defacers* (ou pichadores), são uma classe de cybercriminosos que praticam uma técnica que consiste em realizar severas modificações de conteúdo e estética de uma página web, conhecido como *defacement* (palavra de origem inglesa utilizada na segurança da informação para categorizar ataques realizados por *defacers*).

Numa comparação entre mundo real x mundo virtual, estes são comumente comparados com pichadores**.**

Não é regra, mas os *defacer's* - em sua grande maioria - possuem conhecimento técnico bem aquém do que o mundo dos cybercrimes espera. Por

isso, essa classe de cybercriminosos necessitam de muitas horas para conseguir achar algum tipo de vulnerabilidade em servidores e sistemas, e explorá-la.

Os *defacers* geralmente são indivíduos engajados em alguma atividade de cunho ativista ou político, e sempre ataca servidores com o intuito de degradar, denegrir ou desmoralizar (por meio da internet) informações ou determinadas empresas ou instituições, sejam elas privadas ou públicas. A motivação desses ataques também pode ser algo pessoal; em outras, só o desejo de autoafirmação, ou a busca pela sensação de prazer ao mostrar para si mesmo a capacidade de invadir o alheio de forma virtual.

h) Virii's: *Virii* define uma categoria de indivíduos cuja prática é colecionar todo tipo de vírus que conseguir para sistemas computacionais. Fazem parte de sua coleção vírus dos tipos *worms*, *trojans*, *Keyloggers*, *ransomwares*, etc. Nem sempre o Virii acaba utilizando sua coleção, mas os mantém sempre prontos para uso.

i) Lamer's / Script Kiddie: *Lammer* ", *Lamer* ou *Script Kiddie*" são três termos utilizados para rotular aqueles que não possuem nenhum ou pouco conhecimento sobre técnicas de invasão, programação e demais ferramentas necessárias para invadir sistemas ou servidores, pois estes não estão interessados em tecnologia, mas sim em garantir fama e outros tipos de lucros pessoais. Geralmente, ele tem acesso à códigos maliciosos disponíveis no *Git Hub*, uma plataforma de compartilhamento de códigos online. Ele assiste a vídeos no YouTube, navega em sites que ensinam algumas coisas bem superficiais e aprende algumas técnicas.

Por não possuírem conhecimento aprofundado, apenas motivados pela vontade de trabalhar no ramo ou pelo prestígio que uma invasão no meio virtual carrega e lhes dá, os *lamer*s utilizam ferramentas desenvolvidas por terceiros para realizarem os ataques; muitos deles precisam aprender a manusear tais ferramentas, pois seu conhecimento limitado não lhe permite invadir tão rapidamente.

O termo *Lammer* foi mais usado no final da década de 80, para rotular de forma depreciativa àqueles que executavam ações na área da segurança da

informação, mas não possuíam conhecimento hábil e suficiente para desenvolverem suas próprias ferramentas e executarem trabalhos profissionais.

Nem sempre um *Lammer* era um *cracker*. Ele podia trabalhar seriamente para empresas de segurança de dados. Porém, com a virada da década e com a chegada dos anos 90, foi atribuído o termo *"Script Kiddie",* deixando o termo *Lammer* apenas para o mundo dos jogos digitais.

Com a mudança de termo e com o avanço tecnológico, os *Script Kiddie* ganharam outras atribuições, passando a responderem à *crackers* inexperientes, na maioria das vezes adolescentes ou jovens adultos, precisando de autoafirmação no meio *cracker*, necessitando demonstrar de todas as maneiras uma suposta capacidade no meio virtual. A maioria deles possuem somente a intenção de competir por reputação e reconhecimento dos outros iguais a ele. A maioria destes jovens e adolescentes se iniciam neste meio praticando pequenos ataques a colegas de trabalho ou de escola/universidade, a fim de testarem novas ferramentas e aprenderem a manusear tais artefatos.

Uma grande parcela destes jovens que se auto denominam *Script Kiddie* são arrogantes, pouco conhecedores da lei e do mundo virtual e quase sempre querem cometer ato ilícitos. Por causa disto, os *Script Kiddie* são extremamente inconvenientes para o convívio social (real e virtual) e são ignorados por *hackers* e até outros *crackers*.

Apesar de serem extremamente repudiados no meio virtual, ser um *Script Kiddie* é parte do aprendizado de um futuro *hacker* ou *cracker*. Todo (ou quase todo) *hacker* e/ou *cracker* já fora em algum lugar do tempo um *Script Kiddie*.

1.3.2 Sujeito passivo

O sujeito passivo é uma figura mais fácil de descrever e de se identificar do que o sujeito ativo, pois ele pode ser qualquer cidadão que possua um bem jurídico lesado ou ameaçado de lesão por ações através do ambiente virtual ou que lese bens virtuais.

O sujeito passivo do cometimento de crimes cybernéticos pode ser uma pessoa física, pessoa jurídica ou até mesmo uma entidade titular (seja pública ou privada, desde que titular do bem jurídico tutelado), visto que seus bens patrimoniais

podem ser atingidos, ou seja, deteriorados, desviados, perdidos, deixados inelegíveis ou cujas informações foram violadas.

1.3.3 Pessoa física x pessoa jurídica como sujeitos passivos do crime e a importância da divulgação do delito

Quando falamos de um crime comum, conseguimos identificar rapidamente quem é o sujeito ativo e o sujeito passivo da conduta, ou seja, quem realizou e em quem recaiu a ação ou omissão. Como vimos anteriormente, não muito diferente do crime comum, os crimes virtuais também se utilizam dessa maneira de identificação entre os agentes, sendo o sujeito ativo aquele que comete o delito e o passivo aquele que está sendo lesado, o que sofre a ação.

Acontece que nos dias de hoje, uma grande parcela de crimes cometidos no ambiente virtual não tornam-se públicos. Os motivos para que tais cometimentos delituosos não cheguem ao conhecimento da população variam. No caso de pessoas jurídicas, os principais motivos vagueiam desde a falta de denúncia (quando, por exemplo, empresas multinacionais não afirmam ou divulgam possíveis ataques virtuais ocorridos em seus servidores), ou até mesmo para que essas invasões não demonstrem uma certa fragilidade quanto à segurança de seus servidores e sistemas para a sociedade.

Quando falamos de pessoas físicas, os motivos mais recorrentes são a falta da devida punibilidade aos infratores (ou a sensação dela) e a escassez de mecanismos efetivos de denúncia, muitos deles motivados até por uma certa desinformação quanto à onde se dirigir, a quem recorrer, com quem falar.

O ato de não denunciar e se manter inerte acaba facilitando a propagação de tais crimes e corrobora com a disseminação da ideia de que a internet e o ambiente virtual são terras sem lei.

Contudo, é de extrema importância a divulgação de tais crimes, não só para alertar outros, como também, através de um processo de colaboração, mobilizar o meio virtual e seus usuários a fim de tentarem alertar outros usuários e/ou identificar o sujeito ativo de tais ataques.

A empresa americana Sony Pictures sofreu um duro ataque[1] cybernético em meados de 2014, que atingiu em cheio os servidores da produtora norte-americana.

[1] FONTE: https://www.lanacion.com.ar/tecnologia/el-detras-de-camaras-del-ciberataque-a-sony-nid1756821

Tal ataque forçou seu especialista em segurança cibernética Kevin Mandia soltar uma nota à imprensa – à época – que dava detalhes sobre a maneira como os cybercriminosos atacaram os *datacenters* da empresa, e o tipo de ferramenta utilizada: “O malware era indetectável por programas antivírus comuns na indústria, e destruidor o suficiente para fazer com que o FBI emitisse um alerta para outras organizações sobre a ameaça.”.[2] Desta afirmação é possível dimensionar o que ataques cibernéticos podem gerar, desde crimes comuns contra a honra ou até se infiltrarem em Estados e grandes Corporações.

1.3.4 Da autoria: os agentes criminais ativos e sua difícil identificação

Uma das grandes dificuldades no âmbito de crimes praticados no meio virtual é exatamente identificar o autor da prática delituosa, ou seja, definir a autoria do crime.

Por si só o mundo virtual facilita o anonimato dos usuários. Além disso, não é incomum o agente ativo se passar por outra pessoa, se utilizando de informações furtadas, o que dificulta ainda mais a descoberta do agente causador do crime.

Imperiosa uma profunda investigação a fim de apurar a autoria do fato, e a correlação a posterior da conduta ilícita e sua classificação e qualificação, para que o judiciário possa tomar as medidas cabíveis com o real sujeito ativo e não com inocentes, visto que estes podem ser apontados como causador do delito sendo que muitas vezes este também fora vítima de ações criminosas.

A pretensão punitiva deve incidir sobre quem realmente motivou o crime, e não a possíveis vítimas, como se posiciona TOURINHO FILHO citando CARNELUTTI:

> "O problema da qualificação do acusado é de suma importância, porquanto, em se tratando de qualidade personalíssima, não poderá ser atribuída a outra pessoa que não a verdadeira culpada. Ensina, com autoridade, Carnelutti: ´no puede haber, sin um imputado, um juicio penal, ouesto que este se hace, no com fines teóricos, para resolver uma Duda, sino com fines práticticos, para infligir uma pena´ (leccciones, cit., v. 1, p. 195).

[2] FONTE: https://www1.folha.uol.com.br/tec/2014/12/1562817-entenda-o-caso-da-invasao-hacker-a-sony-pictures.shtml

A identificação do sujeito ativo é um dos principais empecilhos, uma das maiores dificuldades que as autoridades especializadas em tecnologia encontram: o de detectar o delito em tempo hábil, o de descobrir quem é o sujeito ativo, quem deu causa à ação delituosa, chegar até ele e puni-lo.

O reconhecimento desses agentes é dado pelo endereço de IP (*Internet Protocol*), uma identificação única para cada computador conectado à rede. Em uma rápida analogia ao meio físico, podemos descrevê-lo como um documento de identificação único, como o CPF, por exemplo, onde cada um possui o seu. Porém, apesar dele ser uma identidade virtual, ele não é único, muito menos intransferível. Ao contrário do CPF (que nunca muda ou quase nunca muda sua numeração), por questões comerciais e técnicas, o endereço IP pode ser alterado por muitos motivos. É possível camuflá-lo e até alterá-lo com facilidade, se o sujeito ativo possuir vasto conhecimento técnico com redes.

Além disto, essa identificação é dificultada pelo fato de que muitos provedores não armazenam tais informações por muito tempo. Se não bastasse, aqueles que armazenam, dependem de autorização judicial para poder divulgá-las. Algo extremamente dispendioso, moroso e burocrático.

1.4 A CIBERNÉTICA, O AMBIENTE VIRTUAL E O SURGIMENTO DA INTERNET

A cibernética é abordada no meio acadêmico como “a ciência do controle e da comunicação do modo como se relaciona com os mecanismos, indivíduos e sociedades” (GRENZ, Stanley J. e SMITH, Jay 2005). Ela deriva do termo grego *kybernetes*, que significa “timoneiro”. Ela estuda e controla o cyberespaço.

A cibernética inclui os vários tipos de processos que dependem da troca e do fluxo de informações que acontecem no ciberespaço. Um recurso cibernético é um mecanismo ou sistema que processa informações no ciberespaço, tais como um computador ou o sistema de telecomunicações. O estudo da cibernética levanta um sem-número de questões éticas das quais a primeira é o desenvolvimento da inteligência artificial e suas implicações para o que ela considera um ser vivo. (GRENZ, Stanley J. e SMITH, Jay, 2005).

Podemos descrever o que chamamos de “ambiente virtual” como o ciberespaço, uma ferramenta cibernética que liga de maneira totalmente virtual pessoas ao redor do mundo, estando elas perto ou longe uma das outras. A web, rede mundial de computadores, conhecida por todos, é um gigante modelo de ciberespaço, pois consegue interligar não só pessoas, mas informações, dados diversos, tudo isso de maneira totalmente virtual, através da internet, que nada mais é que um conjunto de redes de computadores interligados.

Durante a segunda guerra mundial, o governo dos Estados Unidos iniciou um projeto ambicioso, com o intuito de diminuir as distancias entre quarteis e o alto escalão das forças armadas. Foi aí que começaram a desenvolver um sistema que permitisse que seus computadores conseguissem trocar informações entre si, não necessariamente estes computadores estarem num mesmo ambiente físico.

A ideia era fazer com que uma base militar conseguisse se comunicar com outra e que, mesmo sob forte ataque, salvaguardar os dados. Seria uma tecnologia de resistência. Foi assim que surgiu então a ARPANET, um projeto extremamente ambicioso, iniciado pelo Departamento de Defesa dos Estados Unidos, de forma secreta, e que conseguiu realizar a interconexão de computadores, através de um sistema conhecido como comutação de pacotes, que consistia em dividir as informações em pequenos pacotes, onde cada pequeno pacote levava consigo uma pequena quantidade de informações, de dados sigilosos, de forma embaralhada. Aí adentrava outra tecnologia: a criptografia. Em um dos pacotes, continha o endereço, o local de entrega deste pacote ao destinatário; no outro, a chave criptográfica, ou seja, informações que permitiam a remontagem da mensagem inicial.

Com o passar dos anos, inúmeras pequeninas redes começaram a utilizar a mesma arquitetura, a mesma síntese da ARPANET e a construírem seus próprios meios de comunicação. Universidades, bibliotecas públicas, outros órgãos do governo, todos começaram a se mobilizar em torno desta tecnologia.

Posteriormente, com o surgimento do Protocolo de Comunicação (*The Internet Protocol* - IP), estas pequenas redes de mesma arquitetura da ARPANET que antes funcionavam em separado, foram interligadas. A ARPANET foi desmantelada em 1990, sendo substituída, portanto, por uma nova arquitetura de comunicação em rede, a NSFNET, popularmente conhecida como o que hoje

chamamos de INTERNET, permitindo que qualquer quantidade de computadores se comunicassem entre si e seus pares.

A internet é considerada filha da ARPANET, um projeto militar dos Estados Unidos e de uso exclusivo das forças armadas norte-americanas, totalmente restrito, mas que serviu como modelo para outras pequenas redes, que, juntas, formaram o que chamamos hoje de internet. Ela era restrita a alguns poucos privilegiados, mas hoje é de todos nós, representando um marco na história da sociedade atual, não somente pela quantidade de benesses que proporciona a todas as nações (sobretudo na questão da informação), mas também por estar modernizando e trazendo consigo uma outra visão no tocante às modalidades de crimes, justamente por ter se tornado um instrumento e um local para o cometimento de delitos.

Segundo JOSÉ MANUEL MORAN (1995):

> “Uma das características mais interessantes da Internet é a possibilidade de descobrir lugares inesperados, de encontrar materiais valiosos, endereços curiosos, programas úteis, pessoas divertidas, informações relevantes. São tantas as conexões possíveis, que a viagem vale por si mesma. Viajar na rede precisa de intuição acurada, de estarmos atentos para fazer tentativas no escuro, para acertar e errar. A pesquisa nos leva a garimpar joias entre um monte de banalidades, a descobrir pedras preciosas escondidas no meio de inúmeros sites publicitários. (MORAN, 1995, p. 14). ”

A internet modificou de forma muito positiva a comunicação mundo afora, se fazendo presente, portanto, de uma maneira muito rotineira, influindo em nossa vida em muitos aspectos, sobretudo no acesso à informação, lazer, comércio, educação, enfim, nas mais diversas esferas da sociedade. A verdade é que, hoje, não mais conseguimos viver sem esse advento. Se ela parar, muitas outras coisas também param. Esse novo instrumento de comunicação entre pessoas e máquinas promoveu, impulsionou formas imediatas de convivência, favorecendo, assim, a vida em sociedade, que não é imutável e passa por incessantes mudanças, onde as novas gerações abarcam, recebem um legado, mas também a incumbência de mudar, evoluir e moldar à sua realidade o que receberam.

A relação mútua entre as pessoas por intermédio da internet oportuniza o acesso às mais diversas inteirações, como afirma JOSHUA EDDINGS:

> “É uma sociedade cooperativa que forma uma comunidade virtual, estendendo-se de um extremo a outro do globo. Como tal, a internet é um portal para o espaço cibernético, que abrange um universo virtual de ideias e informações em que nós entramos sempre que lemos um livro ou usarmos um computador, por exemplo. (EDDINGS, 1994, p.38). ”

Mas, como tudo na vida tem seu lado bom e ruim, a internet infelizmente também possui como realidade um lado negro, sombrio, que acarretaram muitos problemas. A propagação de ações e condutas criminosas é uma realidade do advento do ciberespaço, e elas contribuem tanto para o surgimento, o aparecimento de novas modalidades de crimes, quanto para a execução de crimes já habituais no meio real. Mas isso não é tudo.

1.5 O CIBERESPAÇO E SEUS DESDOBRAMENTOS: A METÁFORA DO ICEBERG

Todo mundo já ouviu falar sobre a metáfora do *iceberg*: uma pequena parte do gelo que lhe compõe pode ser visto de forma muito clara por todos, enquanto mais da metade de seu corpo encontra-se escondido, submerso embaixo d’água. Com o ciberespaço, é praticamente a mesma coisa.

A parte do espaço cibernético visível, que é a que conhecemos, já é um campo vasto, mas muito limitado e vigiado (apesar da forma precária em como essa vigilância ocorre), mesmo sendo quase nada diante da imensidão do espaço cibernético.

A *web* que navegamos diariamente abarca somente 5% do total do ciberespaço. Apesar de parecer pouco, não significa que seja muito pequena. Pelo contrário, é uma imensidão, algo que expõe o tamanho do ciberespaço. Em meados de junho de 2015, a ALPHABET INC noticiou pela mídia que seu buscador Google LLC contava com mais de 14,5 bilhões de páginas indexadas, dentre todos os idiomas falados no mundo.

Isso parece ser estranho, mas é a realidade. Estamos acostumados com o trecho onde se permite indexação nos mecanismos de buscas, que nada mais é que a parte que temos contato diariamente, compreendendo os sites usuais e conhecidos, como *Facebook, WhatsApp, Instagram, Twitter, Wikipédia*, Mercado

Livre, sites de lojas e produtos, *blogs*, enfim, qualquer outra que se permita ser visualizada pelos mecanismos de busca. Dessa forma, a *web* em que todas as pessoas navegam ou, ainda, a única aparentemente existente é caracterizada na literatura científica, por *web* visível (BECKETT, 2009) ou indexável, a que todos veem e utilizam. Ela é conhecida como *"surface web"*, ou, internet de superfície, ou, ainda, "aquilo que podemos ver". A *web* de superfície também é conhecida por outros nomes: *clearnet, indexed web, indexable web, lightnet, visible web*.

Na superfície do ciberespaço, ocorrem muitos crimes virtuais, a maioria deles ao menos se tem uma ideia de que ocorrem ou ocorreram.

Falando-se de uma maneira mais específica e técnica, podemos dizer que na *web* de superfície está uma imensidão de páginas *web*, de fácil acesso, todas realocadas em um servidor remoto, geralmente aberto e/ou visível, onde qualquer pessoa pode entrar e os acessar. A *surface web* é formada por vários computadores, cada um deles conectados entre si, através de uma rede de *links* que se encontram por todo o mundo. Nela é conseguível achar qualquer um destes PC's, desde que se conheça seu endereço, único, onde cada computador ou servidor possui, e que, como vimos anteriormente, chama-se IP (*Internet Protocol*), onde somente assim consegue acessar e ser acessado via Internet.

Note que não estamos mais falamos em protocolos de segurança, pois o lado amedrontador do ciberespaço não se encontra mais no formato ou no tamanho do cadeado, ou em sua robustez, tampouco nas ferramentas que o cybercriminoso utiliza para "arrombar" tal área virtual. Na *surface web* não existe anonimato, de fato, pois todos os sites que você visita acabam armazenando informações daquele acesso, como endereços *IP's*, ou até pessoais, além dos *cookies* (rastros de uso) armazenados em seu navegador.

Além disso, se fazem presentes os domínios (nomenclaturas abreviadas que mostram a origem deles, como os mais conhecidos, *.com, .org, .net, .com.br*, ou qualquer outro). Isso ajuda na indexação e na busca pelos mecanismos de rastreio. Daí que surge a ideia do não-anonimato, pois rastros existem, por mais ínfimos que sejam, sendo, portanto, muito mais um problema de falta de habilidades, de ferramentas apropriadas e/ou de conhecimento técnico para chegar até o criminoso do que qualquer outra coisa.

Sabendo dos perigos que podem correr se forem apanhados cometendo delitos na *surface web*, uma boa parte de cybercriminosos se utilizam de um outro desdobramento do ciberespaço, de uma camada mais profunda dele para cometerem seus delitos. Essa camada mais profunda da internet, ao contrário do que ocorre na *surface web*, não se reporta a um servidor visível, ou alcançável nos motores de busca e indexação de páginas, tornando-as completamente anônimas. É aí que se encontra os criminosos e os crimes mais maquiavélicos e perigosos, visto o espaço sombrio e penumbroso que lhes dão morada, chamada *Deep Web*.

A *Deep Web* também é conhecida com outras nomenclaturas, a saber *Deep Net*, *Invisible Web e Hidden Web*. Em português, pode ser chamado de “Internet profunda” ou até a chamam de “Internet invisível”, terminologia que apareceu em meados de 2009.

Nesta área mais profunda do ciberespaço encontra-se vasto material, nenhum deles indexado ou interligados a servidores físicos e pode conter todo tipo de informação imaginável, desde materiais lícitos quanto ilícitos: são mais de 7.500 *terabytes* de conteúdo dos mais diversos, desde bases de dados de órgãos governamentais de todo o mundo, revistas acadêmicas, revistas científicas, blogs com informações lícitas, mas restritas e direcionadas a um público mais peneirado. O exército, as forças policiais, jornalistas, universidades e até mesmo cidadãos comuns com algum conhecimento de Internet são exemplo de pessoas que recorrem à *Deep Web* para fins específicos (MARTINELLI, 2005).

O fato que permeia esse local mais profundo é que o mesmo pode também ser utilizado para o bem. Não é porque alguma coisa não pode ser achada através dos buscadores convencionais – tipo *Google, Yahoo, Bing* ou qualquer outro - signifique que tudo o que se encontra nessa área obscura é ilegal. O ponto chave da *Deep Web* é o anonimato, atributo quase que unânime em todo e qualquer conteúdo dentro desse imenso pedaço da internet, e não sua legalidade ou ilegalidade, algo vedado pela nossa Constituição Federal.

Por falar nisso, o anonimato é o motivo que faz dessa parte do ciberespaço terra fértil para o cometimento de crimes dos mais diversos, alguns que a justiça e as autoridades policiais sequer têm conhecimento; outros que nem a mente humana é capaz de imaginar serem possíveis de ocorrerem.

Uma das formas mais utilizadas para se ter acesso aos conteúdos restritos da *Deep Web* é através de um navegador específico, distribuídos de forma gratuita na *Surface Web*. Existem algumas dezenas deles capazes de darem acesso ao submundo virtual do plano cibernético, porém o mais utilizado é o TOR – sigla de *The Onion Router* - que nada mais é que uma rede de túneis virtuais construídos com a finalidade de dificultar o rastreamento e a identificação de quem navega por eles. A ideia do tunelamento é mascarar a navegação, a fim de obstruir a identificação dos equipamentos que acessam determinado conteúdo. O TOR dificulta de forma muito objetiva o rastreamento, entretanto, ainda assim não garante a total inviolabilidade dos dados, tampouco a identidade das máquinas (sejam elas computadores ou servidores), pois não é criptografado.

Estima-se que a *Deep Web* é entre 400 e 550 vezes maior que a *Surface Web*. Se a internet de superfície é estimada em 14,5 bilhões de páginas *web*, podemos concluir que a *Deep Web* possui entre 5,80 e 7,98 trilhões de sites. Não existem dados oficiais nesse sentido, haja vista que não existe uma ferramenta capaz de contabilizar tais sites e transformar em dados robustos, pois os sites não são indexados, logo, não podem ser rastreados como na *Surface Web*.

A *Deep Web* esconde ainda em sua estrutura uma parte menor e mais profunda. Nessa área, apontada como a ponta imersa do iceberg, tudo é anônimo, totalmente criptografado e praticamente inalcançável pelos usuários bem-intencionados. Lá se encontra o pedaço do ciberespaço mais sujo, terra muito mais fértil para o cometimento dos crimes mais doentios: chama-se *Dark Web*, também conhecida como *Deep Net, Dark Netinternet*, *onionland*, ou ainda, em português, internet obscura, endereço sombrio ou “a terra das cebolas”, tendo em vista que os sites possuem um domínio *.onion*.

Este nome não é por acaso: A *Dark Web* foi assim batizada graças ao conteúdo disponibilizado lá nas profundezas deste imenso *iceberg*: prostituição pesada, pornografia infantil, serviços *crackers* e *hacker*s, assassinos por encomenda, jogos de azar, drogas ilícitas, conexões terroristas das mais diversas, comércio de órgãos humanos e das chamadas bonecas sexuais humanas, sendo esta um dos crimes mais pérfidos e cruéis, onde apenas uma ínfima parcela da população tem conhecimento desta atrocidade.

As bonecas sexuais[3] geralmente são meninas, crianças ou em fase de pré-adolescência, geralmente na faixa dos 8 a 14 anos, de origem muito humilde, onde, aproveitando-se da condição financeira da família dessas pequenas, os pervertidos criminosos sádicos compram-nas por um valor muitas vezes irrisório.

Após a compra, os *"Doll Makers"* (criminosos que compram as infantes) as submetem a procedimentos cirúrgicos dolorosos. Geralmente retiram seus braços, suas pernas e todos os dentes, por vezes substituindo tais partes do corpo por próteses sob medida. Além disso, cortam suas cordas vocais, tudo isso para que não ofereçam nenhuma resistência ou perigo durante as perversões de seus donos.

Essas crianças, após a cirurgia, possuem uma estimativa de vida de apenas um ano, morrendo após esse período. Elas são encomendadas e vendidas através da *Dark Web*, geralmente por um preço exorbitante. Tudo de forma anônima.

Os atos ilícitos que ocorrem neste pedaço sombrio da *Deep Web* só são possíveis pelo uso dos *bitcoins*, uma moeda virtual criptografada, que movimenta dinheiro de verdade, geralmente através de *internet banking*, dispostos em sites na *Surface Web*. Sua finalidade principal é permitir a transação financeira entre quem oferece os serviços escusos e quem procura e paga por eles, de forma anônima. Esta rede atua de forma totalmente autônoma, sem um banco de dados medular ou singular, permitindo que seus usuários possam negociar diretamente uns com os outros sem um atravessador, tudo da forma mais anônima possível e conseguível, sem nenhum problema ou medo de serem apanhados.

Por não possuírem uma força ou base de dados central, sendo, portanto, uma rede totalmente descentralizada, torna suas atividades um grande desafio aos agentes da lei, pois estes não conseguem detectar estas atividades, muito menos identificar usuários, obter registros das negociações financeiras e, consequentemente, iniciar uma ação penal. É aí que os cybercriminosos, sabendo de tudo isso, faz uso máximo dessa incerteza legal para praticarem inúmeros delitos.

[3] Até o presente momento, nenhum órgão governamental mundial conseguiu obter com precisão a origem dos *Dolls Makers* pelo mundo. As informações são escassas, por vezes tratadas como Lenda Urbana. Porém, sabe-se que todas as transações monetárias são via *Bitcoin*, e tudo ocorre de maneira muito sigilosa, não deixando qualquer rastro. Sabe-se, porém, que não são um ou dois grupos, e sim dezenas deles oferecendo o serviço na Deep Web. Sua principal área de atuação é no Leste Europeu, em povoados e lugarejos humildes. Essa informação não anula a possibilidade real de uma ligação entre desaparecimentos de crianças em outros lugares do mundo, sobretudo mais pobres, como América Latina e África.

Apesar de a *Dark Web* ser encoberta e protegida pelo tunelamento e criptografia do TOR, algumas informações vazadas recentemente indicam que a NSA (*National Security Agency*) – a Agência de Inteligência Americana – possui recursos, ferramentas funcionais que consigam rastrear usuários do TOR.

CAPÍTULO II

1. DOS CYBERCRIMINOSOS:

1.1 OS CYBERCRIMINOSOS E SUAS FERRAMENTAS

Na atualidade, é clarividente que a tecnologia vem se difundindo e se alargando cada vez mais em nosso cotidiano. Com isto, crescem também as possibilidades de usuários e empresas serem vítimas do cometimento de crimes e de ataques virtuais. A internet vive uma conjuntura onde qualquer desatenção pode ser mortal, afinal de contas, é a segurança de seus dados que está sob iminente risco. A grande maioria dos golpes realizados pela Internet podem ser apontados como crimes contra o patrimônio, tipificados por nosso código penal como estelionato.

Após o advento do computador e sobretudo da internet, toda a população que faz uso dela se habituou a escutar o termo “vírus” para computadores. Até então, a palavra “vírus” era comum na área biológica, de saúde, sendo utilizada tão somente para designar os agentes ocasionadores de doenças infectocontagiosas. Mas dentro dessa temática, o vírus que aqui exponho não é o biológico, mas sim o eletrônico.

Em uma explicação descomplicada, os vírus são pequeninos softwares, desenvolvidos por conhecedores de linguagem de programação, com o intuito de acarretar danos ao usuário e a seu computador. O vírus tem como objetivo primordial desestabilizar o sistema, seja prejudicando o seu desempenho, destruindo arquivos ou mesmo se espalhando para outros computadores.

Os vírus mais comuns encontrados atualmente são os já inseridos em programas e arquivos existentes, mais precisamente em seus instaladores. Estes aplicativos nocivos são normalmente ativados quando o usuário clica em algum instalador de programa (oriundo da internet) ou em algum programa executável (com a terminação .exe).

Desde que os vírus apareceram, mais precisamente entre 1983 e 1986, nunca foi possível eliminá-los totalmente, pelo contrário, todos os dias surgem novos vírus, cada um com uma finalidade. Sabemos, inclusive, que existe um mercado negro para vírus, principalmente os próprios para roubo de senhas de banco e

também cartões. Por isso, o velho ditado também vale para o mundo tecnológico: É melhor prevenir do que remediar. Assim, o melhor que podemos fazer para nos proteger dessas pragas virtuais é trocar as senhas com frequência de: e-mail, sites de bancos, não clicar em arquivos suspeitos e também sempre deixar o antivírus sempre atualizado.

As maiores ocorrências de infecções no meio tecnológico acontecem por desleixo do próprio usuário, normalmente rodando em seu computador um arquivo já infectado que tenha vindo por e-mail ou outro meio. Esta infecção também pode ocorrer mediante arquivos contaminados em *pendrives*, *CD's, DVD'S*, cartões de memória e outros dispositivos. Outro facilitador para que a contaminação ocorra é a desatualização do SO - Sistema Operacional. Em uma rápida analogia, quando a base de dados deste encontra-se defasada, é como se as portas do seu computador estivessem abertas, totalmente desprotegidas, facilitando a invasão do intruso e a infecção da máquina.

Os cybercriminosos tem se aproveitado e usufruído destas brechas, agindo de forma absolutamente silenciosa, logrando êxito muitas vezes em ultrapassar as barreiras impostas pelos softwares *antivírus*, além do firewall nativo do sistema operacional, sem sequer ser notado.

Desta maneira, vêm aumentando de forma muito significativa o cometimento de crimes virtuais, haja vista que as informações de muitos usuários e até não usuários acabam sendo clonados, copiados, roubados sem sequer perceberem. Uma boa parcela das grandes ameaças existentes está neste exato momento tentando invadir o seu computador, durante todo o dia, por exemplo. E você já deve ter visualizado algumas destas ameaças sendo bloqueadas por seu *software* antivírus.

A seguir, elenco as principais ameaças que permeiam o meio virtual, senão vejamos:

a) Trojan Banking: Essa ameaça foi desenvolvida/programada para roubar e/ou furtar dados bancários, tais como senhas numéricas e alfanuméricas, silábicas, assim como dados de sites de e-commerce, senhas de todos os tipos de redes sociais, como também de servidores de e-mail. É um software nocivo e de alta

periculosidade, pois esse tipo de invasão ocorre por intermédio de sites infectados, mensagens de e-mail, e até mesmo vindo atrelados a outros downloads feitos tanto através de navegadores quanto de programas P2P; é um tipo de vírus que acaba se espalhando de forma muito rápida pela rede e pelo sistema operacional hospedeiro, o que o rotula como um dos tipos mais perigosos.

b) Keylogger: o *Keylogger* é um *software* capaz de acompanhar, fiscalizar e armazenar movimentações no sistema operacional. Ele é instalado na máquina que se deseja monitorar, onde fica de forma oculta, observando tudo que o usuário faz. Para se ter uma noção do perigo desse tipo de *software*, ele armazena até as teclas digitadas pela vítima, sites acessados, programas utilizados, alguns com poder de até armazenar data e hora que determinado procedimento foi realizado; depois de um certo tempo (que pode ser programado também), ele envia um relatório aos cybercriminosos. O risco de deixar informações pessoais (tais como senhas e cartões de bancos, por exemplo) sempre armazenados em alguns sites ou até mesmo no próprio navegador, de maneira automática, é extremamente perigoso. Fazemos isso corriqueiramente, para que não precisemos teclar tudo novamente quando formos acessar novamente, mas é aí que os cybercriminosos se aproveitam para utilizar o *Keylogger* para o roubo de logins e principalmente para dados bancários.

c) Ransomware: O *ransomware* é um conjunto de códigos maliciosos que formam um *software*, que tem como intuito sequestrar dados, principalmente arquivos pessoais, tais como documentos, fotos, músicas, vídeos, textos e instaladores do computador da vítima através de técnicas avançadas de criptografia.

Já existem alguns ransomware mais fortes que sequestram todo o sistema operacional da vítima. Ele bloqueia o computador de forma completa, sem chance para ações coordenadas.

Após a consumação do sequestro, o *malware* fica exibindo na maioria das vezes umas mensagens bem chatas na tela inicial, informando ao sujeito passivo que o dispositivo foi crackeado e se caso a vítima deseje reobter o controle de seu dispositivo, precisará realizar um depósito financeiro em alguma conta corrente fria –

os mais espertos pedem depósitos de *bitcoin*, o que torna a recuperação um pouco mais dispendiosa e morosa - ou pedem até para que a vítima compre para ele determinados produtos; só depois disso, eles passam alguma senha e a vítima reavêm seu sistema de volta.

d) Adware: Os *adwares* são softwares cujo foco e objetivo principal é executar e exibir automaticamente na tela do sujeito passivo e sem nenhum tipo de autorização do mesmo, vários anúncios diversos tipos, desde anúncios de produtos, programação televisiva, dentre outros. São programas que em sua grande maioria vem atrelados a instaladores de *softwares*, geralmente obtidos por meio de *downloads* na internet. Sua função é mostrar anúncios junto às páginas da web, como também fora dela, o que os tornam bastante incômodas e perigosas, pois nada mais são que uma maneira fácil e barata de fazer publicidade para determinadas organizações, de uma forma muito invasiva, além de impertinente, pois consomem muita memória e poder de processamento do computador da vítima, que fica bastante lento. Além de tudo, esse tipo de programa é bastante resistente, pois após ser instalado, são extremamente difíceis de se conseguir desinstalá-los. Na maioria das vezes estes softwares não figuram nas listas de programas instalados, deixando-os praticamente impossíveis de serem desinstalados de maneira habitual, o que faz com que o computador necessite de formatação para poder retirá-los, algo que causa um transtorno enorme para o usuário da máquina.

e) Backdoor: Os *backdoors* também são uma ferramenta usada pelos cybercriminosos para conseguirem acessar de forma remota o sistema operacional do sujeito passivo, ou até mesmo de toda a rede, previamente infectada. O *backdoor* é uma ferramenta capaz de abrir a porta dos fundos da máquina da vítima. Uma vez aberta, esses indivíduos conseguem instalar inúmeros *malwares* na máquina ou no sistema da vítima, tendo em vista que eles exploram falhas muito críticas que já existem, oriundas de *softwares* desatualizados e do *firewall* da máquina ou servidor. Ao ter acesso, o cybercriminoso abre portas do roteador, e assim consegue registrar teclas digitadas, tirar *screenshots*, gravar áudios, visualizar arquivos, altera-los, tudo de maneira remota, sem que a vítima sequer tome ciência do que está acontecendo.

f) Rootkit: Os *rootkits* são um tipo de *trojans* que necessitam de uma forma mais avançada de programação para serem desenvolvidos e instaladas. A instalação ocorre em camadas não documentadas do sistema da vítima, tornando extremamente difícil a atuação de softwares antivírus para detectarem tais intrusos, tendo em vista seu tamanho – que é ínfimo perto de outros tipos – como também por terem sido programados para se esconderem até deles mesmos dentro do sistema operacional da vítima. O meio de funcionamento dele é através de um malware que integra um código ao sistema operacional da vítima e intercepta toda e qualquer solicitação de leitura de arquivos, desde as comuns até as mais complexas. A parte mais complicada do trojan é que mesmo após ser achado e excluído da máquina hospedeira, ele consegue ainda sim se recuperar, se reinstalar automaticamente após a varredura realizada por um software antivírus, o que faz com que o mesmo permaneça dentro do sistema da vítima por muitos meses, até anos, facilitando de forma muito consistente o acesso à equipamento e/ou servidor por crackers, onde estes farão uso deles para o cometimento de atividades criminosas.

g) Timebomb: Essa modalidade de *malware* é comumente chamada de bomba relógio, tendo em vista que o mesmo trabalha com um marcador de tempo, onde o mesmo é programado para apenas ser executado em determinado momento na máquina hospedeira, e não de forma recorrente, como ocorre na maioria dos vírus. Este tipo de malware pode causa dezenas de danos. Geralmente são proliferados via *e-mail*, que, ao realizarem o download do arquivo malicioso, instala também o a bomba relógio no computador do sujeito passivo.

h) Browser Hijacker: O *Browser Hijacker* é uma modalidade muito comum atualmente de vírus, bastante usado por golpistas. Seu objetivo principal é alterar as principais configurações dos navegadores do computador da vítima, desde a homepage, favoritos, e os mecanismos de busca. Rotineiramente também exibem anúncios e propagandas em sites legítimos, como fazem os adwares. Ganham a confiança do usuário pois aparecem em páginas verdadeiras, como a do Google, por exemplo. O usuário acha interessante e seguro, clica e acaba sendo levado a sites maliciosos que podem conter *exploits* ou outros vírus que podem danificar de forma muito forte o computador da vítima.

i) Worm: *Worm* é um programa similar a um vírus, com a diferença de que ele se auto propaga através de uma rede de computadores, e sem ajuda de uma pessoa (CASSANTI, 2014). O *worm* é um tipo de vírus programado para, de forma extremamente maliciosa se espalhar através da rede sem que nenhum dos usuários tome ciência de sua ação e interfira em seu objetivo, que é consumir ao máximo banda de navegação da rede e criar cópias de si mesmo sem nenhum critério. Geralmente são espalhados em um processo totalmente automatizado, previamente programado. Ele pode também ser proliferado através de anexos em e-mail, como o *Timebomb* e outros.

j) Rogue Security Software: Este *malware* geralmente se apresenta aos usuários como um software antivírus ou *antispyware* confiável. Assim, ele já consegue um de seus objetivos primários, que é enganar os usuários. O software Rogue Security é instalado e executado sem a anuência do usuário. Quando é visualizado, se mostra inofensivo, realizando escaneamentos de vírus, mostrando notória eficiência e eficácia, detecta inúmeros vírus existentes no computador da vítima, mas na hora de realizar a limpeza, informa que o usuário precisa adquirir a licença do software, geralmente através de cartão de crédito, depósitos bancários. Entretanto, essa informação é completamente enganadora: na verdade não há vulnerabilidade alguma em seu computador, mas essa é a forma deles aplicarem o golpe, manipulando o usuário, enganando-o, levando a crer que existe ameaças somente a fim de obter vantagens pecuniárias ilícitas sobre os usuários.

k) Vírus Stealth: Os *vírus Stealth* são um raro tipo de malwares. Sua forma de ataque é através da criptografia reversa, capaz de evitar sua detecção por ferramentas de segurança, tais como antivírus e firewalls, sempre instaladas nos computadores. Eles são um tipo de vírus computacional bastante difícil de ser detectado, como também de ser excluído, pois corriqueiramente invadem o sistema operacional quando o usuário da máquina instala *malwares* disfarçados como programas de *websites* e faz *downloads* de anexos de e-mails mal-intencionados.

l) Vírus de Macro: O vírus de macro basicamente é uma gama de comandos automatizados embutidos em diversos softwares ao serem instalados, como processadores de textos como *Word, Excel* e de imagens, como *Photoshop e Corel Draw*. Quando o *software* é executado, também roda o vírus, que de maneira muito rápida se espalha, ocasionando anormalidades das mais diversas em todos os arquivos que aquele *software* consegue ler, como documentos de textos, imagens, dentre outros. Outra atribuição desse tipo de vírus é o acesso a contas de e-mail previamente abertas na máquina doente. Ele consegue enviar cópias de arquivos infectados para outros usuários com a conta que estava aberta na máquina infectada, proliferando-se na rede.

m) Joke Program: Os *Joke Program* são códigos maliciosos que tem como objetivo causar danos temporários no sistema da vítima. Esses danos podem ser de menor ou maior proporção, variando desde pequenos e incômodos travamentos até a interrupção de execução de softwares, além de trocas inesperadas de atitude do software e da máquina do usuário. Tecnicamente, esses códigos não ocasionam nenhum dano real ao computador do sujeito passivo, entretanto causam muita irritação ao usuário. Eles podem ser identificados de uma forma mais rápida que outras modalidades de vírus, sendo corriqueiramente capturados pelos programas antivírus habituais.

n) Greyware: O *Greyware* são softwares maliciosos instalados no computador da vítima sem o pleno consentimento do usuário, ficando situados entre o software convencional e o vírus. O *Greyware* pode ou não conter malícia em sua programação, sendo então na maior parte das vezes um tipo de programa mais irritante do que perigoso. Eles são aqueles programas de piadas e *adwares* que acabam sendo instalados nos computadores sem você saber. Ainda pode ser prejudicial ao usuário, pois ele engloba ameaças como *spyware, adware, trackwares* e muitos outros programas indesejáveis a qualquer usuário de computador, quais são projetados para prejudicar o desempenho das máquinas.

o) Trojan Horse (Cavalo de Tróia): Dentre tantas modalidades, esta com toda certeza é o mais conhecido de todos. O nome cavalo de Tróia é referência direta ao histórico episódio da luta grega contra os troianos, que usaram um imenso cavalo de madeira para se esconderem e, assim, transpassarem os altos e imbatíveis muros da cidade de Tróia, que, achando ser um presente dos deuses, baixaram a guarda e abriram suas portas para trazerem o suposto presente para dentro de seu território.

O cavalo de Tróia faz menção ao primeiro estágio da infecção, cumprindo o papel de esconder o *software* malicioso. Esse vírus tem por objetivo abrir uma porta para que um cracker consiga acessar o computador infectado, tudo de maneira remota. Para CASSANTI (2014), no mundo virtual a ideia é a mesma; ou seja (...), um cavalo de Tróia é um arquivo aparentemente inocente entregue pela porta da frente, mas que contém um elemento malicioso escondido em algum lugar dentro dele.

O Cavalo de Tróia, ao contrário dos *Worms*, por exemplo, não tem a capacidade de se reproduzirem, mas podem infectar através do download de instaladores de softwares previamente infectados ou preparados como hospedeiro, além de músicas, vídeos, fotos, anexos de e-mail e até mesmo o simples acesso a um determinado site malicioso, onde o cybercriminoso se aproveita da fragilidade do navegador da vítima para conseguir instalar a praga. Geralmente os programas antivírus conseguem detectar esse tipo de ameaça e a neutraliza a tempo de causar grandes consequências.

p) Spyware: Segundo mais utilizado pelos *crakers*, os *spywares* são softwares espiões utilizados pelos cybercriminosos basicamente para monitorarem as atividades e capturarem informações e dados sigilosos do sujeito passivo. Desta maneira, eles acabam criando um imenso banco de dados de *spams*, com propagandas personalizadas, que servem para induzirem as vítimas a adentrarem. O *Spyware* geralmente infecta suas vítimas através de *downloads* de anexos de *e-mails*, além do acesso a *websites* previamente ensinados a infectar, além de conexões diretas para o compartilhamento de arquivos.

Apesar de todo esse rol aqui esmiuçado, estas não são todas as ameaças existentes, e sim as mais conhecidas e utilizadas atualmente pelos cybercriminosos, a fim de praticarem crimes virtuais, tirarem proveitos de suas vítimas. Apesar de ter sido apresentado uma vasta lista, existem inúmeras outras.

2.2 ONDE SE ESCONDEM OS CYBERCRIMINOSOS?

Até bem pouco tempo atrás, os cybercriminosos estavam, em sua imensa maioria, localizados nos Estados Unidos, Canadá, Europa e Ásia. Porém, devido às questões políticas, os olhares se voltaram para a América Latina, em especial para o Brasil. E não só por questões políticas: questões sociais ou até mesmo em razão dos grandes eventos ocorridos nos últimos 5 anos no país (Copo do Mundo FIFA, Jogos Olímpicos, etc), nosso país e continente entraram de uma vez por todas no mapa do crime virtual, não só como destino de ameaças, como também de desenvolvimento de grupos *crackers*.

Um relatório divulgado em 2017 pela Norton Cyber Security[4] revelou que o Brasil é o segundo país do mundo com o maior número de casos de crimes cibernéticos. Esses crimes afetaram aproximadamente 62 milhões de pessoas e gerou um prejuízo de mais de R$80 bilhões.

Nesse contexto, diversas ameaças surgiram nessa época no cenário nacional. As mais recentes são o *ransomware*, o malware sequestrador e o Dilma Locker (que teve seu nome inspirado na ex-presidente Dilma Rousseff). Este último atingiu uma pequena parcela de usuários, afetados por arquivos falsos enviados por e-mail. O resgate inicial solicitado pelo cyberatacante foi de R$ 3 mil.

Mas, afinal, que tipo de criminoso está por trás de ameaças como essa?

Entre tantas modalidades de cybercriminosos, já listadas anteriormente neste trabalho, os "*script Kiddie"* (aqueles que possuem pouca ou quase nenhuma habilidade técnica) são os mais frequentes. Geralmente, os que se dispõem a praticar tais ameaças conseguem acesso à códigos maliciosos disponíveis no *Git Hub,* uma plataforma virtual para cooperação e compartilhamento de códigos de

[4] FONTE: https://www.geledes.org.br/web-registra-cerca-de-100-mil-casos-de-racismo-em-uma-decada/

programação. Esses indivíduos assistem alguns vídeos no YouTube, aprendem algumas técnicas básicas e já se intitulam *crackers*. Conseguem causar alguns estragos, mas nada numeroso e relevante.

Por outro lado, existem os superprofissionais, aqueles que conseguem realizar ataques em série, criar códigos indecifráveis e causarem estragos gigantescos se munidos com a ferramenta correta e frente a um sistema sem segurança.

Existe no Brasil, atualmente, um notório crescimento de grupos que programam *ransomwar*e. Esse tipo de criminosos efetua provas de conceito consistentes aqui no Brasil e depois que tomam ciência que o golpe online de fato funciona, oferecem traduções para outros idiomas, geralmente espanhol, italiano e inglês. Aqui no Brasil já fazem uso de um tipo de *ransomware* cujo valor chega a custar US$ 400. Esse arquivo é disponibilizado através de um kit para quem não possui qualquer conhecimento no mundo de segurança cibernética.

A verdade é que o *cybercriminoso* brasileiro percebeu que o *ransomware* é uma zona de segurança para ele, tendo em vista que o pagamento ocorre de maneira totalmente anônima, na maioria das vezes não por moeda real (dólar, real, euro, por exemplo), mas sim através de bitcoin, sendo, portanto, muito difícil de se rastrear quem efetuou ou quem recebeu tal pagamento.

É fato que existe uma clarividente tendência desse tipo de ameaça aumentar no Brasil nos próximos anos. Até o momento, não existem relatos através da grande mídia de que alguém tenha sido preso no país por causa de *ransomware*. Entretanto, o desafio e a sorte estão lançados, e se encontra em todas as direções possíveis.

Entretanto, para que tais atos cheguem a tomar proporções que atentem a sociedade quanto a seus perigos, dois pontos tornam-se cruciais e de extrema importância: Primeiro, é necessário que a vítima da agressão cybernética formalize o ataque através dos poucos meios oferecidos atualmente, e nem todas as vítimas os fazem, justamente por se tratar de um ameaça muito recente e pouquíssimo conhecida.

O segundo ponto importante é quanto a regulamentação. O Brasil necessita urgentemente de leis capazes de oferecer proteção de dados de uma forma mais

eficaz e menos burocrática. Mas a classe política e judiciária não parece estar muito preocupada com isso. E isso tem muito a ver com a ignorância dessas classes frente aos perigos dos cybercrimes para a sociedade.

2.3 A ORGANIZAÇÃO CYBERCRIMINOSA E O MERCADO DE CRIMES CYBERNÉTICOS

À medida em que a tecnologia se desenvolve ao longo dos anos, os criminosos virtuais também caminham a passos largos, a fim de acompanharem o frenético ritmo do desenvolvimento tecnológico e virtual, para não ficarem de fora do "mercado". Com isso, eles estão ficando cada vez mais organizados e profissionais. É o que mostra o site Canaltech[5], especializado em tecnologia e segurança de dados, em matéria veiculada em seu site no ano de 2013. A prova disso é o último relatório de crimes cibernéticos da *FORTINET*, empresa especializada em segurança digital, que os chamam de "empresários" do mundo virtual.

A pesquisa mostra que o crime virtual também está se organizando, assim como acontece com o tráfico. Já existem diversas organizações que dividem seus "funcionários" em diferentes cargos que devem respeitar uma hierarquia, como executivos, gerentes e funcionários de baixo escalão.

Mas que tipo de serviço essas organizações oferecem? Geralmente elas trabalham para gerir e proteger redes zumbis, fazendo a mudança constante de endereços de IP, por exemplo. Além disso, elas podem até mesmo cobrar por consultoria dessas *botnets* e, segundo o relatório da *FORTINET*, o valor cobrado gira em torno de US$ 350 (R$ 1400) a US$ 400 (R$ 1600) pelo serviço.

A pesquisa da empresa também conseguiu descobrir outros valores da "tabela de preços" de serviços dos criminosos da Internet. O aluguel de uma rede *botnet*, por exemplo, custa US$ 535 (R$ 2140), com direito a uso por cinco horas diárias durante uma semana.

[5] A matéria do site Canaltech também traz em seu escopo um link que direciona ao site da empresa FORTINET, onde lá são apresentados, mediante um cadastro prévio, dados mais completos e de extrema relevância, base da referida informação.
Disponível em: https://canaltech.com.br/hacker/Cibercriminosos-estao-cada-vez-mais-organizados-e-agora-agem-como-empresarios/

Quem deseja descobrir uma senha desembolsa US$ 17 (R$ 68) a cada 300 milhões de tentativas, algo que é feito em cerca de 20 minutos. Para infectar e distribuir vírus, os cybercriminosos cobram cerca de US$ 100 (R$ 400).

2.4 CRIMES VIRTUAIS MAIS FREQUENTES

Tecnicamente, a internet é um belo modelo de “sociedade ideal”, onde todas as pessoas que dela fazem uso são iguais e anônimas, e possuem as mesmas condições de serem e terem o que quiserem. Todos – na rede mundial de computadores – são alguém e ninguém ao mesmo tempo. Ela é universal do ponto de vista do alcance, e inevitável, do ponto de vista da necessidade. E isso formou um modelo de sociedade da informação, cujas características são seus próprios benefícios e malefícios.

A internet abarcou e carregou consigo uma rapidez de relacionamentos em todos os âmbitos, seja nos negócios, no comércio, nas relações pessoais íntimas e derrubou fronteiras, principalmente as físicas, oportunizando uma autonomia e independência a quem lhe faz uso totalmente extraordinária e jamais pensada antes.

No entanto, na mesma velocidade em que ocorre essa ascensão da internet e da tecnologia a ela ligada, as ameaças cometidas através e pelo computador se refinam ao longo do tempo. A disseminação de novos equipamentos e tecnologias, além de novos conhecimentos, linguagem de programações, também fizeram surgir novos métodos para a proliferação de ameaças.

O cidadão corriqueiro, que faz uso da tecnologia no dia a dia é a principal vítima do delito informático, onde falando de forma geral, sua grande maioria sequer compreende o meio em que estão inseridos, tampouco as dificuldades e os danos, os estragos que podem lhe serem impostos por outro usuário, seja esse mal-intencionado ou não. O uso sem conhecimento deste meio informático e de qualquer tecnologia de modo geral estabelecem uma ameaça muito forte e real.

É fato que a internet além de ensejar a comunicação entre as pessoas, também carregou a seu lado uma infinidade de benesses que podem ser acessados com apenas um simples clique. Comprar no conforto de sua casa ou realizar pagamentos de contas corriqueiras através da internet banking por exemplo, ficou

extremamente mais fácil, tranquilo e conveniente, tendo em vista que se evitou as filas muito comuns.

Todavia, simultaneamente ao que a internet passou a significar clareza, incomplexidade e economia de tempo, foi base para o aparecimento de novíssimos transtornos, tendo em vista que pessoas mal-intencionadas também se aproveitaram da tecnologia para tirar proveito. Foi nesse contexto que surgiram os primeiros casos de crimes no espaço virtual. E são várias as transgressões realizadas através da internet, desde fraudes bancárias, desvios de quantias milionárias de dinheiro, pornografia infantil (desde a produção, oferta e procura de materiais audiovisuais com crianças, além da transmissão e posse de fotografias de menores de idade em comportamento sexual explícito), falsificação de dados públicos e particulares, estelionatos eletrônicos, racismo e xenofobia (difusão de imagens, ideias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica, injúria e ameaças qualificadas pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade), etc.

A lista de crimes cometidos no ambiente virtual é, sem dúvidas, muito extensa, demasiadamente longa. No entanto, existem aqueles que são praticados de forma mais corriqueira, podendo afetar qualquer cidadão de uma forma mais recorrente.

Listamos os mais corriqueiros na rotina de um cidadão comum, a seguir:

2.4.1 Crimes contra a Honra: Calúnia, Injúria e Difamação

O Código Penal Brasileiro dispõe sobre a injúria e a difamação nos arts. 138, 139 e 140 e esclarece:

> “Art. 138. Caluniar alguém, imputando-lhe falsamente fato definido como crime: (...) “
>
> “Art. 139. Difamar alguém, imputando-lhe fato ofensivo à sua reputação: (…) ”
>
> “Art. 140. Injuriar alguém, ofendendo-lhe a dignidade ou o decoro (…) ” (Código Penal Brasileiro, 1940, n.p).

De forma objetiva, os artigos 138, 139 e 140 do Código Penal Brasileiro alega que divulgar informações falsas em relação a uma pessoa ou a uma empresa é crime e pode levar a diversas penalidades. Quando a divulgação é realizada por meios de comunicação tradicionais, como conversas ou jornais impressos, o crime é comum, mas se ela ocorrer por meio da internet, será um crime virtual. Neste caso, o meio virtual é uma ferramenta para o cometimento da ilicitude, além de ser o meio para a consecução do delito.

As vítimas de tais delitos penais podem e devem procurar o poder judiciário, a fim de requerer indenização e reparação do dano. Entretanto, é de extrema importância procurar uma Delegacia Especializada (caso exista) e registrar a denúncia.

Caso o problema aconteça com você ou com o seu negócio, a orientação dada pelas autoridades policiais é que a vítima deve tomar as providências de forma rápida e evitar que a informação mentirosa chegue a mais pessoas e cause transtornos, e procurar a delegacia urgentemente.

Para evitar transtornos e dores de cabeça o ideal é adotar medidas preventivas e fazer um controle intenso sobre o conteúdo que se divulga na internet. Analisar os textos e pensar no impacto que eles podem causar antes de tornar público é extremamente importante.

2.4.2 Apologia ao crime e ameaça a vida e a dignidade de terceiros

É muito corriqueiro o surgimento de páginas em redes sociais e perfis falsos que estimulem o cometimento de crimes como pedofilia, xenofobia, racismo, furtos e roubos, venda de drogas e armas, etc.

Esses tipos de perfis comumente dispõem de acesso restrito e seus membros compartilham dicas, e até sugestões para o cometimento de vários atos ilícitos. A questão é que, além de serem absolutamente extralegais, podem acabar penalizando e envolvendo pessoas que jamais ingressaram em tais páginas como membros.

Em caso de suspeita de páginas com conteúdo desse tipo o ideal é realizar a denúncia imediata do site ou da página na rede social. Essas denúncias costumam ser verificadas com rapidez e contribuem muito para o controle e para a segurança das redes.

Também é importante procurar as delegacias de crimes cibernéticos e registrar reclamações. Além de possibilitar a investigação, essa medida auxilia nas estatísticas e aumenta as discussões sobre mecanismos de proteção aos usuários.

2.4.3 Furto e/ou roubo de dados virtuais e informações pessoais privadas

Outro crime que acontece de forma muito habitual na internet é o de furto de dados. Ele é bastante vasto, podendo acontecer de inúmeras formas diferentes. Tecnicamente, a maioria de seu cometimento é enquadrado como estelionato e definido da seguinte forma pelo Código Penal Brasileiro:

> “Art. 171: Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento. ”
>
> (Código Pena Brasileiro, 1940, n.p). ”

Uma maneira bastante corriqueira de cometer esse delito é geralmente criando sorteios ou entregas fictícias de prêmios em páginas de redes sociais. Em troca de possíveis premiações, os interessados precisam se cadastrar e instalar alguns aplicativos, tendo que inserir dados pessoais, endereço, CPF, datas de aniversário, enfim, uma série de informações. Após o envio para o fraudador, esses dados são utilizados a posterior para o cometimento de outros crimes. A fraude não para por aí, sendo este somente o primeiro momento do golpe.

2.4.4 Utilização, reprodução e comercialização de *softwares* falsos (*copyright*)

Assim como no crime anterior, este também possui inúmeras maneiras de ser aplicado. O mais corriqueiro deles é a venda de licenças piratas de softwares comerciais, que geralmente são bem caros se comprados de forma legal. Não é difícil achar anúncios em sites de vendas, como Mercado Livre, por exemplo, de pessoas comercializando licenças de programas como Corel Draw, Photoshop,

Office, enfim. Além da comercialização desses produtos desta maneira, a compra também é caracterizada como crime.

Além disto, alguns destes softwares quando instalados no computador de quem adquiriu, permite o acesso a todos os dados pessoais registrados na máquina. Com estes dados em mãos, o criminoso consegue cometer outras dezenas e delitos, desde a falsificação de cartões de créditos, realização de transações bancárias, dentre outros.

O crime é mais comum do que pode parecer e está previsto no art. 154-A do Código Penal Brasileiro, nos seguintes termos:

> “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: (…) (Código Penal Brasileiro, 1940, n.p). “

A recomendação de especialistas na área de segurança de dados é, antes de instalar qualquer programa, pesquisar sua confiabilidade, além de adquirir softwares e licenças de forma online através de sites seguros. É possível fazer isso a partir de pesquisas no Google ou de conversas com o seu suporte de TI.

Esteja sempre atento aos riscos e evite instalar programas com nomes desconhecidos. O roubo de dados pode demorar anos para ser descoberto e você pode ter prejuízos enormes em razão dele.

Para as empresas, os danos podem ser ainda maiores do que para as pessoas físicas, já que os computadores costumam guardar informações confidenciais e dados bancários de maior relevância.

2.4.5 Crimes de falsidade

A internet, sobretudo as redes sociais tornaram-se um autêntico fenômeno de popularidade que se confundem com o próprio conceito de internet para vários brasileiros.

Se por um lado esta nova maneira de comunicação propicia o surgimento de vários negócios, amizades e até relacionamentos amorosos (namoros, noivados, casamentos, uniões estáveis, etc.), por outro, tem sido o cenário ideal para a prática de inúmeros abusos previstos na nossa legislação. E um deles é o crime de falsidade.

Apesar de comumente ser imaginado como sendo apenas uma modalidade, os crimes de falsidade ocorrem de três maneiras, e sua penalidade visa a proteção da fé pública e particular objetiva, um bem jurídico tutelado pelo Estado e que expõe a indispensável e inescusável fidúcia da sociedade em determinadas informações, instrumentos públicos ou privados, assim como nas características pessoais de cada um de nós.

Os documentos escritos, digitados, redigidos, possuem como função social tornar físico a externação de uma vontade, de um ato relevante. É a perpetuidade da ânsia, de um propósito, é a garantia probatória de um fato relevante para a sociedade e para o judiciário.

Nosso Código Penal, em seu artigo 232, dispõe o seguinte:

> “Art. 232: Consideram-se documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares.
>
> Parágrafo único. À fotografia do documento, devidamente autenticada, se dará o mesmo valor do original.

É baseado nessa proposição de fé pública que construímos o conceito de que tudo que é aventado por meio de um documento - seja ele público ou particular - deve ser verdadeiro. Essa premissa forma o conceito do crime de falsidade, e o torna antônimo de fé pública.

A seguir, elenco os três tipos que caracterizam e tipificam o crime de falsidade, senão vejamos:

2.4.5.1 Falsidade Material: A identidade Dissimulada (falsificação de documento público e/ou particular)

A falsidade material ocorre quando o agente cria um documento falso com informações falsas ou altera o conteúdo de um documento verdadeiro com informações ludibriadoras utilizando o computador. O documento torna-se materialmente falso. A falsificação ocorre mediante contrafação (fingimento, simulação, disfarce, falsificação de modo a iludir sua autenticidade). Neste caso, o meio digital por vezes é utilizado somente como ferramenta para o cometimento do ilícito.

Os crimes de falsidade material (que pode ser quanto a documento público ou particular), estão tipificados, respectivamente, nos artigos 297 e 298, do Código Penal, senão vejamos:

> "Falsificação de documento público
>
> Art. 297 – Falsificar, no todo ou em parte, documento público, ou alterar documento público verdadeiro:
>
> Pena – reclusão, de dois a seis anos, e multa.
>
> (…)
>
> Falsificação de documento particular
>
> Art. 298 – Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
>
> Pena – reclusão, de um a cinco anos, e multa.
>
> (Código Penal Brasileiro, 1940, n.p). "

Apesar da efetividade demonstrada em nosso Código Penal, os crimes informáticos trouxeram também a separação dos crimes de falsidade, fazendo surgir mais dois tipos, senão vejamos:

2.4.5.2 Falsidade Ideológica: Documento verdadeiro com informações falsas

A falsidade ideológica, por sua vez, configura-se pelo falso conteúdo posto quando da feitura de um documento verdadeiro. O documento é verdadeiro, emitido por órgão competente, mas seu conteúdo, suas informações não condizem com a realidade. Temos por exemplo a declaração de valor menor na escritura pública de

compra e venda de imóvel, ou a omissão ou declaração de informações falsas no ato da Declaração do Imposto de Renda, por exemplo.

O crime de falsidade ideológica está disposto no artigo 299, do Código Penal:

> "Art. 299 – Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante:
>
> Pena – reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, se o documento é particular. (Código Penal Brasileiro, 1940, n.p). "

Assim como nos crimes de falsidade material, o computador somente é utilizado como meio para o cometimento do ilícito.

2.4.5.3 Falsidade Pessoal: A Falsa Identidade

A falsidade pessoal consiste na utilização de documento verdadeiro, com conteúdo verdadeiro por quem não pode, de fato, utilizá-lo, seja por não ser a pessoa ou por outros motivos. Aqui, o agente se faz passar pelo que não é, ou seja, mentido sobre sua identidade ou outra característica pessoal. Um exemplo clássico é a tentativa de fraudar o sistema de pontuação de delitos no trânsito na Carteira Nacional de Habilitação, transferindo os pontos do delito para outra pessoa.

Aquele que se utilizada da identidade de outrem ou mesmo uma fictícia, com o propósito de cometer atos ilícitos comete o crime de Falsidade Pessoal, previsto no art. 307 do Código Penal, abaixo:

> "Art. 307 – Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:
>
> Pena – detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave. (Código Penal Brasileiro, 1940, n.p). "

Por muitas razões, é importante observar a distinção que existe entre o falso material e o falso ideológico. Na falsidade material, o que se frauda é a própria forma do documento, que é alterada, no todo ou em parte, ou é forjada pelo agente, que cria um documento novo. Na falsidade ideológica, ao contrário, a forma do

documento é verdadeira, mas seu conteúdo é falso, isto é, a ideia ou a declaração que o documento contém não corresponde à verdade. (DELMANTO, 1991).

2.4.5.4 A criação de perfis falsos: o emaranhado entre os crimes de falsidade

Nos vários sites de relacionamento existentes hoje em dia, os usuários exibem suas fotos pessoais, expõem a sua biografia, manifestam preferências, falam da família, exibem seus amigos e associam-se a comunidades de temas que se identificam com o seu perfil. Porém, o perfil exibicionista do brasileiro vem causando diversos problemas durante a interatividade *online*. A incidência dos perfis falsos, também conhecidos como *fakes*, tem aumentado e por este motivo tem sido recorrente o uso não autorizado de imagens de terceiros, divulgando conteúdos que atacam a honra, expondo as pessoas ao ridículo, e, por estes motivos, em alguns casos, poderão ser punidos pela legislação brasileira.

Como a criação de contas nas redes sociais é bem rápida e simples, é normal que pessoas mal-intencionadas se utilizem disso para prejudicar pessoas físicas ou empresas.

Ao criarem contas utilizando nomes falsos, elas podem divulgar conteúdos mentirosos e gerar vários problemas. Imagine se um perfil falso divulga promoções e descontos que não estão sendo oferecidos por uma certa empresa, por exemplo?

A criação dos fakes, em regra, se manifesta de duas formas distintas. A primeira delas o internauta tem o intuito de buscar o anonimato para abordar terceiros se passando por uma pessoa fictícia, seja do mesmo sexo ou não. Esta prática resulta da escolha uma imagem de uma pessoa desconhecida (porém que previamente permitiu que sua imagem figurasse em determinado banco de dados destinado para esta finalidade) para atribuí-la ao seu perfil falso. Já existem sites

especializados na oferta de uma ampla seleção de fotos de terceiros de acordo com diferentes perfis para esta finalidade.

Ao contrário do que comumente é divulgado, esta prática não é crime, pois o internauta pode estar apenas infringindo alguma regra dos Termos de Serviço do site de relacionamento, que obriga o criador do perfil zelar pela integridade dos dados cadastrais. Se houver alguma denúncia de abuso, o infrator poderá ter o seu perfil excluído. Caso não existam meios para comprovar a incidência de danos à imagem do terceiro que teve sua foto utilizada, está descartada a possibilidade de indenização pela prática deste ato. Entretanto, se a pessoa que teve sua foto utilizada indevidamente, descobrir este fato e julgar que houve danos a sua imagem, terá legitimidade e meios para comprovar o alegado e obter uma indenização judicial.

Portanto, criar um perfil falso, de alguém que não existe, só para preservar sua identidade durante os relacionamentos na internet, sem que esta prática não tenha causado danos, não é crime, mas pode ensejar a quem pratica, sua remoção por infração as condições estipuladas para a prestação do serviço, e, eventualmente, suportar uma indenização se houver meios desta comprovação.

Entretanto, se o *fake* é criado a partir de uma pessoa real, viva ou morta, o responsável poderá cometer o crime de falsidade ideológica, desde que cause danos a vítima. O ato de incorporar a personalidade de outras pessoas e manifestar em nome de outrem, inserindo declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante é crime de falsidade ideológica.

Outra situação comum é a utilização de imagens de terceiros. O direito à imagem é um dos direitos da personalidade previsto pelo Código Civil (clique aqui). A utilização de uma foto de outra pessoa em seu perfil viola o direito de imagem já que só é permitido usar fotos se a pessoa fotografada fornecer autorização por escrito. Nossa Constituição Federal já prevê em seu artigo 5°, inciso X que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação, bem como é possível a livre manifestação do pensamento, desde que se faça sem a proteção do anonimato.

Então, é necessário ter cuidado ao usar a internet, sempre colocar informações que possibilitem a conferência da procedência. Uma estratégia é oferecer telefones para contato e colocar avisos nas suas páginas: “perfil oficial” ou “não realizamos promoções online” etc.

2.4.6 Plágio

Outro crime cometido com frequência e que pode trazer grandes dores de cabeça é o plágio: a cópia de informações veiculadas por terceiros sem a indicação da fonte.

O crime está previsto na Lei nº 9.610/1998, que dispõe sobre a proteção dos direitos autorais e aquele que o comete pode sofrer pena de detenção e ser obrigado ao pagamento de multa.

Para evitar problema nessa questão, precisamos tomar alguns cuidados, principalmente verificar todas as divulgações antes de publicar algo, e lembrar de colocar as referências de pesquisa, além de utilizar as normas adequadas para citações.

O crime, além de gerar penalidades graves, pode prejudicar o nome e a credibilidade de quem publica material de outrem.

2.4.7 *Revenge Porn*: A divulgação de fotos e vídeos íntimos de terceiros

Esse é um dos problemas mais recorrentes atualmente em nosso país.

Aqui no Brasil, inúmeros são os casos de divulgação de conteúdo sem autorização, e que ocorrem meio de invasão computacional. Um deles foi tão divulgado pela grande mídia que foi considerado o estopim da criação de uma Lei nacional de combate a este tipo de crime.

Pesquisas apontam que as mulheres são vítimas recorrentes de tal conduta. Segundo dados oficiais disponibilizados pela SAFERNET[6] Brasil, uma organização não governamental criada em 2007 e que ajuda a promover os Direitos Humanos na Internet, somente no ano de 2016[7], 300 pessoas tiveram suas fotos íntimas vazadas. Destas, 202 eram mulheres. Desde sua criação até 2016, mais de 3,8 milhões de denúncias sobre pornografia de vingança foram contabilizadas pelo órgão.

Apesar de serem dados verdadeiros e relevantes, esses números são construídos a partir do momento em que a ONG toma ciência do ocorrido. Entretanto, sabemos que por medo ou vergonha, muitas pessoas que sofrem com esse tipo de incidente não procuram ajuda, atitude que fazem desses números algo bastante superficial e impreciso.

Na maioria das situações, os casais trocam fotos íntimas – as tão faladas imagens popularmente conhecidas como “nude/ nudes” – ou seja, fotos sem vestimentas, por sentir segurança em seu parceiro, mas que ao término de relação, como forma de vingança ou de não aceitação, um deles acaba por divulgar o conteúdo através da internet, acarretando por vezes inúmeros danos (alguns até irreparáveis) à pessoa exposta.

Apesar de haver tipificação para tal conduta, como será abordado no próximo tópico, as punições não são suficientes para coibir os criminosos. Um indivíduo ao espalhar as fotos, comete o crime, porém quem sofre as maiores consequências é a pessoa exposta. É o que afirma Juliana Andrade Cunha[8], psicóloga e coordenadora do Canal de Ajuda da SAFERNET Brasil:

> "A violência contra as mulheres, especialmente na internet, não é levada muito a sério (...). Além das pessoas diretamente envolvidas

[6] A SAFERNET atua em cooperação com diversas instituições governamentais – como o Ministério Público Federal (MPF), a Polícia Federal (PF), a Câmara dos Deputados, o Senado Federal e a Secretaria de Direitos Humanos – e parceiros da iniciativa privada, além da entidade internacional INHOPE, uma rede de canais de denúncias de crimes na internet presente em quase 50 países.

[7] Dados disponibilizados em matéria da Revista Eletrônica HUFFPOST, disponível em: https://www.huffpostbrasil.com/safernet-brasil/mulheres-sao-as-maiores-vitimas-do-vazamento-de-fotos-intimas-na-internet_a_23300691/

[8] Juliana Andrade Cunha é Graduada em Psicologia (2002) pela Faculdade de Filosofia e Ciências Humanas da UFBA, Mestre em Cultura e Sociedade (2007) pela Faculdade de Comunicação da UFBA, psicanalista membro da Associação Científica Campo Psicanalítico. É professora de Psicologia da Universidade Salvador (UNIFACS) e tem experiência docente como professora substituta do Instituto de Psicologia da UFBA. Dedica-se ao ensino e pesquisa em Psicologia e Psicanálise e suas relações com os demais campos epistêmicos das ciências humanas, com ênfase em estudos multidisciplinares. Tem especial interesse por clínica psicanalítica, processos de subjetivação e cultura, Internet e sociabilidade.

> no episódio, devemos chamar a atenção para uma audiência que compartilha, curte, comenta e torna a violência um viral."

Apesar da culpa ser totalmente de quem divulga de forma sorrateira e vingativa as imagens íntimas, ou seja, de darem causa ao crime, não podemos deixar de lado a responsabilidade que cabe às redes sociais, por horas deveras coniventes, pois mesmo que de forma indireta, também possuem participação efetiva no cometimento deste tipo de ilícito, vez que são utilizadas como ferramentas para a disseminação desses conteúdos e as vezes não fazem nada para coibir tais práticas em suas plataformas e datacenters.

Sabendo disso, a Facebook Inc. desenvolveu um sistema dentro de uma de suas redes sociais a fim de coibir tais crimes, o que vem conseguindo diminuir a incidência em sua plataforma ao longo dos anos.

Vale salientar, ainda, que quem curte e compartilha tais materiais também acaba cometendo ilícito.

2.4.8 Crimes de Ódio: Racismo, Xenofobia e outras formas de preconceito

O não permitido, mas alcançável anonimato nas redes sociais da *surface web* tem aflorado o sentimento de impunidade na internet.

Arraigados nessa ideia, os crimes de ódio têm se tornado recorrentes nos últimos anos.

Os crimes de ódio são uma forma de violência que normalmente se iniciam por palavras, podendo chegar a forma física. São ofensas sempre direcionadas para um determinado grupo de pessoas que possuem algum tipo de características em comum e que incomodam o agressor. Essas ofensas nascem de uma apatia, na maioria das vezes baseada em ideias pré-conceituadas, pré-formadas, alimentadas das mais diversas formas, geralmente por desconhecimento da história de determinado grupo, por não gostar de uma determinada característica física ou pessoal, ou até por problemas pessoais.

De acordo com o Portal SAFERNET[9] Brasil, os crimes de ódio ocorrem com mais frequência por causa de cor (racismo), seguidos das por regionalidade (xenofobia, nativismo e etnocentrismo), preferências sexuais (homofobia e sexismo), preferências religiosas ou filosóficas (intolerância religiosa e/ou filosófica), classes sociais (preconceito social), e preconceitos velados (direcionados a quem possui, por exemplo, deficiência física ou determinados atributos não aceitos, como estar acima ou abaixo do peso, usar *piercing*, brincos, por ter determinados traços na aparência física, dentre outros).

Qualquer modalidade de preconceito que seja baseado na ideia de superioridade, seja ela por raça, aversão e discriminação que demonstram nítida ideia de segregação, de coação, de agressão, de intimidação, de difamação ou exposição de pessoa ou grupo, encontra-se qualificada na Lei, passível de punição.

A Declaração Universal dos Direitos Humanos assegurou a igualdade entre todos os indivíduos. Independente do grupo social ou do modo de ser e agir, todo ser humano tem o direito ao tratamento digno e imparcial.

Nossa Carta Magna também afirma em seu escopo que a promoção do bem-estar de todas as pessoas, sem discriminações é um dos objetivos principais do nosso país. A Constituição Federal Brasileira (1988) versa em seu Artigo 3º, inciso XLI, o seguinte:

> "Constituem objetivos fundamentais da República Federativa do Brasil: promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação"; e no Art. 5º, inciso XLI, que "a lei punirá qualquer discriminação atentatória dos direitos e liberdades fundamentais". (Constituição Federal Brasileira, 1988, n.p) "

O Código Penal brasileiro, por sua vez, assegura punição exemplar nos casos em que essa igualdade de tratamento não for aplicada e, assim sendo, ocorre discriminação.

A lei nº 7.716 de 5 de janeiro de 1989, em nova redação dada pela Lei nº 9.459, de 15 de maio de 1997, decreta em seu 1º artigo que:

[9] Artigo jornalístico escrito por Giovane Mangueira e Leonardo Fraga, sob supervisão da Professora Polyana Bittencourt Andrade, ao GELEDÉS – Instituto da Mulher Negra. Disponível no endereço https://www.geledes.org.br/web-registra-cerca-de-100-mil-casos-de-racismo-em-uma-decada/

> “Art. 1: Serão punidos, na forma desta Lei, os crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. (CRIME DE INCITAÇÃO AO PRECONCEITO - Lei nº 7.716, 1989, n.p). “

Há muitos tipos de Crime de ódio que não são englobados pela Lei nº 7.716, porém todo e qualquer tipo de delito de intolerância vai contra as leis. Se não uma lei específica, encontra amparo na Constituição.

2.4.9 Pedofilia e Pornografia Infantil

Este talvez seja um dos mais complicados crimes desse rol para se dissertar.

Crimes de abuso e exploração sexual contra crianças e adolescentes ocorrem de forma corriqueira mundo afora, e a internet é utilizada como ferramenta para o cometimento do ilícito.

Recentes levantamentos realizados pela SAFERNET Brasil apontam que a pornografia infantil foi o crime mais denunciado no ano de 2018. Dados da plataforma mostram que já houveram entre janeiro e dezembro aproximadamente 60 mil denúncias[10].

Segundo Márcia Bernini, Delegada da Delegacia Especializada de Atendimento à Mulher (DEAM) no município de Lajeado, estado do Rio Grande do Sul, em entrevista ao site Jornal Informativo, os registros ligados a esses tipos de crimes não ocorrem com frequência, pois geralmente os pais conseguem identificar antes da consumação. Ela informou que o (caso) mais comum é quando os adolescentes começam a conversar com pessoas não identificadas nas redes sociais e depois descobrem que elas querem apenas receber fotos íntimas, e não

[10] FONTE: https://www.destakjornal.com.br/brasil/politica/detalhe/pornografia-infantil-foi-o-crime-mais-denunciado-na-internet-em-2018-diz-pesquisa

uma amizade. “Normalmente os pais vêm e denunciam, e a gente tenta fazer a investigação de quem é o autor para apurar o fato"[11].

Conforme a delegada, são penalizadas as práticas de crime envolvendo crianças e adolescentes que vão caracterizar ou não o resultado da pena. "A pedofilia caracteriza uma questão da pessoa que tem desejo sexual envolvendo crianças e adolescentes. Tudo depende da pena do Estatuto da Criança e do Adolescente (ECA)".

Para atrair esse público, na maioria dos casos, os criminosos se passam pela mesma faixa etária das vítimas, utilizando fotos de crianças e adolescentes. Primeiro tentam ganhar a confiança delas, depois criam a barreira de blindagem da criança com a família, pedindo sigilo, alegando que se os pais dela descobrem, não conseguirão manter uma amizade ou relacionamento. Por fim, começam a enviar e solicitar material pornográfico, chegando alguns a até marcarem encontros.

As penas para quem comete tais crimes variam entre 1 e 8 anos de prisão, a depender do tipo ilícito caracterizado pelo seu envolvimento. Quem armazena material pornográfico com crianças e adolescentes nas cenas pode pegar de 1 a 4 anos de prisão. Para quem compartilha, a pena vai de 3 a 6 anos de prisão. Já para quem produz tal material, a punição aumenta para 4 a 8 anos de reclusão.

A Secretaria de Segurança Pública do estado do Rio Grande do Sul (SSP/RS) explicou por nota através de sua assessoria de imprensa que, com relação às ocorrências relacionadas ao crime de pedofilia, tem-se um sério problema de conceito na avaliação, tendo em vista que "a pedofilia é uma condição psicológica, ou seja, uma patologia, e não um tipo de fato criminal. ”

Estudos recentes atestam que em média 50% dos casos de abusos sexuais infantis não são praticados por pedófilos, entretanto, é praticamente impossível ainda determinar quais os casos em que o autor possui tal patologia ou não. Além disso, o simples distúrbio psicológico (orientação sexual com preferência etária) não constitui crime, ou seja, não há previsão legal no Código Penal Brasileiro.

O Ministério da Justiça, através da Secretaria de Operações Integradas do Ministério da Justiça e Segurança Pública, conjuntamente com autoridades policiais

[11] FONTE: https://www.informativo.com.br/geral/brasil-teve-60-mil-denuncias-de-pornografia-infantil-em-2018,295404.jhtml

dos estados brasileiros, deflagrou em meados de março deste ano a quarta fase da “Luz na Infância”, projeto cuja finalidade é apurar crimes de crimes de abuso sexual, exploração infantil pela internet. São investigados crimes de armazenamento, compartilhamento e produção de material pornográfico que contenham crianças e adolescentes.

2.4.10 *Cyberbullying* (intimidação sistemática praticada via internet) e C*yberstalking* (assédio via internet)

Outros dois relevantes crimes que vem ocorrendo com muito recorrência são os crimes de *Cyberbullying* e *Cyberstalking*. É cada vez maior o número de pessoas que sofrem com esses dois crimes, que, apesar de receberem nomes próprios para a identificação do delito, são práticas já tipificadas nos códigos penais da maioria dos países, inclusive no Brasil. Na Alemanha, por exemplo, país referência em legislação penal, comete o delito de *cyberstalking* quem "perseguir ilegalmente uma pessoa buscando sua proximidade" ou "tentando estabelecer contato" "por meio de telecomunicação ou outros meios de comunicação ou através de terceiros" (SEÇÃO 238 DO CÓDIGO PENAL ALEMÃO, 1871).

O *Cyberstalking* é um termo em inglês usado para descrever a conduta de quem ilegalmente persegue ou assedia virtualmente alguém de forma muito contumaz.

No Brasil, porém, ainda não há a figura deste crime específico. Tramita no Senado Federal o Projeto de Lei nº 236/2012, que visa a reforma do Código Penal, cujo escopo de seus artigos traz a seguinte redação: "perseguição obsessiva ou insidiosa", realizada por quem, "de forma reiterada ou continuada, ameaça à integridade física ou psicológica" da vítima, "restringindo-lhe a capacidade de locomoção ou, de qualquer outra forma, invadindo ou perturbando sua esfera de liberdade ou privacidade", é punida com prisão de dois a seis anos. Entretanto, este projeto de Lei encontra-se, ainda, em fase de discussão no Legislativo brasileiro.

Porém, a atual ausência de tipificação clara e nítida da perseguição virtual e do assédio persistente em nosso defasado e tão remendado Código Penal atual não significa, contudo, que tais ilícitos fiquem impunes por falta de previsão legal.

Casos de menor gravidade podem ser enquadrados como “perturbação à tranquilidade”, prevista no artigo 65 do Decreto-Lei Nº 3.688, de 3 de outubro de 1941 (Lei de Contravenções Penais), cuja competência para julgamento é do JECRIM - Juizado Especial Criminal.

Os casos de maior proporção, em que constatada fundamentadamente ameaça, seja ela "por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar" à vítima "mal injusto e grave", o autor poderá responder ao delito previsto pelo artigo 147 do Código Penal.

Em casos de maior complexidade e perigo, tal comportamento pode levar no cometimento do crime de lesão corporal, igualmente já previsto no artigo 129 do Código Penal Brasileiro, apois pratica tal delito quem, de qualquer forma, atente contra a sua integridade física, incluindo a saúde mental.

O mesmo ocorre com a prática de *Cyberbullying,* um tipo de violência moral virtual, cuja ação visa hostilizar pessoa ou grupos delas neste espaço, a fim de intimidá-la. A prática é bastante comum no meio físico em escolas, ocorrendo entre crianças e adolescentes, e geralmente são alimentadas pelo preconceito "*cyberbullie*" – termo utilizado para rotular quem comete tal prática. Hoje, com o advento das redes sociais e a popularização da internet, tem ocorrido com mais frequência, vez que o anonimato, a impunidade e a desinformação servem como álibis ideais para seu cometimento.

Apesar de ocorrer num ambiente diverso do meio físico e não consistir em agressões físicas visíveis, é muito comum não ser levada a sério como se deve. Entretanto, o *cyberbullying* pode chegar a proporções inimagináveis, sendo tão cruel e violento quanto, podendo gerar sérios danos em mentes e personalidades em formação.

Apesar de não existir uma lei específica para tal feito, os crimes contra a honra (calúnia, injúria e difamação) conseguem abarcar tais práticas nocivas de forma muito objetiva. Apesar disso, também já consta no Projeto de Lei nº 236/2012 (reforma do Código Penal) redação específica para tais atos.

CAPÍTULO III

3. LEGISLAÇÃO NO BRASIL

3.1 O QUE DIZ A CONSTITUIÇÃO FEDERAL DO BRASIL (1988) E O CÓDIGO PENAL BRASILEIRO (1940)

A Constituição Federal assevera em seu escopo que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas”, e ainda assegura possível indenização em caso de comprovado dano material ou moral. Nossa Carta Magna ainda garante o sigilo das comunicações, que, apenas por determinação judicial e de acordo com a referida lei que a regulamenta pode ser violada. Entretanto, com o avanço da tecnologia e o fácil acesso à internet, a sociedade em geral está cada vez mais suscetível a sofrer com os crimes virtuais.

É extremamente importante ressaltar que o direito à informação é um tipo de direito que se encontra previsto no *caput* do artigo 5º e em alguns de seus incisos, conforme se destaca abaixo:

> “Art. 5 – Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

> IV – É livre a manifestação de pensamento, sendo vedado o anonimato;
>
> V – é assegurado o direito de resposta, proporcional ao agravo, além de indenização por dano material, moral ou à imagem;
>
> IX – É livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
>
> XIV – é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício ao exercício profissional;
>
> XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade de do Estado;
>
> LXXII – conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constante de registros ou banco de dados de entidades governamentais ou de caráter público; b) para retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; (Constituição Federal do Brasil, 1988, n.p). “

De acordo com o trecho acima, nossa Constituição apresenta algumas importantes garantias à sociedade, onde todas elas estão ligadas de alguma forma à liberdade informática, referindo-se ao direito de cada cidadão utilizar-se dos instrumentos disponíveis e necessários para informar e obter informações.

Segundo o artigo 220 da Constituição Federal, a expressão do pensamento, a criação e a informação sob qualquer forma, processo ou veículo não sofrerão qualquer restrição (BRASIL, 1988).

Entende-se ainda que não cabe à Constituição Federal, mas sim ao Direito Penal estruturar os mecanismos que forem necessários a fim de prevenir e punir de forma efetiva e dentro de seu próprio rigor - mediante o respaldo dos ditames constitucionais - a manifestação do comportamento lesivo dos bens e valores jurídicos.

Muitas vezes tem-se pensado que a regulamentação específica não tem favorecido o mundo virtual, porém a legislação tem avançado, sempre arraigado nos ideais contidos na Constituição Federal, possibilitando, portanto, a promoção e a resolução de vários crimes virtuais.

Assim, conforme, o desenvolvimento da técnica, a transformação das condições econômicas e sociais, a ampliação dos conhecimentos e a intensificação dos meios de comunicação poderiam produzir mudanças na organização da vida

humana e das relações sociais, criando condições favoráveis para o nascimento de novos carecimentos (BOBBIO, 1992).

Cabe lembrar que a efetiva limitação ao poder punitivo estatal conforme o princípio da legalidade ou da reserva legal é uma vertente penal do princípio da intervenção mínima (BITTENCOURT, 2006)

Outro fato importante é o princípio constitucional do Direito Penal, isto é, o princípio da anterioridade da Lei penal, enunciado no artigo 5°, XXXIX da Constituição Federal e no artigo 1° do Código Penal. Nesse sentido, em caso de crime, primeiro se faz necessário que o fato tenha sido praticado em momento posterior à criação da norma incriminadora (MONTEIRO NETO, 2008).

É certo e inconteste que vivemos em meio à tecnologia e que essa mesma tecnologia trouxe também os crimes virtuais e novos bens jurídicos, ao qual a ordem constitucional precisa proteger. Sendo assim, é notório o impacto na sociedade da informação no que diz respeito à ordem constitucional, gerando consequências na esfera penal.

Acredita-se que os crimes virtuais e a legislação vigente remetem à discussão das condutas ilícitas, evidenciadas no ambiente virtual, tendo em vista que causam algum tipo de dano à pessoa ou empresas, prejudicando a segurança e credibilidade, interferindo na rotina e no dia a dia de muitas pessoas. Desse modo, o ambiente virtual vem se tornando um lugar de cuidados e atenção para que se mantenham relações sociais seguras.

Salienta-se aqui ainda, algumas considerações sobre as leis ordinárias 12.735/2012 e 12.737/2012, no sentido de entender-se a expansão dessa tecnologia e a importância da criação de legislação especifica voltada a coibir os atos ilícitos praticados nesse ambiente virtual. Sendo assim, a legislação é necessária bem como a atualização da norma penal para que os crimes virtuais não fujam do controle.

Dessa forma, a Lei 12.735 de 30 de novembro de 2012, possui a seguinte ementa: "Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de

sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências" (BRASIL, 2012).

Percebe-se que, a criação dessa norma teve como principal objetivo atender as questões referentes à impossibilidade da proteção aos bens da vida, uma vez violados através dos crimes virtuais (OLIVEIRA, 2013).

Contudo, a Lei 12.737 de 30 de novembro de 2012 traz o argumento da mesma ideia da Lei 12.735, ou seja, a legislação penal existente é suficiente para combater os crimes virtuais e destaca em sua ementa o seguinte: "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" (BRASIL, 2012).

Assim, as duas leis aqui destacadas têm como objetivo inicial preencher as lacunas deixadas na lei que impedia a tipificação de atos ilícitos praticados pelos meios digitais.

Os crimes virtuais classificados como “*cybercrimes* próprios” já vem alcançando uma média de 90% de punição; assim, podemos dizer que quase todos os delitos reconhecidos nesta modalidade já se encontram dentro dessa porcentagem, e, portanto, tipificados e abarcados pelo/no Código Penal.

Apesar de não existirem estatísticas oficiais específicas sobre a incidência de crimes cibernéticos no Brasil, incidentes de segurança são reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil que apresentam denúncias sobre violações. Segundo informações do órgão, em 1999 foram reportados 3.107 incidentes. Em 2006 um total de 197.892 e do início de 2011 até o mês de setembro de 2017 já teriam sido reportados 318.720 incidentes.

Estatisticamente destaca-se os dados acima informados pelo Centro de Estudos, Respostas e tratamento de Segurança (CERT BR) que, de 2013 para 2014, o número de notificados de cyberataques reportadas a entidade aumentou em 197% de 352.925 incidentes para 1.047.031, a maioria absoluta 44% composta de tentativa de fraudes.

Cabe lembrar que o Código Penal, de acordo com sua previsão legal, expõe uma lista de crimes que visa contribuir para a punição exemplar dos que cometem delitos através da internet.

3.2 Marco Civil da Internet

Em abril de 2014, foi promulgado no Brasil a Lei nº 12.965, a materialização da incorporação de outros 37 projetos similares, que ficou popularmente conhecida como Marco Civil da Internet. Ele é uma espécie de código, de constituição da internet nacional. Seu principal objetivo é reger a utilização da internet no país. Ele define os direitos e deveres, tanto dos usuários quanto daqueles que a proveem.

O texto do Marco Civil prevê basicamente a proteção da liberdade de expressão, a privacidade e a neutralidade da rede como princípios básicos da internet. Outro ponto importante em seu escopo é que ele deixa de forma extremamente clara quais as responsabilidades de cada um no ambiente online, protegendo, assim, portanto, a todos que navegam.

O Marco Civil da Internet foi desenvolvido com direta participação popular, através de audiências públicas, que ocorreram por todo o país. Ele também recebeu apoio e sugestões de várias redes sociais, como o Twitter, Facebook e o portal e-Democracia da Câmara dos Deputados.

A referida Lei se fez necessária, diante da quantidade exacerbada de crimes cometidos no/e através dos meios digitais, arraigados na falta de uma legislação efetivamente eficaz e específica em terras tupiniquins.

Além de seu objetivo principal, traz de forma intrínseca e secundária o objetivo de contribuir afim de que haja punição para todos aqueles que cometam abusos através da internet, classificando-os de acordo com a especificidade do dolo cometido, apesar de não trazer em seu escopo penalidades para a imensidão de crimes possíveis.

Ainda em relação a esta lei que se propõe a punir - ao mesmo tempo em que busca regulamentar as questões referentes aos abusos cometidos via internet - é fundamental analisarmos que ela não passa de uma ferramenta oriunda da justiça e do poder legislativo nacional, que, com ela, mostram à sociedade que o assunto não passa despercebido. Ambos os poderes vêm investido significativamente, afim de garantir a segurança dos indivíduos que de alguma forma forem vítimas de crimes virtuais. Ela mostra que o judiciário e o poder legislativo podem e devem ver

relevância no tema, e agirem em conformidade com os anseios da sociedade frente ao *boom* tecnológico.

Com o advento da Lei nº 12.965/2014, uma lacuna fica levemente preenchida, no que tange em garantir respeito e privacidade aos usuários da internet, independente dos benefícios e facilidades que a mesma possa proporcionar à sociedade. Afinal, o mundo virtual é de suma importância em virtude de que as ferramentas nela contidas podem facilitar o cotidiano de muitas pessoas que utilizam os serviços contidos e disponibilizados pela internet.

Dentre todos os seus 32 artigos, um ponto bastante importante discutido em seu corpo é o da privacidade na rede. Nesse contexto, o Marco Civil da Internet busca mediante os diversos dispositivos assegurar a inviolabilidade e o sigilo das comunicações, entrando claramente em conformidade com o que determina a Constituição Federal Brasileira, em seu artigo 5º, inciso X, senão vejamos, *in verbis*:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> (...)
>
> X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (Constituição Federal do Brasil, 1988, n.p). “

Outro aspecto que merece destaque é a atenção direcionada a liberdade de expressão. Conforme os dispositivos da Lei, percebe-se a relevância dada a esse importante tópico. A liberdade de expressão é uma garantia constitucional fundamental, e indubitavelmente encontra apoio no Marco Civil. Como prova inconteste disso, podemos evidenciar os artigos 2º e 3º da Lei nº 12.965/2014, que claramente proporciona-nos a qualidade do direito à liberdade de expressão; liberdade esta que deve ser limitada, mas sem prejudicar o direito alheio, devendo ser observado a proporcionalidade e a ponderação.

A liberdade de expressão é assegurada como um dos princípios do Marco Civil, afirmada em seu artigo 3º, onde este também atesta que a disciplina do uso da internet no Brasil possui, além deste, outros princípios:

> “I - Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II - Proteção da privacidade;
>
> III - proteção dos dados pessoais, na forma da lei;
>
> IV - preservação e garantia da neutralidade de rede;
>
> V - Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
>
> VI - Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
>
> VII - preservação da natureza participativa da rede;
>
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. (Marco Civil da Internet, 2014). “

Outro ponto deveras relevante na Lei 12.965/2014 é a atenção dada ao monitoramento, armazenamento e disponibilização de dados dos usuários, que somente podem ser feitos caso o provedor receba ordem judicial com esta instrução. Ainda, a exclusão dos dados dos usuários deve ser garantida àqueles que decidirem apagar seus dados após o término de relação entre as partes.

Outra importante mudança trazida pelo Marco Civil da Internet refere-se ao tempo de armazenamento dos dados, que passou a ser de no máximo um ano, ao invés de 2 anos, como no passado.

Já o 7º artigo, *caput*, do Marco Civil da Internet visa garantir, com seu escopo, a inviolabilidade da intimidade e vida privada de quem utiliza os serviços da internet, ao mesmo tempo em que salvaguarda a liberdade de expressão, elencada no artigo 5º, IV, da Constituição Federal do Brasil, de 1988.

Entende-se que o advento da legislação do Marco Civil da Internet trouxe como papel essencial ao Direito e à justiça acompanhar o desenvolvimento social e tecnológico da sociedade, tomando ciência de que a internet no Brasil não começou a ser utilizada nos anos 2000, mas sim em meados da década de 1980/1990. Sendo assim, a sua regulamentação desde 2014 ainda está descompassada com a realidade frente à necessária regulamentação. A presente normatização vem garantir o dever de amparar os cidadãos na sociedade informacional, mesmo que de forma muito embrionária e por vezes nada efetiva. O surgimento da regulamentação

da internet é de suma importância, em virtude do avanço da comunicação e da rapidez do acesso às mesmas, via internet, que tem facilitado cada vez mais o acesso as informações como um todo.

No que se refere ao processo legislativo de tramitação e aprovação da Lei do Marco Civil, este pode ser considerado eficiente, justamente por contar com o auxílio da população para sua efetivação.

Percebe-se que, na atualidade, a sociedade está progressivamente mais dinâmica e informacional, e a rapidez da informação sobre os acontecimentos torna-se global devido a uma gama ampla de facilidades em relação ao acesso à internet, e consequentemente a efetiva prática de compartilhamento. Esta acessibilidade é positiva para o crescimento da população e traz o acesso a novos conhecimentos que também pode ser bastante prejudicial.

Dentro dessa linha de pensamento considera-se o abuso ao conteúdo dos compartilhamentos e a liberdade de expressão e respeito da vida privada, o que caberá a todos os aplicadores do Direito, tanto magistrados, promotores como advogados, a observarem os dispositivos legais do Marco Civil e a Lei de Proteção aos dados pessoais em conjunto com a Constituição Federal, para uma justa aplicação, não podendo deixar de lembrar a importância dos princípios da proporcionalidade.

Apesar do Marco Civil da Internet ser considerado um importante passo rumo a uma legislação mais efetiva, em algo mais coeso, cujo objetivo seja proteger de forma mais consistente direitos e deveres dos usuários da rede, é necessário compreender que mudanças substanciais somente ocorrerão se esta apresentasse condições eficazes para punir de fato e de direito os criminosos.

E por falar nisso, dentro dessa perspectiva podemos dizer que as normas contidas na Constituição Federal Brasileira, Código Civil, Código Penal, Códigos de Processo Civil e Penal, Código de Defesa do Consumidor, Estatuto da Criança e do Adolescente e na Lei nº 9.296/96 (Lei de interceptação de comunicações) não possuem aplicação clara nas relações jurídicas estabelecidas na internet. Um dos pontos que a tornam nada eficazes é sua correlação com leis e tratados internacionais, além da incongruência com as legislações dos outros países.

Este aspecto do Marco Civil da Internet impressiona pela ingenuidade do legislador brasileiro de manter a pretensão de solução de problema de escala mundial, com efeitos extraterritoriais, por meio de uma lei nacional. Sabe-se que, a própria conjuntura da rede de comunicações e informações pela internet possibilita a ocorrência das transgressões de direitos das pessoas com evidência em qualquer parte do mundo, perpassando o âmbito da jurisdição brasileira.

O que aparece como uma dificuldade ao se afirmar, no artigo 2º, I, do Marco Civil da Internet, diz que um dos fundamentos da disciplina do uso da internet é o "reconhecimento da escala mundial da rede". Entende-se como uma possibilidade de impedir o crescimento das violações, principalmente quanto a privacidade por meio da obtenção dos dados, ou armazenamento e tratamento desses registros ou comunicações. Na realidade, o artigo11, *caput*, §§1º e 2º, estabeleceu pelo Marco Civil da Internet a aplicabilidade da lei quando, pelo menos, um dos atos forem realizados no Brasil ou quando um dos terminais utilizados para o cometimento do delito estiver em terras brasileiras; estas vítimas jurídicas com sede no exterior podem sujeitar-se à lei brasileira quando estiver um integrante do mesmo grupo empresarial no Brasil.

A respeito deste ponto, a violação pode não acontecer no Brasil, mas poderá acontecer a transmissão dos dados no exterior. Assim, cabe a previsão das sanções contidas no artigo 12 do Marco Civil da Internet, dentre as quais consta advertência e multa de 10% do faturamento dessa empresa; suspensão temporária das atividades ou proibição do exercício pelo das atividades econômicas.

Entretanto, apesar dessa atitude ser válida e muito útil, é inconstitucional nos termos do art.170 da Constituição Federal, pois o Brasil não tem jurisdição para controlar as atividades dessas grandes empresas em suas sedes no exterior.

Lamentavelmente devido a todas essas dificuldades, especificamente em relação ao gerenciamento de uma rede mundial de computadores, questiona-se a falta da exigência de instalação dos *datacenters* para fins de provisão e aplicações de internet no Brasil, nos termos do art.24, VII, haja vista que a informação virtual não é física e não adianta armazenar no Brasil, se a mesma pode ser reproduzida infinitamente para qualquer parte do mundo. Não é impossível que, através dos envios de um e-mail para uma máquina, os dados circulem livremente em países devido o próprio tráfego da rede.

A proposta de nacionalização de *datacenters* comprova a falta de conhecimento sobre o funcionamento da internet, pois esta não se limita a um ambiente físico de determinado território, sem qualquer conexão com a estrutura física de internet dos demais países.

É notório que os aspectos positivos trazidos pelo Marco Civil da Internet deixam a desejar, porém, o primeiro passo foi dado. O foco agora deveria ser garantir a segurança, a vedação da imposição de mecanismos de censura, bloqueio, monitoramento, filtragem e análise de dados que trafegam pela infraestrutura da internet dentro do território brasileiro, conforme previsto no art.9°, §3º.

Entretanto, a discussão de tal medida traz à tona uma outra preocupação: o medo de implantarem-se no Brasil mecanismos de controle estatal por meio de *firewalls*. O que nos chama atenção como ponto positivo desta atitude é a consistência na regulamentação dos procedimentos judiciais específicos, justamente para a obtenção dos registros de navegação para fins de instrução processual civil e penal. E só.

Inicialmente, o Marco Civil da Internet não tratava da interceptação de dados transmitidos via internet ou o acesso das informações por terceiros, nem sobre a questão da ilegalidade dessas práticas, limitando-se ao que está armazenado nos servidores esquecendo-se do que está movimentando-se entre eles.

Outro ponto positivo se refere à disciplina dos chamados *cookies*, arquivos, instalados nos computadores ou *smartphones* com a finalidade de registrar informações e preferências dos usuários quando acessam determinada página na internet. Este ponto encontra-se regulamentado na Lei 12.965/2014, conforme o art.7°, VIII. No projeto inicial essas normas também não estavam presentes.

Nesse contexto, as páginas de internet terão que informar logo no primeiro acesso do usuário que pretendem coletar tais informações. As situações preocupantes e reais que surgem a cada dia nos alerta para a questão da falta de privacidade, já que as empresas com acesso à internet conhecem quase tudo o que determinada pessoa costuma acessar, significando um alerta também para as autoridades.

Enfim, apesar disso, seria importante a obrigação de concordância referente a coleta desses dados, conforme é exigido em páginas da internet de outros países, a exemplo no continente europeu.

Por fim, é importante o reconhecimento no art.7º, VII, da proibição de fornecimento a terceiros dos dados pessoais, e outras informações se necessário e conveniente que seja mediante o consentimento livre e expressamente acordado com as prescrições previstas em lei.

3.3 Lei Carolina Dieckmann

Um caso de grande repercussão nacional foi o da atriz Carolina Dieckman, que sofreu um ataque em seu equipamento eletrônico interligado à internet, onde invasores subtraíram de seu computador pastas de conteúdo pessoal, onde uma delas continham fotos íntimas pessoais, que foram posteriormente publicadas em redes sociais. Esse fato deu origem a uma considerável mudança no Código Penal Brasileiro.

O caso foi tão discutido na grande mídia e judicialmente que a atriz, assim como Maria da Penha, cedeu seu nome para uma Lei. Neste caso em comento, a Lei nº 12.737/2012 foi batizada com seu nome, e trouxe relevantes alterações ao nosso Código Penal, ordenando acerca da tipificação criminal de crimes informáticos. Foi o embrião do que posteriormente tornar-se-ia o Marco Civil da Internet.

Além de criminalizar a invasão de sistemas informáticos de outrem e a subtração de arquivos pessoais, a lei também visou estabelecer pena de até um ano de prisão para quem produzir ou oferecer tais materiais conseguidos através de invasão cybernética para a venda, com objetivo de causar algum dano.

Entretanto, a “Lei Carolina Dieckmann” só abarca a invasão de computadores que possuam algum tipo de proteção. Para caracterizar a invasão, e assim o criminoso poder ser enquadrado na Lei, a invasão de algum material de cunho informático/tecnológico alheio precisa sofrer direta violação indevida de algum mecanismo de segurança, ou seja, o usuário precisa possuir em seu computador pelo menos um mecanismo de segurança que possibilite provar a violação, ou seja, é preciso ultrapassar um mecanismo de segurança. O texto não define exatamente qual seria, mas basta o instrumento apenas possuir uma senha e esta ser quebrada, descoberta, violada, ultrapassada sem o consentimento do proprietário que já se pode caracterizar uma quebra da segurança, e, por conseguinte, o enquadramento na Lei.

A “Lei Carolina Dieckmann” foi considerada positiva, justamente por fortalecer e determinar a punição aos invasores dos sistemas, tais como redes, sites e celulares, onde passou-se a ser considerado crime.

Cabe ainda dizer que a Lei foi promulgada com o objetivo de adequar o direito às mudanças tecnológicas que se transformam continuamente na sociedade *(ubi societas, ibi jus,* ou, em português: “Onde existe o homem, há sociedade; onde existe sociedade, há Direito”*)*. Para basificar essa afirmação, utilizo trecho dela mesma, onde alega que nela “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”. A Lei Carolina Dieckman visava suprir um extremo vazio legislativo que ocorria sobre os crimes cybernéticos, prevendo dentro do próprio ordenamento jurídico, especificamente na norma da Lei as penas de atipicidade da conduta.

Entretanto, um ponto de grande questão trazida com a Lei nº 12.737/2012 foi a alteração no artigo 154-A do Código Penal, que remete a liberdade, a intimidade dos cidadãos, bem como a privacidade de forma geral.

Após 21 anos de sucessivos governos militares, qualquer tentativa de controle da informação soa para a sociedade brasileira como censura, uma clara e grave ameaça à liberdade de expressão. A junção das três legislações - Marco Regulatório da Comunicação no Brasil, o Marco Civil da Internet, juntamente com a Lei Carolina Dieckmann - tornaram-se instrumentos recentes de debates políticos totalmente

relacionados com o controle de comunicação no país e reacenderam esse medo. O primeiro ainda se mantém como discussão. Os outros dois já são realidade.

Apesar disso, o Marco Regulatório traz à discussão que mexer nos meios de comunicação (que atualmente se concentra em um número reduzido de pessoas) é uma tentativa de democratizar a comunicação, mas não é somente esse ponto o discutido. Existem pontos obscuros levantados pelos contrários, e um deles é justamente quanto ao controle dos mecanismos, que levariam à falta de privacidade dos usuários.

Entretanto, ficam reconhecidos a Lei Carolina Dieckmann e o Marco Civil da Internet são os primeiros documentos da legislação brasileira direcionados a julgar casos relacionados à violação dos direitos no ambiente digital, são as primeiras ferramentas regentes do uso da comunicação propiciada pela internet.

Entretanto, apesar de existirem esses dois mecanismos, que são totalmente ineficientes em alguns pontos, entendo que é imprescindível discutir a segurança digital na esfera política, tendo como fundamento o respeito aos Direitos Humanos, uma vez que alguns cidadãos precisam inevitavelmente repensar sobre como estão se utilizando da internet.

No mesmo momento em que as mídias atuais podem ser instrumento necessário para o ativismo mundial e a ascensão de uma cultura de direitos humanos, podem prontamente serem utilizados para ferir esses direitos. (RADDATZ, 2014).

CONCLUSÃO

A utilização do ambiente virtual e da tecnologia pelos cybercriminosos a fim de cometer ilícitos e lesar a sociedade está incluída na modalidade dos crimes virtuais, seja como meio para a realização do ato criminoso, seja como método, isto é, como ferramenta para sua consumação.

Em face do desenvolvimento, estudo e pesquisa na área computacional no mundo todo, novas tecnologias têm surgido, proporcionando à sociedade uma série de benefícios e comodidades.

Entretanto, esse mesmo desenvolvimento proporciona a evolução e o aprimoramento de ferramentas que auxiliam ainda mais os piratas cybernéticos em cometer crimes no meio virtual. O dinamismo da tecnologia também aumenta as dificuldades encontradas para a resolução de tais crimes e poder punir com rapidez e severidade os que se utilizam desse progresso para o mal.

Se não bastasse, esse mesmo dinamismo ajuda no surgimento de novas modalidades de crime, exigindo das autoridades judiciárias, policiais e do poder legislativo maior e melhor efetividade.

Mas como acompanhar tamanha transformação, vez que não conseguimos nos livrar das amarras políticas e burocráticas que nos prendem e nos atrasam? Como punir aquilo que não se consegue tipificar de forma objetiva? Como legislar sobre aquilo que não conhecemos e nem dominamos? Como atuar de forma sistemática sobre algo que se comporta de forma totalmente ametódica? Como ocorre em outros países o combate a tais delitos?

A União Europeia, por exemplo, declarou guerra contra os crimes virtuais. Esse ato se tornou um marco na busca por leis mais eficientes e efetivas naquele continente. Encabeçadas por Portugal, Espanha, Alemanha, França, Holanda, e financiadas pela EUROPOL, criaram o “Centro Europeu para o Combate a Crimes Cibernéticos”, um centro integrado, sediado neste último, cuja função principal é combater fraudes em transações financeiras *online* e pegar casos de pornografia infantil, além de combater crimes contra a honra, preconceitos e outros crimes cometidos virtualmente.

Além disso, o centro mantém um setor de treinamento de pessoal, onde pesquisadores, investigadores e promotores públicos dos 27 países membros da União Europeia – e mais Estados Unidos, Canadá e Austrália, que também podem se beneficiar das instalações – se utilizam dessa estrutura para obter conhecimentos técnicos. As informações são compartilhadas. Por isso, esses países já mostram uma legislação muito mais efetiva que a nossa, pois há investimento, atualização e reciclagem, se mostrando ainda mais eficazes e efetivas que a Convenção de Budapeste, por exemplo, um tratado internacional de direito penal e direito processual penal, firmado no âmbito do Conselho da Europa para definir de forma harmônica os crimes praticados por meio da Internet e as formas de persecução, tratando basicamente de violações de direito autoral, fraudes relacionadas a computador, pornografia infantil e violações de segurança de redes, mas que possui a cooperação completa de apenas 15 nações. O Brasil não é signatário.

Entretanto, mesmo em meio a tantas dificuldades, sobretudo a escassez de investimentos e a falta da devida relevância ao tema em nosso país, a legislação brasileira vem buscando, através das Leis, garantir a punição desses crimes. Os legisladores têm se empenhado em garantir o cumprimento da lei segundo os rigores da justiça, acompanhando os avanços do crime digital e atualizando o ordenamento jurídico para tipificar as condutas e adaptar o crime praticado no ambiente virtual, já tão presente no cotidiano dos cidadãos brasileiros.

Mas ainda é pouco. E de forma lenta. Como vimos, tramita desde 2012 no Senado Federal o Projeto de Lei nº 236/2012, que visa a reforma do Código Penal. E não sai disso. As vezes aparenta não ser importante para a classe legislativa votar pautas deveras relevante e que poderia oportunizar de forma contundente a punição pra determinados crimes.

Enquanto isso, nos seguramos sob um Código Penal de 1940, um Código de Processo Penal de 1941, construídos numa época em que os anseios e os problemas da sociedade eram outros, e que se mostram cada dia mais ineficazes em alguns aspectos, sobretudo quando se fala da questão tecnológica, apesar de ainda conseguir abarcar alguns dos crimes mistos, comuns, impróprios e impuros já efetivamente conhecidos do meio físico.

Nossa Constituição Federal faz sombra, frente a alguns aspectos essenciais quando nenhuma outra regulamentação legislativa consegue atingir sua efetividade

quanto ao meio virtual. Garantias constitucionais como a igualdade perante as leis, a livre manifestação do pensamento, o direito de resposta, a expressão da atividade intelectual, artística, científica e de comunicação, a asseguração para todos do acesso à informação, a inviolabilidade da intimidade, da vida privada, da honra e a imagem das pessoas, além, claro, da ampla liberdade de expressão são premissas efetivas e servem de aporte na maioria dos casos.

Outros crimes virtuais existentes e não abarcados por nossa Constituição Federal e Código Penal encontram-se tipificados de acordo com legislação especifica surgidas posteriormente, como é o caso do Marco Civil da Internet e da Lei Carolina Dieckmman, que, apesar de terem, cada uma a seu modo, estabelecido princípios e garantias dos direitos e deveres para o uso da internet, dando embasamento para o judiciário ter o poder de punir de forma especifica os autores de crimes virtuais, não conseguem atingir por completo a gama de novos atos nocivos que surgem diariamente, deixando esses novos delitos à mercê da impunidade.

Aliás, por falar em impunidade, percebe-se claramente que a mesma é o combustível que alimenta a prática de condutas ilícitas. A falta de tipificação - em razão da complexidade do tema e da necessidade de medidas a serem tomadas – estimulam a prática delituosa no meio virtual.

Outro ponto estritamente relevante é quanto ao anonimato proporcionado com o uso da internet, permitido, sobretudo nas redes sociais. Nossa Constituição Federal veta o anonimato, entretanto, não raros são os casos em que pessoas inescrupulosas se utilizam dessa permissão dada pelas plataformas para que qualquer um, munido de má fé e péssimas intenções se vista de uma carcaça virtual que não é sua e cometa crimes no âmbito cibernético.

Posto isto, podemos afirmar que o trabalho foi de grande relevância para minha formação acadêmica, por me oportunizar conhecer algumas fragilidades da legislação voltada para os crimes virtuais, que, consequentemente, abarcam as redes sociais, além de me trazer alto grau de conhecimento quanto a dinâmica do crime virtual, que prejudica o mundo real de inúmeras formas, geralmente através do roubo de dados e informações pessoais, se utilizando de arquivos nocivos, infectados, pré-programados para tal ação, e que são utilizados para a prática criminosa.

Outro ponto que merece atenção é a questão da segurança. A melhor prevenção quanto aos crimes informáticos é o investimento em segurança, que se inicia ao aprendermos a usar o meio de forma mais consciente. Ao evitar que suas senhas sejam compartilhadas com outras pessoas, e se evita expor dados sigilosos, sobretudo pessoais, significa que a segurança começou. E o usuário conscientemente utiliza-se dos meios de comunicação, evitando negligenciar as regras básicas de proteção.

Ademais, este trabalho proporcionou a compreensão de que a garantia da segurança e proteção dos danos via digital só poderá ser consolidada mediante um cuidado contínuo, em virtude do avanço da tecnologia e da dinâmica dos *hackers* e *crackers* e de suas ferramentas, que se atualizam constantemente e não podem nos fazer parar no tempo. É através da falta de atualização e de informação que estes piratas conseguem realizar seus crimes, desde o roubo de senhas de redes sociais, *e-mail*, sequestro de *smartphones*, até a invasão de sua casa, lojas, apartamentos, ao conseguirem e terem acesso a imagens de câmeras de segurança, por exemplo.

Enfim, é possível dizer que a temática em questão nos levará a aprofundar os conhecimentos sobre o problema do crime via internet por ser uma questão também de segurança nacional, que merece punição eficaz para os criminosos que atuam no ambiente virtual ilicitamente. Além disso, é uma temática que não se esgota a necessidade para as discussões na sociedade.

Percebe-se que o meio de comunicação como a Internet deveria estar a serviço da educação e informação além da aquisição de novos conhecimentos, bem como a conduta desta nova modalidade criminal que tem acarretado danos aos cidadãos e a sociedade. Entende-se que o combate ao cybercrime se faz necessário, pois tem contribuído para a reflexão sobre a segurança pessoal e empresarial, tanto nacional como internacional, visto que, tais meios poderiam levar a sociedade a maior segurança.

Dessa forma, é de suma importância a regulamentação das condutas e análise de provas, inclusive a validação para identificar a autoria do delito. Fato é que, a legislação existente ainda necessita ser agregada a adequação dos crimes praticados por meio da internet, o que demonstra a necessidade da tipificação de determinadas condutas e a reflexão desta necessidade no universo jurídico.

REFERÊNCIAS

ABOSO, Gustavo Eduardo; ZAPATA, María Florencia. **Cibercriminalidad y derecho penal**. Buenos Aires: B de F, 2006.

ALMEIDA, Jéssica de Jesus. et al. **Crimes cibernéticos**. Periódicos Grupo Tiradentes, v. 2, n.3. p. 215-236, 2015. Disponível em: <https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217 >. Acesso em 16 de março de 2019.

ATHENIENSE, Alexandre. **Criar perfis falsos na internet é crime?**. In: Âmbito Jurídico, Rio Grande, XIII, n. 75, abr 2010. Disponível em: <

http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=7640

>. Acesso em 27 de maio de 2019.

AZEREDO, Eduardo et al. **Crimes Cibernéticos**. Revista juridica: Consulex. Ano 2008, v. 12, n. 284.

BAAS, NJ. **Stalking: slachtoffers, daders en maatregelen tegen deze vorm van belagen** Onderzoeksnotities 1998/1 van het Wetenschappelijk Onderzoek-en Documentatiecentrum van het Ministerie van Justitie. Report on victims, perpetrators and measures against stalking. Research notes 1998/1 of the Scientific Research and Documentation Centre of the Ministry of Justice.

BENAKOUCHE, Rabah. **O choque informático**. In: A informática e o Brasil. São Paulo: Polis, 1985.

BITENCOURT, Cezar Roberto: **Tratado de direito penal: parte geral,** 1 / Cezar Roberto Bitencourt. – 17ª Ed. rev., ampl. e atual. de acordo com a Lei n. 12.550, de 2011. – São Paulo: Saraiva, 2012.

BLUM, Renato Opice (Coord). **Direito Eletrônico – A Internet e os Tribunais**. São Paulo: Edipro, 2001.

BOBBIO, N. **A era dos direitos**. Trad. Carlos Nelson Coutinho. 10. ed. Rio de Janeiro: Campus, 1992.

BRASIL, Angela Bittencourt**. Informática jurídica: O ciber direito**. Rio de Janeiro: Juris Doctor, 2000.

BRASIL. Casos de Racismo na Internet. Disponível em <http://www.brasil.gov.br/consciencianegra/noticias/casos-de-racismo-na-internet-e-redes-sociais-devem-ser-denunciados> Acesso em 28 de maio de 2019.

BRASIL. **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. Obra coletiva de autoria da Editora Saraiva com a colaboração de Luiz Roberto Curia, Livia Céspedes e Juliana Nicoletti. 9ª Ed. São Paulo: Saraiva, 2013.

BRASIL. **Constituição (1988). Constituição da República Federativa do Brasil**. 28. ed. São Paulo: Saraiva, 2008.

BRASIL. Lei 12.735 de 30 de novembro de 2012. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: < http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 27 maio de 2019.

BRASIL. **Lei 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.** Disponível em: < http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em 14 março de 2019.

BRASIL. **Lei 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 22 abril de 2019.

BRETON, Philippe. **História da informática.** Tradução de Elcio Fernandes. São Paulo: Universidade Estadual Paulista, 1991.

CAPEZ, Fernando. **Curso de direito penal: parte geral.** 18ª Ed. Vol. 1. São Paulo: Saraiva, 2014.

CAPEZ, Fernando. **Curso de direito penal. Parte geral**. 6ª Ed. Vol. 1. São Paulo: Saraiva, 2003.

CASTRO, Carla Rodrigues Araújo. **Crimes de informática e seus aspectos processuais.** 2. ed. Rio de Janeiro: Lumen Juris, 2001.

CARNEIRO, A. G. **Crimes Virtuais: Elementos Para uma Reflexão Sobre o Problema na Tipificação.** In: Âmbito Jurídico, Rio Grande, 15, n. 99, abr. 2012. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=11529>. Acesso em 26 de abril de 2019.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. 1ª ed. Rio de Janeiro: Brasport, 2014.

CERT.br. **Estatísticas de Notificações de Spam Reportadas ao CERT.br**. Disponível em: http://www.cert.br/stats/spam/. Acesso em 10 maio de 2019.

Crimes CIBERNÉTICOS, disponível em <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acesso em 17 março de 2019.

DAMÁSIO DE JESUS, E. De. **Direito penal: parte geral.** 23ª ed. V. 1. São Paulo: Saraiva, 1999.

DAMÁSIO DE JESUS, E. De. **Direito penal: parte especial.** 15ª ed. V. 3. São Paulo: Saraiva, 2002.

DAMÁSIO DE JESUS, E. De. **Direito penal: parte geral.** 27ª ed. V. 1. São Paulo: Saraiva, 2005

DULLIUS, Aladio Anastacio. O **Dos Crimes Praticados em Ambientes Virtuais.** Disponível em: http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-em-ambientes-virtuais,38483.html/>. Acesso em 16 fevereiro de 2019.

EDDINGS, Joshua. **Como funciona a Internet.** Tradução de Tulio Camargo da Silva. São Paulo: ed. Quark, 1994.

FABBRINI, Renato N.. **Manual de direito penal: parte especial,** arts. 121 a 234 do CP. 25. ed. ver. e atual. Até 31 de dezembro de 2006 – 3. Reimpr. São Paulo: Atlas, 2008. V.2.

FURLANETO NETO, M.; GUIMARÃES, J. A. C. **Crimes na Internet: Elementos para uma Reflexão Sobre a Ética Informacional.** Revista CEJ. Brasília, n. 20. 2003. Disponível em: <http://www2.cjf.jus.br/ojs2/index.php/cej/article/viewFile/523/704>. Acesso em: 13 de fevereiro de 2019.

FURLANETO NETO, Mario. Lourenço dos Santos, José Eduardo. Veríssimo Gimenes, Eron. **Crimes na internet e inquérito policial eletrônico.** Ed. 1 – São Paulo. Edipro, 2012.

GATTO, Victor Henrique Gouveia. **Tipicidade penal dos crimes cometidos na internet.** Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=9962&revista_caderno=17>. Acesso em: 09 de março de 2019.

JESUS, Damásio Evangelista de. **Direito Penal.** 1º V. 2ª Edição, ampliada e atual. São Paulo: Saraiva, 1980.

JESUS, Damásio de. **Direito penal: Parte Geral.** 31ª edição. São Paulo: Editora Saraiva. 2011. vol 1.

JESUS, Damásio Evangelista de. **Direito penal.** São Paulo: Saraiva, 2005. v.1.

LECCCIONES, cit., v. 1, p. 195 - **Do acesso não autorizado a sistemas computacionais.** Rio de Janeiro: Forense, 2003.

LIMBERGER, Têmis. **Direito e informática: os desafios de proteger os direitos do cidadão**. In: SARLET, Ingo Wolfgang (Org.). Direitos fundamentais, informática e comunicação e algumas aproximações. Porto Alegre: Livraria do Advogado, 2007.

MARTINELLI, João Paulo Orsini. **Aspectos relevantes da criminalidade na internet.** Disponível em: <http://jus.com.br/artigos/1829/aspectos-relevantes-da-criminalidade-na-internet>. Acesso em 26 de outubro de 2018.

MENDES, Maria Eugencia Gonçalves. VIEIRA, Natália Borges. **Os crimes cibernéticos no ordenamento jurídico brasileiro e a necessidade de legislação específica.** 2012. Disponível em: <http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2>. Acesso em 26 de outubro de 2018.

MIRABETE, Julio Fabbrini; FABBRINI, Reanato N.. **Manual de direito penal: parte geral,** arts. 1º a 120 do CP. 29. ed. rev. e atualizada até 10 de janeiro de 2013. São Paulo: Atlas, 2013.

MIRABETE, Julio Fabbrini. **Manual de Direito Penal.** São Paulo: Atlas, 2001. v. 3.

MIRABETE, Julio Fabbrini. **Manual de Direito Penal.** 23ª1 ed. rev. e atual. São Paulo: Atlas, 2006.

MONTEIRO NETO, J. A. **Aspectos Constitucionais e Legais do Crime Eletrônico**. Fortaleza, 2008.

MORAN, José Manuel. **Novos caminhos do ensino à distância.** Informe CEAD - Centro de Educação à Distância. SENAI. Rio de Janeiro, Ano 1, n. 5, out/nov/dez 1994.

MORAN, José Manuel. **Novas Tecnologias e o Reencantamento do Mundo**. Tecnologia Educacional. Rio de Janeiro, vol. 23, n.126, setembro-outubro 1995.

MORAN, José Manuel. **Como Utilizar a Internet na Educação.** Disponível em: <http://www.eca.usp.br/moran/internet.htm>. Acesso em 11 de março de 2019.

NORONHA, Edgard Magalhães. **Direito penal: Dos crimes contra a pessoa e dos crimes contra o patrimônio.** 28. ed. rev. e at. São Paulo: Saraiva, 1996. Atualizado por Adalberto José Q.T de Camargo Aranha. v. 2.

NORONHA, Edgar de Magalhães. **Direito penal.** 20ª. ed. São Paulo: Saraiva, 1982.

NUCCI, Guilherme de Souza. **Código penal: comentado.** 17. ed. rev. e atual. Rio de Janeiro: Forense, 2017.

NUCCI, Guilherme Souza. **Manual de Direito Penal - Parte Geral - Parte Especial,** 9ª Edição. São Paulo; Editora Revista dos Tribunais, 2013.

NUNES, Massio Barbosa. **Crimes Virtuais: Uma análise acerca de alguns de seus aspectos.** Fortaleza, 2015. Disponível em: http://www.faculdadescearenses.edu.br/biblioteca/TCC/DIR/CRIMES%20VIRTUAIS%20UMA%20ANALISE%20ACERCA%20DE%20ALGUNS%20DE%20SEUS%20ASPECTOS.pdf. Acesso em: 03 de março de 2019.

PINHEIRO, Patrícia Peck. **Direito digital.** 4ª ed. São Paulo: Saraiva, 2010.

PINHEIRO, Emeline Piva. **Crimes virtuais: uma análise de criminalidade informática e da resposta estatal.** Disponível em: <http://www.egov.ufsc.br:8080/portal/conteudo/crimes-virtuais-uma-an%C3%A1lise-da-criminalidade-inform%C3%A1tica-e-da-resposta-estatal>. Acesso em: 17 de fevereiro de 2019.

PIRAGIBE, Clélia. **Indústria da Informática: Desenvolvimento Brasileiro e Mundial**. Rio de Janeiro: Campus, 1985.

PRETTO, Nelson; BONILLA, Maria Helena. **Sociedade da informação: democratizar o quê?** Salvador. Disponível em: <http://www.faced.ufba.br/not/83.htm>. Acesso em: 11 de outubro de 2018.

REMY; Gama Filho, Editora: CopyMarket.com, 2000 - **Teoria do Delito, Suspensão Condicional do Processo Penal,** Editora Revista dos Tribunais.

SANTOS, W. **Dicionário jurídico brasil**eiro. Belo Horizonte: Del Rey, 2001.

SOUZA, G. L. M.; PEREIRA, D. V. **A Convenção de Budapeste e as Leis Brasileiras**. Paraíba, 2009.

SILVA, Rita de Cássia Lopes da. **Direito Penal e sistema informátic**o. São Paulo: Editora Revista dos Tribunais, 2003.

TERCEIRO, Cecílio da Fonseca Vieira Ramalho. **O problema na tipificação penal dos crimes virtuais.** Disponível em: <http://jus.uol.com.br/revista/texto/3186/o-problema-na-tipificacao-penal-dos-crimes-virtuais>. Acesso em: 09 de março de 2019.

VALZACCHI, Jorge R. **Internet y Educacion: Aprendiendo y Ensensando em los espacios virtuales.** 2. Ed. Versão Digital, 2003. Disponível em: <http://www.educoas.org/portal/bdigital/es/indice_valzacchi.aspx>. Acesso em: 19 de abril de 2019.

WIERNER, Norbert. **Cibernética e sociedade – O uso humano de seres humanos**. São Paulo: Cultrix, 1950.

WENDT, Emerson, JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos – Ameaças e Procedimentos de Investigação.** 1. ed. Rio de Janeiro: Brasport, 2012.

ZANDONADI, Viviane. Na cola dos crackers. Info Exame, São Paulo, v. 19, n. 221, p. 66-67, ago. 2004.