PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

CRIMES CIBERNÉTICOS E A ATUAÇÃO DO ESTADO BRASILEIRO SOBRE ELES

ORIENTANDA- ÉVILIN NOGUEIRA DOS SANTOS LIMA

ORIENTADORA- PROF.ª DR.ª FERNANDA DE PAULA FERREIRA MOI

GOIÂNIA- GO

2022

ÉVILIN NOGUEIRA DOS SANTOS LIMA

CRIMES CIBERNÉTICOS E A ATUAÇÃO DO ESTADO BRASILEIRO SOBRE ELES

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof.ª Orientadora – Drª Fernanda de Paula Ferreira Moi

GOIÂNIA-GO

2022

ÉVILIN NOGUEIRA DOS SANTOS LIMA

CRIMES CIBERNÉTICOS E A ATUAÇÃO DO ESTADO BRASILEIRO SOBRE ELES

Data da Defesa: 18 de maio de 2022

BANCA EXAMINADORA

Orientadora: Prof ª: Dra. Fernanda de Paula Ferreira Moi Nota:

Examinador Convidado: Prof. Me. Frederico Gustavo Fleischer Nota:

CRIMES CIBERNÉTICOS E A ATUAÇÃO DO ESTADO BRASILEIRO SOBRE ELES

Évilin Nogueira dos Santos Lima[1]

Este trabalho, de natureza teórica, possui como objetivo analisar o cenário dos crimes cibernéticos e a atuação do Estado Brasileiro sobre eles, bem como entender as mudanças relacionadas ao mundo digital e a importância da educação digital. A pesquisa inicia destrinchando elementos do ambiente virtual e explicando conceitos como rede, protocolo e microprocessador. Após os conceitos se debate a importância do mundo virtual como ferramenta imprescindível atualmente e se analisa o anonimato no meio virtual explicando as "camadas" da internet, sendo elas Surface Web, Deep Web e Dark Web. Após a análise do mundo virtual, a pesquisa traz o debate de o que são os crimes virtuais e delitos informáticos e como a legislação brasileira dispõe sobre, complementando trazendo um enfoque para a importância da perícia nos casos dos crimes virtuais. Por fim, debate-se dentro da cibercriminologia se o melhor caminho a ser escolhido como resolução dos delitos seria a punibilidade ou a prevenção, aprofundando a pesquisa para o campo da prevenção com a educação digital.

Palavras-chave: Cibercrimes; digital; educação; lei; internet.

[1] Acadêmica do Curso de Direito pela Pontifícia Católica de Goiás.

SUMÁRIO

INTRODUÇÃO

Juntamente com o fenômeno da globalização, a expansão digital potencializou a conexão mundial e a deixou mais tecnológica. A tecnologia está presente em todos os espaços e repercute, por exemplo, nos costumes, nos hábitos, no lazer, e no exercício das profissões. Nesse sentido, no campo das Ciências Jurídicas, o impacto da tecnologia foi impulsionado pelo evento pandêmico da Covid-19.

À vista disso, a presente pesquisa buscou abordar os conhecimentos dentro do Direito digital, em específico sobre crimes cibernéticos e como o Estado atua sobre eles. Preocupou-se em pensar no direito digital de forma a contribuir socialmente para que em teoria, possamos alcançar uma evolução “segura”.

Com a popularização da internet juntamente com o crescimento do número de usuários, surgiram problemas jurídicos que até então nunca haviam sido enfrentados. A nova modalidade de crime que surgiu a partir do meio digital, gerou a preocupação com um novo bem jurídico que hoje é tutelado pelo ordenamento jurídico brasileiro.

Assim sendo, foi utilizado na pesquisa o método hermenêutico que contribuiu para interpretar o problema e os elementos relacionados ao tema buscando respostas para os questionamentos levantados e esclarecendo conceitos e os elementos que compõem o meio digital e seus instrumentos.

Portanto, nos capítulos seguintes, fez-se uma análise do ambiente digital, da necessidade de criar formas de proteção ao usuário da internet e da imprescindibilidade de o Estado Brasileiro ser mais eficiente no combate ao crime cibernético a partir de uma legislação bem estruturada e de investimentos tanto na área da perícia forense computacional quanto na educação digital.

1 O AMBIENTE DIGITAL

Desde o surgimento da internet, a civilização como um todo sofreu a ação da tecnologia ao logo do tempo. Hoje entendemos a internet como um bem que possui valor central e que está em constante evolução. Não há o que se falar em um mundo desconectado, sem a internet e a virtualidade.

O mundo passou por grandes mudanças e todo o universo online da informação contribuiu para disseminar informações globais resultando em questões jurídicas que nunca foram encontradas até agora. Nunca, na história, a vida privada ou empresarial, teve uma exposição tão grande, onde informações falsas ou verdadeiras são espalhadas de forma desregrada, e a sabotagem e o sequestro de informações tem acontecido cada vez mais.

Traz a reflexão:

> "[...]Muito ainda se fala em geração X, geração Millenials (ou geração Y) e geração Z. Mas hoje já experimentamos em nossa sociedade uma nova geração: a geração C², de "conectada". São as pessoas que nunca viveram sem que estivesse constantemente conectadas na virtualidade. Pessoas para as quais o normal é conviver com uma parte material e uma parte imaterial de suas vidas. [...]" (SYDOW, 2021, p. 21 - 22).

As sociedades e seus membros mudam e consequentemente seus pensamentos também. A inovação tecnológica afeta todas as atividades humanas. Conosco, as leis coexistem e estas têm de adaptar as novas necessidades de cada era.

Para Pinheiro (2010): "A capacidade de adaptação do Direito determina a própria segurança do ordenamento, no sentido de estabilidade do sistema jurídico por meio da atuação legítima do poder, capaz de produzir normas válidas e eficazes". (*Apud* BEZERRA, 2020, p. 11)

Neste sentido, podemos vislumbrar a expansão tecnológica pela qual toda nossa sociedade passou e ainda passa, pois, como dito anteriormente, é um bem em permanente evolução.

A tecnologia e o ambiente digital, ainda nas palavras de Sydow, são rapidamente construídos, absorvidos, aceitados, entendidos, modificados, adaptados e até mesmo substituídos. E dessa forma "a tecnologia é inserida comercial e inconsequentemente frente às cautelas jurídicas e apenas após sofrerá efeitos e controles" (SYDOW, 2021, p.12).

Desde o ano de 2016, a ONU definiu o entendimento de que a descontinuação intencional do acesso à Internet, feita por um Governo, viola os Direitos Humanos. Vejamos,

entende-se que o acesso à internet a partir dessa resolução é um meio de expressão social e como traz o texto resolutivo os mesmos direitos que as pessoas têm offline também devem ser protegidos on-line.

Tamanho é o impacto dessas tecnologias que já se propôs a criação de uma quinta geração de direitos, os direitos da realidade virtual. (*Apud* BARRETO, 2021. p.100)

Sendo assim, percebemos que o meio digital, além de manter conexões intercontinentais, acelerar e modernizar o estilo de vida, é também um meio extensivo dos direitos do homem, nos permitindo, portanto, entender a importância de se tutelar as práticas do meio eletrônico.

Para Pinheiro (2010):

> Tecnicamente, a Internet consiste na interligação de milhares de dispositivos do mundo inteiro, interconectados mediante protocolos IP (abreviação de Internet Protocol), ou seja, essa interligação é possível porque utiliza um mesmo padrão de transmissão de dados. A ligação é feita por meio de linhas telefônicas, fibra ótica, satélite, ondas de rádio ou infravermelho. A conexão do computador com a rede pode ser direta ou através de outro computador, conhecido como servidor. Este servidor pode ser próprio ou, no caso dos provedores de acesso, de terceiros. O usuário navega na Internet por meio de um browser, programa usado para visualizar páginas disponíveis na rede, que interpreta as informações do website indicado, exibindo na tela do usuário textos, sons e imagens". (Apud BEZERRA, 2020, p. 14)

Importante deixar claro que entende-se o meio digital como a união de uma grande rede conectada, a qual é um ambiente aberto, volátil e que permite o empoderamento de quem acessa o meio.

A rede é um ambiente formado pela conexão de milhões de aparelhos que se comunicam gerando um tráfego de informações. Nesse sentido, a internet é um conglomerado de redes que através de protocolos trafegam informações. Entende-se o protocolo por um conjunto de regras que padronizam a comunicação através das redes.

O protocolo existe, portanto, para parametrizar a comunicação entre serviços, sendo que as informações possuem uma forma definida de envio e recebimento, como por exemplo, o protocolo que utilizamos para navegar na internet não é o mesmo que utilizamos para enviar um e-mail.

Todo equipamento que se conecta à internet, possui um endereçamento conhecido como *Internet Protocol- IP*, que é o protocolo de endereçamento de equipamentos conectados à rede. Atualmente, o ambiente digital está passando por uma atualização deste protocolo transitando da versão IPv4 para a versão IPv6. O objetivo da atualização é trazer maior segurança e privacidade, além do aumento de *hosts*[2].

Necessário trazer ao tema outro agente do ambiente digital, o microprocessamento. "Este causou uma enorme evolução tecnológica permitindo um crescimento exponencial da capacidade computacional, a miniaturização de dispositivos eletrônicos e a diminuição de seus custos, visto que foram feitos em larga escala e à base de silício." (BARRETO, 2021, p. 35)

O microprocessador é um componente computacional que realiza função de cálculo e tomada de decisões de um uma máquina. Ele é o cérebro do computador. Através da disponibilização deste processador nos mais variados dispositivos temos a viabilização barata e simples do acesso à internet. Assim temos a construção do fenômeno da conversão digital. (BARRETO, 2021, p. 35)

A internet nos dá o poder e a força que por vezes, se fosse somente a partir do mundo real não a teríamos e, sendo assim, a partir do virtual crescemos e modificamos a realidade fazendo com que um coexista com o outro. Assim como a liberdade ampla permite denúncias de violações de direitos humanos por cidadãos de países totalitários, seja de modo expresso ou seja de modo tácito, ela também permite as prejudiciais fake News. (SYDOW, 2021, p. 22).

Com a globalização, houve uma mudança na mentalidade social, transgredindo de indivíduos passivos e inertes para indivíduos atuantes e ativamente críticos. Existe, portanto, a coexistência entre dois mundos o real e o virtual. Imperioso dizer que na mesma proporção que se tem bons feitos a partir do meio digital, tem-se a parte negativa, a qual engloba assuntos como: fake news, roubos, estelionatos, sequestro de informações sigilosas e "cancelamentos" -termo utilizado para descrever a depredação de imagem.

Neste sentido, pode-se dizer que a globalização modificou pensamentos e valores que provocaram novas análises de instituições e legislações.

> [...]. As ações delitivas que são iniciadas em um determinado local e se utilizam de computadores infectados em diversos países para produzir resultados danosos em outro ponto do globo, levam a uma imperiosa necessidade de os países reverem conceitos de territorialidade, mitigarem aspectos de sua soberania, disporem-se a

[2] Host é um equipamento/computador/máquina conectado a uma rede, portanto IP e nome definidos que provê alguma informação, recurso e serviços aos usuários ou clientes.

> partir e prestar cooperação, sob pena dos cibercrimes restarem impunes. (BARRETO, 2021, p. 35)

Portanto, a tecnologia em sua constante evolução, requer novos limites e respostas legais, de forma a manter o ordenamento jurídico atualizado, para que não fique ultrapassado.

1.1 A INTERNET E O SEU MEIO OBSCURO

A internet é um meio de comunicação cada vez mais utilizada no dia a dia. Dentro da rotina das pessoas, ela é considerada por muitos indispensável para realizar diversos serviços, como por exemplo trabalhar, assistir aula, participar de congressos, fazer compras e conhecer novas pessoas. Logo, estar on-line promove relações sociais sem ter que sair de casa

Esta ferramenta imprescindível se comunica com um banco de dados, que pode até ser considerada como uma fonte de ouro na visão daqueles que possuem a intenção de praticar crime a partir desses dados, possibilitando, portanto, em muitos casos um grande prejuízo financeiro e pessoal ao usuário de boa-fé da internet.

A internet é o “Eldorado” da informação, por ela circulam diversos dados, de todo quanto é tipo, de bilhões de pessoas. Esses dados, após serem identificados, catalogados, tratados e organizados, geram informações valiosas.

Quanto mais navegamos pela internet, mais obtemos acesso à informação e mais ainda nos é oferecido novas informações. A impressão que deixa ao usuário é a de que ele consegue acessar qualquer parte do mundo e fazer o que ele bem entender através da internet.

Por detrás da parte mais acessível da internet, habita um submundo peculiar e multifacetado. A chamada Deep Web, possui em suas características uma menor transparência e um maior anonimato.

Mas engana-se aquele que pensa que a grande maioria dos crimes acontece na Deepweb. Primeiramente, é importante fazer um breve apanhado das camadas que possui a internet, para que se possa vislumbrar melhor o assunto trabalhado. Vejamos a imagem abaixo:

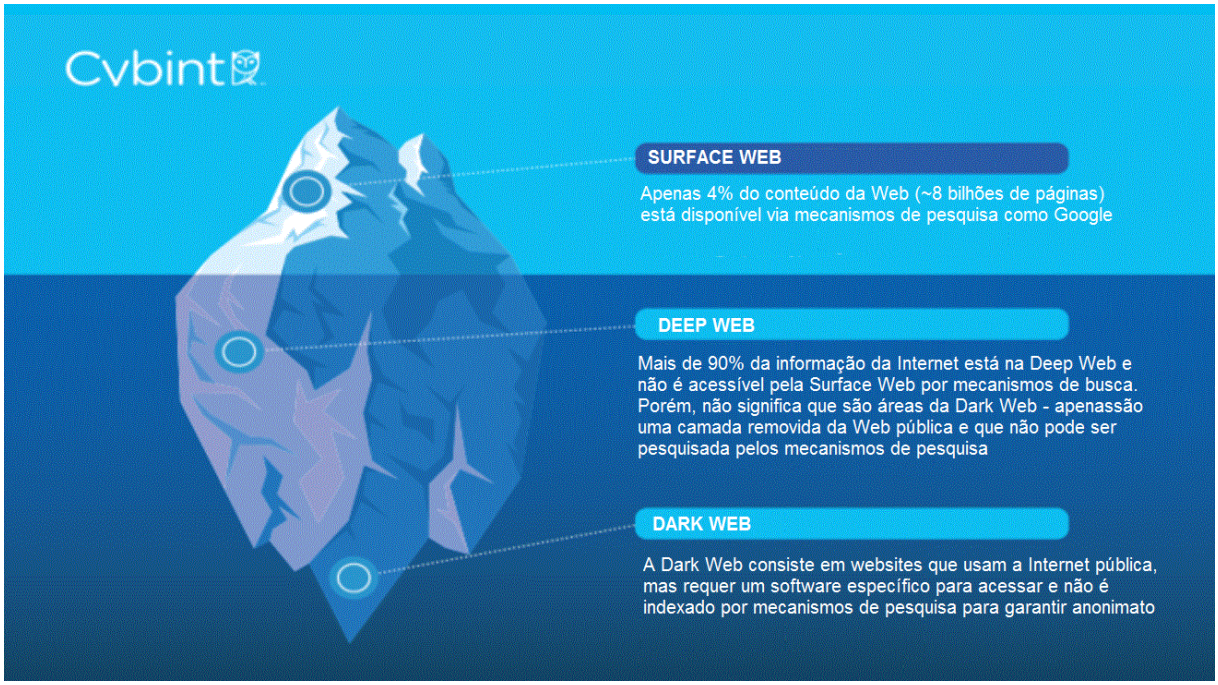

Figura 1: Tamanho da Deep Web

Fonte: secureworldexpo.com (acessado em 02/06/19)

A partir da imagem, percebemos a internet em 3 camadas. A Surface Web é a camada que contém os mecanismos de busca fornecendo um conteúdo aberto aos usuários, é onde acessamos sites como Amazon, Google, Bing, Pinterest, Facebook e Jornais como o BBC News. Em resumo, é onde as atividades diárias acontecem, é também o que a maioria das pessoas conhecem como Internet. A Surface Web é a parte indexada.

A Deep Web é a camada seguinte, que se encontra abaixo da "internet comum", essa é a parte não indexada da internet, ela não pode ser encontrada por navegadores comuns. Ocorre que ela é formada por dados feitos para serem ocultos do público, nela guarda-se todos os tipos de informações.

Nas palavras de Sydow:

> Uma parte da deepweb, assim como uma parte da sociedade, é utilizada especialmente para a delinquência ou para desvios sociais. Tal parte normalmente só não está indexada, mas também não raro possui forma especial de acesso, a partir de mecanismos de anonimidade mais complexos como o uso softwares dedicados, uso de configurações especiais ou autorizações específicas. (SYDOW.2021. P.58)

Nessa perspectiva, chegamos à conclusão de que ao contrário da imaginação da maioria das pessoas, a DeepWeb não é um lugar terrível contendo apenas conteúdo estranho e criminoso. Parte dela é utilizada para a confidencialidade, anonimidade, armazenamento de informações financeiras e bancárias, direitos autorais, e-mails e armazenamento na nuvem.

E por último, temos a camada mais profunda da internet, a chamada Dark Web, nela utiliza-se o anonimato proveniente do TOR, um navegador específico que utiliza um protocolo

de funcionamento conhecido como cebola (do inglês onion, formando a sigla do navegador de nome The Onion Router- TOR).

Esse navegador camufla a localização do servidor, permitindo que apenas usuários TOR ou outra aplicação que utilize o sufixo "onion" visualiza as páginas e sites registrados na Dark Web.

Os sites que habitam a Dark Web utilizam servidores fora do convencional compostos por uma redes voluntárias ao redor do mundo, criando uma comunicação fortemente criptografada em camadas, é daí que surge a comparação com uma cebola, pois contém camadas e camadas de criptografia.

O nome de Dark Web vem do conceito de darknet. A darknet é uma rede sobreposta que só pode ser acessada sob requisitos específicos e usa protocolos que excedem completamente a superfície da web e outros padrões da Deep Web. Isso leva ao uso da dark web para distribuição de conteúdo e transações ilegais. Por exemplo, o site do Silk Road foi fechado pelo FBI em 2013 porque era uma plataforma para transações ilegais de drogas e um serviço oculto que usa a rede TOR para garantir o anonimato de compradores e vendedores.

Portanto, devido ao seu anonimato, a Dark Web está realmente inundada com atividades ilegais que vão desde a compra de drogas até a compra e venda de órgãos humanos. Nela ainda pode-se encontrar material sobre pedofilia e zoofilia, contratos com assassinos e tráfico de pessoas, fóruns de terrorismo, nazismo e sites com uma variedade de conteúdos e tópicos inimagináveis.

Para uma melhor compreensão das camadas da internet explicadas acima, se faz necessário a explicação do conceito de indexação. A indexação ou indexar uma informação é o processo de identificação dos sites que existem e o armazenamento da URL[3], nome e o assunto do que se trata o site.

Logo, todas as informações que encontramos quando pesquisamos algo no Google, por exemplo, só é possível pois aquele conteúdo foi indexado, permitindo em consequência a identificação do site.

1.2 ANONIMATO

[3] A URL, Uniform Resource Locator, na sua tradução literal é um localizador uniforme de recursos, é o endereço onde se encontra um recurso informático (documento, serviços, mídia) na internet.

O anonimato no ambiente virtual é um assunto polêmico, pois normalmente não temos informações se é uma pessoa agindo ou um computador de forma automatizada. Nos últimos tempos, nota-se uma crescente atuação de bots[4] comandados por pessoas para disseminar informações em massa.

O significado de anonimato conforme o dicionário Priberam de língua portuguesa é a qualidade do que é anônimo; sistema de escrever anonimamente. Na internet, o anonimato é uma posição de bloqueio ou impedimento no que diz respeito a identificação da autoria de uma postagem.

O anonimato na Internet pode ser empregado através de VPNs, serviço que criptografa o tráfego de internet e disfarça sua identidade online por meio de redirecionamentos entre servidores, mascarando a real localização do usuário.

Antes de adentrarmos a fundo no assunto, é interessante discutir a relevância do anonimato na rede ou quando pode ser usado para fins bons ou ruins. Portanto, é importante fazer uma pergunta: o anonimato é bom? Se é bom, em que cenário se aplica? Por quê? As respostas a essas perguntas dependem da finalidade do serviço anônimo.

Por exemplo, o anonimato pode ser visto em um cenário positivo quando pensamos na conservação da privacidade e segurança na internet, visto que, por um lado auxilia na prática da liberdade de expressão. De outro lado, o anonimato pode ser algo ruim quando um indivíduo sequestra os dados de uma empresa e exige um resgate de alto valor financeiro, deixando a empresa em um cenário totalmente vulnerável e à mercê da pessoa que está do outro lado da tela.

A vida moderna, nos permite compartilhar muitas informações pessoais online. Nesse sentido as redes sociais são catalisadoras dessa prática, visto que, nela as pessoas compartilham os hábitos de consumo, a rotina pessoal, a rotina profissional, estilos de vida, e as opiniões manifestas sobre os diversos assuntos que percorrem na rede.

Importante distinguir os conceitos de anonimato e privacidade. A privacidade é um direito constitucional defendido no artigo 5°, inciso X da Constituição federal de 1988, nela tutela-se o direito de controlar a divulgação de dados e imagem pessoal. O anonimato é a ação de ocultar, não divulgar, a identidade.

Túlio Vianna demonstra que o direito à privacidade corresponde a um conjunto de direitos, vejamos:

[4] Bot- abreviação de robô- é um programa que executa tarefas automatizadas, repetitivas e pré-definidas.

> Direito de não ser monitorado, ou seja, de manter o que diz e sua imagem privadas
>
> Direito de não ser registrado, que discorre sobre a preservação quanto a gravações sem consentimento
>
> Direito de não ser reconhecido, se referindo a não ter conteúdos sobre si publicados em qualquer canal, incluindo a internet.
>
> (*Apud* SABINO, Marco Antônio da Costa. 2020).

Assim, resta clara a diferença que há entre a privacidade e o anonimato, sendo errôneo confundir os dois conceitos que denotam circunstâncias diferentes.

Ao refletirmos sobre a facilidade de se encontrar informações na Internet, e analisando também a facilidade de se espalhar, copiar e reproduzir arquivos, percebemos que, distanciando o pensamento da atividade criminosa, para o usuário comum é difícil estar ou ser totalmente anônimo.

Ora, tudo que se faz no meio virtual deixa um rastro e é impossível apagar todos os rastros digitais visto que alguns sistemas podem manter seus dados mesmo após a solicitação de exclusão. Logo tempos uma falsa sensação de controle sobre as nossas próprias informações.

Em se tratando das atividades delitivas no meio virtual, o anonimato por um lado permite uma segurança para denunciar abusos, violências e transgressões, sendo possível preservar a imagem da vítima, ou seja, o anonimato contribui para dar voz aqueles que de alguma forma são coibidos. Em contrapartida, se torna possível, em função do anonimato, a promoção de discurso de ódio, fake News, fraudes, chantagem, assédio sexual, estelionatos, sequestro de dados, cyber terrorismos e vários outros delitos que têm sua prática mais "acessível" por se utilizar da proteção que o anonimato oferece.

Assim sendo, a internet proporciona a todos os usuários a sensação da total anonimidade. Essa sensação impulsiona alguns indivíduos a ir de encontro a lei, na ilusória sensação de que não serão descobertos, de que agirão sem serem percebidos ou julgados.

A legislação brasileira proíbe o anonimato expressamente, tanto no mundo real quanto no virtual, traz o artigo 5° inciso IV da Constituição:

> 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:
>
> IV - é livre a manifestação do pensamento, sendo vedado o anonimato;

A intenção do artigo ao vedar o anonimato é identificar e, nos casos em que couber, responsabilizar o autor por conteúdo ilegal ou criminoso que tenha sido reproduzido.

No mesmo sentido, o Marco Civil da Internet, Lei nº 12.965 de2014, no seu artigo 3° reafirma a livre manifestação do pensamento, nos termos da Constituição Federal, desde que haja também a responsabilização dos usuários de acordo com suas atividades.

A Lei Geral de Proteção de Dados, Lei n° 13.709 de 2017, foi promulgada objetivando complementar a literatura do Marco Civil da internet, também tutela sobre o anonimato, garantindo o direito ao mesmo desde que esteja manifestamente expresso pelo titular das informações. Como por exemplo, traz o artigo 18, inciso IV da lei:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> [...] IV - Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

Ou seja, o documento confirma o direito de anonimato no uso, bloqueio ou eliminação de dados que estejam sendo tratados em desconformidade com a lei. Logo, percebe-se que é protegido pelo ordenamento brasileiro o direito ao anonimato no tocante ao zelo e a privacidade de dados e informações, não se permite, portanto, o uso desse direito para práticas ilegais e criminosas além de coibir a expressão de pensamento de forma anônima.

1.3 AGENTES VIRTUAIS: HACKER E CRACKER

No universo da virtualidade, há alguns termos que definem alguns usuários com habilidades e conhecimentos avançados em relação ao universo das tecnologias, administração de banco de dados e servidores, e principalmente segurança da informação.

No geral, ambas as classificações demonstram que os agentes são experts em encontrar vulnerabilidades em sistemas operacionais e softwares. Contudo, os objetivos que os levam a encontrar essas falhas nos sistemas são contrários. Enquanto um utiliza de forma legal e construtiva os seus conhecimentos, que é o Hacker, o outro utiliza para cometer delitos por meio de quebras de segurança e invasões de programas ou sistemas operacionais, que é o Cracker.

Contudo, parte da comunidade tecnológica não se agrada em apenas definir um como bom e o outro como ruim. Assim, dentro da Ética Hacker os termos mais corretos, para essas pessoas, seriam: “White Hat” (chapéu branco), “Black Hat”(chapéu preto) e “Gray Hat”(Chapéu Cinza).

White Hat, é o hacker defensivo, ele é o especialista em utilizar suas habilidades para o bem e identificar as fragilidades de um sistema. O White Hat, age com ética e propósito legal.

O Black Hat, é o tipo de hacker mais conhecido, é aquele que viola a segurança de um sistema visando benefício próprio, como por exemplo, roubar dados de cartão de crédito, sequestrar dados de empresas e pedir um resgate com alto valor econômico. Ele pode identificar a vulnerabilidade de um sistema e vender para uma organização criminosa (os Crackers).

Já os Grey Hat, são os Hackers que ficam “em cima do muro”, eles agem de forma legal, mas em certos casos eles se utilizam de ideais pessoais e tomam ações que prejudicam os sites contudo não cometem crimes utilizando essas informações. Eles são bem-intencionados, contudo, se perdem na sua vontade de ajudar e cometem comportamentos que são eticamente questionáveis.

2 CRIMES VIRTUAIS, DELITOS INFORMÁTICOS E A LEGISLAÇÃO PENAL

O ciberespaço teve sua popularização no final da década de 1990, é a partir desse fenômeno que surgiu a necessidade de compreender esse espaço sob todas as suas vertentes, social, cultural, científica e demais. A internet se mostrou uma poderosa arma para ampliar conhecimentos e socializar com o outro, assim tornou-se possível uma troca cultural maior.

A tecnologia proporcionou e ainda proporciona um crescimento exponencial de sistemas, programas e aplicativos que foram desenvolvidos para facilitar a adoção do meio virtual. Além disso, no início dessa nova cultura, não havia um limitador do espaço virtual, logo foi inserido na sociedade a expansão de um meio não controlado pelas autoridades e aparentemente totalmente livre, para se fazer, ser (enquanto "personagem virtual") e falar o que quiser.

Essa aparente liberdade juntamente com a facilidade de esconder quem realmente é no espaço virtual, possibilitou abertura para o cometimento de crimes. No Brasil, os primeiros casos de crimes cibernéticos surgem em 1996, foram descobertos casos de pornografia infantil pela internet. A partir daí temos o seguinte histórico: 1998- primeiros casos de clonagem de cartão; 2000 – primeiros casos de fraude bancária pela Internet; 2002 – Phishing: cavalo de tróia; 2009- Grande explosão de fraudes bancária através de clonagem de cartão de crédito e intetnet banking, desse último evento foi apurado pela Federação Brasileira de bancos um prejuízo estimado em um bilhão de dólares; 2011- ataques a páginas eletrônicas do governo brasileiro como por exemplo IBGE e Receita Federal.

Vejamos, segundo o entendimento da Patrícia Peck, a Ciência Jurídica é a responsável por equilibrar a relação comportamento-poder, o que só pode ser feito com a interpretação adequada das realidades sociais, criando normas que garantam a segurança esperada por meio da eficácia e aceitação, dessa forma é possível compreender e abarcar a mudança através de uma estrutura flexível que poderá ser sustentada no correr do tempo.

É a partir desse entendimento que caminhamos para o ramo que hoje é conhecido por Direito Digital. Contudo, a Ciência Jurídica não consegue acompanhar a tecnologia pelo fato de que, esta, por constante evolução, sempre estará a sua frente. Sendo assim, sempre haverá uma lacuna na regulamentação jurídica, visto que esta última é impossibilitada de dar uma resposta rápida por depender de uma adequada interpretação da realidade social, que hoje é modificada a passos largos.

É no desencontro da evolução tecnológica que surge o espaço para os crimes e delitos virtuais, assim urge a necessidade de nos protegermos com medidas legais para combater este tipo de delito. Prescinde ressaltar que o crime virtual possui característica de auto renovação e desenvolvimento, já que evolui juntamente com as tecnologias.

Para termos uma breve noção, a nível mundial, o primeiro registro de tutela jurídica do meio virtual surgiu com a Convenção de Budapeste, firmada pelo Conselho da Europa em 23 de novembro de 2001, entrando em vigor no ano de 2004. A convenção trazia nos seus quarenta e oito artigos a tentativa de uniformizar uma legislação que combatesse o cibercrime, uniformizasse terminologias e estabelecesse uma cooperação internacional.

Portanto, neste capítulo, o objetivo é entender como foi percebido pelo ordenamento jurídico brasileiro os crimes virtuais e delitos informáticos, e como foi desenvolvida a legislação penal informática.

2.1 DELITOS INFORMÁTICOS

A nova modalidade de crime que surge a partir do meio digital deixa exposta a nossa integridade física, moral e financeira. Segundo Jonathan Clough, existem três fatores necessários para a prática de crime: a existência de criminosos motivados, disponibilidade de oportunidades adequadas e a ausência de vigilância eficaz. Ou seja, esses elementos são facilmente encontrados no meio digital. Portando, com uma conexão e um dispositivo com acesso à internet, qualquer pessoa mal-intencionada, pode cometer delitos no ciberespaço.

Inicialmente vale entender o que seria o bem jurídico informático e por que protegê-lo. Pois bem, a fundamentação dessa pesquisa é de que a passos largos surge para o direito uma nova preocupação e uma nova necessidade de se proteger a sociedade e o cidadão decorrente dos avanços tecnológicos. Para defendermos que é necessário criar essa proteção, é necessário que haja um bem jurídico a ser tutelado.

Entendemos o bem jurídico como circunstâncias dadas ou finalidades que são úteis para o indivíduo e seu livre desenvolvimento no marco de um sistema global estruturado(...) (*Apud* SYDOW, p 178. 2022) A vista disso, podemos partir do ponto que o avanço tecnológico gerou a imprescindibilidade de se criar um novo bem jurídico. Doutrinariamente, o bem jurídico informático é denominado “segurança informática”, conceito que reúne 3 elementos

compreendidos como ativos informáticos: disponibilidade, confidencialidade e integridade telemática.

A disponibilidade refere-se à necessidade de os dados de um usuário estarem sempre ao seu alcance para que ele utilize sempre que desejar. A confidencialidade diz respeito ao sigilo acerca dos dados, tal como o sigilo bancário, se um usuário decide por não publicar determinada informação, ela deve ser protegida até que o portador do dado permita a utilização do dado. Podemos exemplificar isso usando como modelo o aviso de permissão que alguns aplicativos de celular solicitam, para que aquele determinado aplicativo colete ou não informações acerca do usuário. Já a integridade nos remonta a ideia de que os dados produzidos por usuários e inseridos em um sistema configuram um patrimônio individual que merece ser protegido, visto que cabe somente ao usuário titular do dado dispor sobre alterações no mesmo, os ataques a essas informações colocam-nas em risco deixando-as expostas a perca de características originais.

Pois bem, esclarecido o bem jurídico informático e os elementos que o compõem, passamos a analisar os delitos informáticos. Entendemos que o surgimento do Direito Digital e do Direito Penal informático é uma nova especialidade das Ciências Jurídicas. Quanto ao Direito Penal informático, tal como o Direito Penal, faz-se necessário analisar diversas características e princípios que compõe logicamente o estudo dessa nova área.

Ainda há uma divergência quanto à nomenclatura da ciência jurídica que acompanha e estuda os impactos tecnológicos. Nesse sentido, também há discordância na terminologia que trata da criminalidade da área em estudo. Nos ensinamentos de SYDOW:

> O termo mais adequado seria “delito informático” e não “crime informático” porque há crimes que podem ser realizados a partir de tecnologias, mas também há contravenções penais que o podem. Destarte, a expressão genérica “delitos” engloba tanto “crimes” quanto “contravenções penais”. Quiçá, também, poderse-ia utiliza do termo “infrações”. Nesse sentido, a rubrica da Lei 12.737/12 ao apresentar que a lei “Dispõe sobre a tipificação criminal de delitos informáticos”. (SYDOW.2022. P.266)

Portanto, para analisarmos o delito informático deve-se partir de diferentes perspectivas em decorrência das suas particularidades. O crime virtual é aquele que não utiliza contato físico entre vítima e ofensor, não possui a necessidade de vistoriar e mapear o local do fato, não apresenta alto risco físico e nem grande violência. Contudo essa categoria delitiva apresenta sempre um padrão que age de forma silenciosa, rápida e sem muito esforço, apresentando por vezes uma simultaneidade de lugares e contando principalmente com o

desconhecimento de agentes públicos para falharem na investigação e assim não conseguirem analisar os indícios do crime.

A vista disso, podemos considerar crimes virtuais aqueles que se utilizam de alguma maneira de um sistema de processamento de dados para atentar contrainformações armazenadas e assim se concretizarem. SYDOW, define delito informático da seguinte maneira:

> Delito informático é a conduta típica, antijurídica e culpável cometida através de recursos informáticos contra bens jurídicos comuns e/ou cometida em faze de bem jurídico informático, atingindo ou buscando atingir a esfera da segurança informática em seus elementos confidencialidade, integridade e disponibilidade. (SYDOW.2022. P.272)

Atualmente ainda não há uma uniformização da classificação dos crimes informáticos, mas para que seja executado um delito, podemos partir de 3 formas: 1- violando-se o bem jurídico informático em si, em seus elementos, fazendo uso de ferramentas comuns; 2- Utilizando-se do meio informático como instrumento para atacar bem jurídico diverso do informático; 3- Violando-se o bem jurídico informático entre si, em seus elementos, e utilizando-se para isso de meios exclusivamente informáticos.

Em conseguinte, podemos classificar o delito a partir da sua natureza que pode ser quanto ao bem jurídico atingido ou quanto a necessidade do meio. Considerando a primeira natureza, o bem jurídico atingido, o delito poderá ser **puro**, que é aquele em que o objetivo da conduta do agente é de atingir necessariamente o bem jurídico informático, ou **impuro**, que é aquele em que pretende atingir um bem jurídico diferente do informático, como por exemplo a honra, patrimônio, dignidade.

Partindo da análise da prescindibilidade do meio, podemos entender o delito por próprios, onde o meio informático é obrigatório para cometer o crime; ou impróprios, que ocorrem quando o agente voluntariamente utiliza o meio informático para cometer o crime, mas ele poderia ter sido praticado por qualquer outro meio.

Com a atualização das tecnologias, novas classificações e modalidades de delito vão surgindo, por conseguinte é atual pensarmos em um mundo virtual que se prepara para emergir globalmente, o Metaverso, que promete ser um mundo virtual onde as pessoas poderão interagir entre si e realizar diversas atividades como fazer compras.

Dessa maneira, o doutrinador Sydow nos convida a refletir sobre a necessidade de se pensar nas possíveis condutas delitivas que poderão ser praticadas no Metaverso[5] e atacarão as NFT's e as criptomoedas[6]. Assim sendo, quando estivermos diante esse cenário, presenciaremos um delito informático que, conforme as classificações aqui explicadas, podem ser entendidos como delitos próprios por necessitarem do meio informático para se concretizarem.

Para concluirmos o assunto, mister citar que o uso do meio informático gera, necessariamente, um rastro dos sites frequentados, dos registro dos comandos utilizados e da máquina por onde saiu o comando.

2.2 A LEGISLAÇÃO PÁTRIA E O SEU DESENVOLVIMENTO NO CENÁRIO VIRTUAL

É necessário ressaltar que a pobreza de regulamentações do cenário virtual e as questões decorrentes requer do poder judiciário brasileiro a regulamentação através de decisões judiciais. Logo ficamos dependentes do caso concreto para passar a analisar a realidade virtual e suas modificações, esse cenário gera incertezas ao usuário pelo simples fato de que é perigoso e pouco prático visto que a velocidade com que a tecnologia e os delitos decorrentes do meio se modificam é muito maior que o tempo de resposta de uma decisão jurídica.

A primeira preocupação do legislador brasileiro com a interferência do mundo virtual no mundo real foi em 1990 com a criação do Código de Defesa do Consumidor e em 1995 foi publicada a norma 001 que tratava do uso dos meios da rede de telecomunicações para provimento e utilização de serviços de conexão à internet, esse foi o marco comercial da tecnologia no país.

A OAB em 1999 manifestou a primeira tentativa de regulamentação sobre os assuntos virtuais, onde criou uma comissão para apresentar um projeto de lei a ser proposto para o Congresso Nacional que versava sobre a regulamentação de comércio eletrônico, de forma mais específica sobre a validade do documento eletrônico e da assinatura digital.

---

[5] Metaverso é uma junção do prefixo "meta" e "universo" que descreve o conceito de uma interação futura da internet, composta por espaços virtuais.

[6] NFT (Non Fungible Token) é um tipo especial de token criptográfico que representa algo único; Criptomoedas ou Criptocurrency é um meio de troca financeiro artificial, criado pelo homem.

Mundialmente, a preocupação em regulamentar o ciberespaço foi concretizada a partir da chamada Convenção de Budapeste, publicada em novembro de 2001 e que só foi aderida pelo Brasil em dezembro 2021. O objetivo da Convenção é facilitar a cooperação internacional para combater o cibercrime, a prioridade do tratado conforme o seu Preâmbulo é formar uma política criminal comum para que seja possível proteger a sociedade contra a criminalidade no ciberespaço através de uma legislação adequada e de uma melhoria da cooperação internacional.

Pois bem, voltando ao ordenamento jurídico brasileiro, é a partir do ano de 2012 que o legislador inicia os debates sobre leis específicas do meio digital, assim tivemos a primeira publicação que é a Lei 12.735/2012. A referida lei tramitou no Congresso por mais de dez anos e ao ser publicada foi alvo de várias críticas no quesito sobre sua constitucionalidade.

Originalmente o projeto inicial dessa lei procurava dispor princípios, definições e criminalizar condutas de dano informáticos que alterariam o Código Penal, contudo, dentro do conteúdo aprovado tivemos somente um artigo que alterou o Código Penal, no que diz respeito aos crimes de preconceito de raça ou cor, e outro que alterou Código Penal Militar. Restou nítido que houve grande desvirtuamento do objetivo inicial do projeto, que trazia uma visão necessária ao ordenamento jurídico brasileiro e concentrou-se os esforços nas mudanças do Código Penal Militar quanto aos delitos em tempo de guerra.

A Lei 12.737/ 2012, conhecida como Lei Carolina Dieckmann, que diz respeito aos crimes contra a intimidade e os dados alheios, foi um produto da pressão sobre o legislador para que este criasse um tipo penal capaz de tutelar os dados informáticos. Assim sendo, a referida lei criou o delito de invasão de dispositivo informático simples, alterando o art. 154/CP e criando o art. 154-A com duas figuras. Alterou o art. 266/CP para "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, de informação de utilidade pública ou telemático". E acrescentou ao art. 298/CP a expressão "falsidade de cartão", equiparando o cartão de crédito ou débito a documento particular.

Em seguida, tivemos a promulgação da Lei 12.965/ 2014, conhecida como Marco Civil da Internet. Essa lei trouxe ao ordenamento pátrio as definições e expressões específicas que fazem parte do direito Informático, além disso, regrou circunstâncias de atuação do provedor e dos usuários, limitando ainda eventuais abusos que podem derivar do poder público, por fim, assegurou formalidades significativas para o Estado de Direito no contexto do Digital.

Já em 2020, temos a validade da lei 13.709/ 2018, a Lei Geral de Proteção de Dados que foi aprovada e promulgada no ano de 2018, mas só passou a valer em 2020. Esse dispositivo nasceu da inspiração do Regulamento Geral sobre a Proteção de Dados (RGPD), que é um pacote de medidas sobre proteção de dados regulado na União Europeia. Tal como a RGPD, o dispositivo brasileiro é uma medida para tutelar especificamente a proteção de dados dos usuários e estabelecer algumas definições necessárias como a definição de dados sensíveis, constantes no art. 5°, II da lei 13.709/218. A vista disso, a LGPD trouxe obrigatoriedade de tratamento de dados somente para fins legítimos específicos explícitos, sem possibilidade de tratamento posterior de forma incompatível com o estabelecido no dispositivo legal.

E por último, no ano de 2021, tivemos as maiores alterações na legislação brasileira digital que foram: 1- A aderência do brasil a Convenção de Budapeste, que demorou 20 anos para acontecer e agora o Estado brasileiro tem uma grande oportunidade para gerar discussões sobre a melhoria da legislação quanto a regulamentação do ciberespaço e da legislação das matérias afins ao assunto.

2- A promulgação da Lei 14.155/2021- que trata sobre os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, e trouxe alterações para: o artigo 154-A do CP, promovendo um progresso relativo para o Direito Penal Informático ao expandir as possibilidades da invasão informática, mas ainda apresenta certa insuficiência legislativa na sua compreensão do delito informático ao se preocupar somente com a conduta de "ingressar sem autorização dispositivo informático alheio"; o artigo 171 do CP que teve acrescentado ao tipo penal o parágrafo 2°-A inserindo a fraude eletrônica; o parágrafo 2°-B inserindo causas de aumento para quem utilizar servidores fora do país sem analisar os riscos da virtualidade e por último ainda nesse dispositivo modificou o parágrafo 4° criando uma causa de aumento nas situações em que a vítima for idosa ou pessoa vulnerável; o artigo 70 do CPP incluindo o parágrafo 4° e por último acrescentou ao artigo 155, também do CPP, o parágrafo 4°-B e 4°-C.

3- A promulgação da Lei 14.197/2021- que trata sobre os crimes contra o Estado Democrático de Direito e modificou o artigo 359 do CP inserindo no ordenamento jurídico os seguintes tipos penais: Atentado a soberania; Atentado à integridade nacional; Espionagem; Abolição violenta do Estado Democrático de Direito; Golpe de Estado; Interrupção do processo eleitoral; Violência política; e Sabotagem.

É imprescindível citar a Resolução 423/2021 do CNJ que incluiu a disciplina de Direito Digital nos concursos públicos para ingresso na magistratura. Essa resolução traz para o Direito Digital maior peso e importância aos juristas brasileiros, visto que apesar de "novo" entender e estudar o meio Digital é extremamente importante vislumbrando que caminhamos para um futuro cada vez mais tecnológico.

Assim sendo, mesmo que a passos lentos para aprovar leis brasileiras sobre as implicações cibernéticas na sociedade, cabe relembrar que apesar de termos alguns tipos legais, é necessário sempre melhorá-los e modernizar cada vez mais todo o aparato legislativo, jurídico, policial e de colaboração para com outros países a fim de alcançarmos soluções cada vez mais atuais e cirúrgicas.

2.3 PERÍCIA COMPUTACIONAL E A SUA IMPORTÂNCIA INVESTIGATIVA

Delitos informáticos demandam pessoal altamente especializado e equipamentos de última geração; afinal é possivelmente com um agente munido da última geração de dispositivos que se terá que lidar. (SYDOW.2022. P.420)

A fala de SYDOW, é imprescindível para iniciarmos o estudo da importância da perícia computacional nos casos de delitos informáticos. Para isso, insta ressaltar que é do entendimento da doutrina policial, que vigora na Academia Nacional de Polícia, que a internet é berço de crimes que deixam vestígios como registros de conexão e utilização da internet, como por exemplo, envio de e-mail, acessos a serviços de pesquisas (Google e Firefox, por exemplo), além do próprio acesso ao computador com o intuito de praticar ato criminoso.

A perícia computacional é entendida por um aglomerado de técnicas, cientificamente comprovadas, empregadas para colher, reunir, identificar, examinar, correlacionar e documentar, e documentar evidências digitais que estejam processadas, ou armazenadas ou transmitidas por computadores.

Essa competência tem como objetivo compreender os eventos ocorridos que levaram ao acontecimento do delito informático e deixar comprovado como ocorreu a ação do agente delitivo. Nesse sentido podemos citar dois tipos de forense computacional:

> São dois os principais tipos de forense computacional: online e o *post mortem* (ou *off line*). No primeiro, o sistema está ligado e é dinâmico, sendo que os dados mudam ou podem mudar durante a análise, sendo o principal objetivo a análise de conteúdos voláteis. Neste caso, importante que se diga, é indispensável a "fé pública" do profissional encarregado da atividade. Já no segundo, no método *offline*, o sistema

> está desligado e é estático, além de os dados originais poderem ser preservados, através do trabalho do perito sobre a imagem deles e não sobre o original. Neste caso, a análise é sobre as informações armazenadas e é totalmente auditável. (BEZERRA, 2020, p.187)

Nesse sentido, fica claro os tipos de perícia forense sendo ainda válido destacar que quanto as modalidades valem citar a forense de redes cabeadas e/ou sem fio, com possibilidade de reconstrução de sessões e geração de metadados. Também, cabe espaço para a forense remota, que trata das conexões online e silenciosas.

Pois bem, é através da forense computacional, que em vários casos é possível fazer o levantamento de informações importantes que servem como uma espécie de mapeamento da forma que ocorrem os delitos, como por exemplo a verificação de hardwares nos crimes de defesa do consumidor.

A nível do cibercrime transnacional, é necessário salientar que a perícia forense é imprescindível, visto que sem ela não seria possível realizar a coleta, armazenamento, lapidação e análise das diversas condutas criminosas realizadas de forma conexa e espalhada pelos servidores ao redor do mundo. Dessa forma, a Forense computacional ressalta sua imperiosidade na captura de criminosos e quadrilhas que agem tanto dentro do território pátrio quanto em território estrangeiro.

Quanto a evolução tecnológica, cabe compreender que o crescimento das tecnologias juntamente com o número dos dispositivos que acessam a rede, criam um cenário fértil para aprofundar as técnicas criminosas aumentando de forma conjunta às vulnerabilidades consequentes do uso massivo dos dispositivos informáticos.

A cada nova forma de praticar um delito, temos um novo desafio para órgãos de persecução penal que devem estar munidos de instrumentos de última tecnologia para enfrentar a investigação criminal. Nesse sentido a estrutura nacional carece de melhorias, sendo fundamental a necessidade de um treinamento das polícias para compreender linguagens, técnicas e métodos específicos utilizados pelos agentes delitivos, valendo-se ainda de peritos judiciais exclusivamente voltados a investigação virtual e informática.

3 CIBERCRIMINOLOGIA: PUNIBILIDADE OU PREVENÇÃO?

Até os dias atuais, o posicionamento do legislador brasileiro, versa no sentido de em todos os casos punir a conduta e a prática delitiva informática, o que de todo não está errado. Contudo, cabe trazer à discussão que dentro do ordenamento jurídico, o direito penal tem como princípio norteador a *Ultima ratio*, ou seja, teoricamente deveria ser a lei aplicada nos casos em que somente ela é capaz de evitar o ato ilícito ou de puni-lo à altura em que ofendeu ou lesou o bem jurídico.

Nesse sentido, o Direito Penal, só deveria ser aplicado quando estritamente necessário, porém, conforme o ânimo e a pressão social, não é o que se verifica no cenário jurídico brasileiro. Percebemos que caminha o Direito Penal informático ao mesmo cenário, sendo utilizado como primeira solução aos embates virtuais que nossa sociedade enfrenta.

Foucault, em Vigiar e punir, mostra que a evolução das práticas punitivas demonstram ser o resultado de uma série de processos sociais, políticos, históricos e econômicos sobrepostos. Assim sendo, cada época e cada sistema de punição tem suas características inerentes e sua premissa de existência.

A vista disso, a prisão cumpre um papel social que transcende o limite da punição ou correção do infrator. O comportamento do delinquente torna-se matéria prima do sistema industrial carcerário. Dessa forma uma legislação que está na maioria das vezes objetivada na punição de determinado ato, alimenta a forma mais comum de manifestação do poder nas instituições sociais modernas.

Não há o que se negar que é necessário uma cibecriminologia para compreender a nova modalidade de crime, o informático, a pessoa do infrator, da vítima e do controle social do comportamento delitivo.

Conforme diz SYDOW (2022), há um novo perfil de delinquente que surgiu na rede, que se mostrou, por sua alta velocidade e multiplicidade, quiçá o mais importante meio de cometimento de delitos, pela simultaneidade e pela sofisticação necessária para sua investigação.

> A linguagem mudou. As palavras mudaram. O crime mudou. A concepção de uma sociedade de riscos voltou potencializada, como bem apresentado por Pierpaolo Cruz Bottini ao apresentar seu “paradoxo do risco” em que tecnologias surgem para combater o delito, mas servem de ferramentas também para o cometimento de novos delitos. Por sua vez, novas tecnologias surgem para combater esses novos delitos e assim o ciclo se perpetua. (SYDOW.2022. P.734)

Pois bem, a criminologia é essencial para compreendermos de forma completa todo o cenário do ciberespaço e os delitos nele inseridos. Para isso, é necessário um estudo profundo das tecnologias e a cada novo avanço uma reanalise do processo acadêmico.

A imprescindibilidade de se estudar, explorar e debater o delito informático é para que, através disso, possamos permitir o Poder Público identificar espécies de usuários mais ou menos propensos a serem vítimas e agentes de delitos. (SYDOW, 2022).

O fato de o Brasil possuir uma legislação fraca, com pouca técnica e repressora, permite os altos índices de impunidade, o que diretamente impulsiona o aparecimento de novos delinquentes informáticos e ao surgimento de novos golpes.

Em relação ao usuário brasileiro, nós representamos um número massivo de consumidores nas principais redes sociais da atualidade como Instagram, TikTok e Twitter. Contudo o entendimento dos riscos e de como se configura cada rede social é pequeno, o usuário geralmente tem pouca ou nenhuma noção de educação digital.

> Outro fato fundamental é o de que apesar do brasileiro ser afim da tecnologia, apenas recentemente cresceu o acesso da população à tais aparatos, iniciando a quebra do *digital divide* (segregação acerca dos excluídos digitais). Outrossim, os usuários ainda engatinham na compreensão dos fundamentos e riscos da rede.
>
> Há uma vítima virtual diferente da vítima do mundo real. O usuário brasileiro via de regra não tem compreensão boa da língua inglesa, que predomina o ambiente eletrônico e isso facilita golpes em tal seara. (SYDOW.2022. P.740)

Dessa forma, urge a necessidade de dispor ao usuário elementos suficientes de conhecimento para informatizá-los e gerar a consciência do que versa nos contratos de serviços informáticos, o que se disponibiliza, quais os riscos da atividade, qual o grau de exposição da imagem, tudo potencializado aos efeitos a longo prazo.

É necessário criar uma sociedade que seja educada digitalmente para criar uma consciência informática e assim gerar uma prevenção primária. O usuário precisa entender que ele é responsável pelos dados que ele aceita inserir na rede, sendo conscientizado ainda pelas consequências e riscos que existe na rede.

Logicamente, é mais prático modificar o comportamento do usuário, que é potencialmente uma vítima do delito informático, que modificar o comportamento do agente delitivo.

Se conseguirmos trazer ao público, que tanto adora a interação virtual e as facilidades que a tecnologia proporciona a vida, a noção de que uma postura mais educada digitalmente

colabora na prevenção do crime informático, provavelmente construiríamos uma sociedade mais consciente e menos vulnerável no ciberespaço.

Portanto, tutelar sobre os delitos informáticos e tentar regular o ciberespaço isoladamente sem a conduta da educação digital, se mostra pouco eficaz contra o cibercrime. O ideal é alinhar o estudo da criminologia com o Poder Público e uma sociedade digitalmente educada para seja possível estabelecer um risco tolerável no ciberespaço.

CONCLUSÃO

A expansão da era digital, modificou os padrões sociais e impactou diretamente no modo como vivemos. A tecnologia permitiu a cada dia o surgimento de um novo fato prático provocando as autoridades e órgãos julgadores a tutelarem sobe um novo bem jurídico que surgiu a partir do uso da internet.

Surge a necessidade, no atual momento, da criação de uma legislação e de todo um aparato para regulamentar o meio ambiente digital, proteger e educar os usuários, a fim de que se construa uma estrutura onde se puna os delitos informáticos e se forme uma sociedade educada digitalmente gerando uma maior consciência a respeito do uso da internet.

O mundo virtual trouxe e continua trazendo, ao passo que se atualiza, novos conflitos e novas tipificações delitivas que possuem características não pensadas dentro da realidade que nos encontramos. Com essa nova realidade, tipos penais, territorialidade, bem jurídico, jurisdição e competência precisaram ser reinterpretados sob novos desdobramentos do Direito identificados dentro do direito informático.

Nesse sentido, este trabalho propôs um pensamento maduro e sistemático objetivando a solução do problema aqui discutido, pretendendo falar não somente da punição do criminoso digital, mas a trazer a noção de que uma postura mais educada digitalmente colabora na prevenção do crime informático.

Atualmente, na legislação brasileira já existem alguns tipos legais em relação as implicações cibernéticas na sociedade, contudo, entendemos ser necessário melhorar e modernizar o aparato legislativo, jurídico, policial e de colaboração para com outros países a fim de alcançarmos soluções cada vez mais atuais e cirúrgicas, pois até o momento possuímos uma legislação fraca, com pouca técnica e repressora. O que paralelamente permite os altos índices de impunidade que diretamente impulsiona o aparecimento de novos delinquentes informativos e o surgimento de novos golpes.

Portanto, foi a partir dessa realidade que se pensou o presente trabalho com a intenção de demostrar a importância do Direito digital e de problematizar o surgimento de possíveis novos comportamentos delitivos para que se preserve a harmonia da sociedade informatizada. Não há o que se negar que a virtualização das coisas provoca modificações sociais imediatas, assim sendo, requer-se da sociedade jurídica uma maior atenção ao tema de forma a promover um equilíbrio entre a sociedade e o ambiente digital.

CYBERCRIMES AND THE BRAZILIAN STATE'S PERFORMANCE ABOUT THEM

ABSTRACT

This work, theoretical in nature, aims to analyze the scenario of cybercrimes and the performance of the Brazilian State on cybercrimes, as well as to understand the issues to the digital world and the importance of digital education. The research begins by unraveling elements of the virtual environment and explaining concepts such as network, IP, microprocessor. After the concepts, the importance of the virtual world as an essential tool is discussed today and anonymity in the virtual environment is analyzed, explaining the "layers" of the internet, being surface web, deep web, and dark web. After analyzing the virtual world, the research brings up the debate of what are virtual crimes and computer crimes and how Brazilian legislation provides for them, complementing bringing a focus to the importance of expertise in cases of virtual crimes. Finally, it is debated within cybercriminology whether the best path to be chosen for solving crimes would be punishment or prevention, deepening research into the field of prevention with digital education.

Keywords: cybercrimes; digital; education; law; Internet.

REFERÊNCIAS

ARAS, Vladimir Barros; MENDONÇA, Andrey Borges de; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA, Marcos Antônio da Silva. **Proteção de Dados Pessoais e Investigação Criminal**. Brasília: Editora ANPR, 2020. Disponível em: http://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf. Acesso em: 05 de abril de 2021.

ARAUJO, Yuri Saramago Sahione de. **Adesão à Convenção de Budapeste sobre o crime cibernético é importante, mas também impõe desafios ao Brasil.** Disponível em: https://www.migalhas.com.br/depeso/357721/adesao-a-convencao-de-budapeste-sobre-o-crime-cibernetico-e-desafios. Acesso em: 05 de abril de 2022.

ARAUJO, Luís Guilherme N. de. **Resenha Vigiar e punir: poder, punição, disciplina e indústria.** São Paulo: Editora Primeiros Escritos. 2018.

BARRETO, Alessandro Gonçalves. **Cibercrimes e seus reflexos no Direito brasileiro**. 2 ed. rev. e. atual. São Paulo: Editora JusPodivm, 2021.

BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso. **Combate ao Crime Cibernético**. 1. ed. Rio de Janeiro: Mallet Editora, 2020.

BUDAPESTE. **Convenção sobre o Cibercrime,** 2001**.**Hungria: Conselho da Europa. Disponível em: https://rm.coe.int/16802fa428. Acesso: em 05 de abril de 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso: em 05 de abril de 2022.

BRASIL. **Lei N° 8.078, de 11 de setembro de 1990.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 06 de abril de 2022.

BRASIL. **Lei N° 12.735, de 30 de novembro de 2012.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 06 de abril de 2022.

BRASIL. **Lei N° 12.965, de 23 de abril de 2014.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 06 de abril de 2022.

BRASIL. **Lei N° 13.7019, de 14 de agosto de 2018.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 06 de abril de 2022.

BRASIL. **Lei N° 14. 155, de 27 de maio de 2021.** Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-

2022/2021/Lei/L14155.htm?msclkid=5041b729c69011eca04eb0ba2b483db0. Acesso em: 06 de abril de 2022.

BRASIL. **Lei N° 14.197 de 1 de setembro de 2022.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm. Acesso em: 06 de abril de 2022.

BRASIL. **Resolução Nº 423.** Brasília, DF: Presidência da República, 2021. Disponível em: https://atos.cnj.jus.br/atos/detalhar/4147. Acesso em 06 de abril de 2022.

Brasil aprova adesão à Convenção de Budapeste que facilita cooperação internacional para combate ao cibercrime. Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/brasil-aprova-adesao-a-convencao-de-budapeste-que-facilita-cooperacao-internacional-para-combate-ao-cibercrime. Acesso em: 04 de abril de 2022.

FERREIRA, Poliana Agostinho Calheiros; COELHO, Vânia Maria Bemfica Guimarães Pinto. **Crimes Virtuais.** Varginha: FADIVA,2014. E-book. Disponível em: http://www.fadiva.com.br/documentos/jusfadiva/2014/18.pdf. Acesso em: 06 de abril de 2022.

LEMOS, Ronaldo**. REVISTA OBSERVATÓRIO ITAÚ CULTURAL**.N-16. Jan/Jun 2014. São Paulo: Itaú Cultural.2007. ISSN 1981-125X versão online. Disponível em: https://itsrio.org/wp-content/uploads/2017/01/OBSERVATORIO16_0.pdf. Acesso em: 30 de out. de 2021. (perguntar se pode usar o nome do editor).

O que são bots? - definição e explicação. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-are-bots. Acesso em: 04 de abril de 2022.

RODRIGUES, Marco Antonio; TAMER, Maurício. **Justiça digital: O Acesso à Justiça e as Tecnologias da Informação na Resolução de Conflitos**. São Paulo: Editora JusPodiv, 2021.

SABINO, Marco Antônio da Costa. **Afinal, existe mesmo anonimato na internet?.** Disponível em: https://fia.com.br/blog/anonimato-na-internet/. Acesso em: 01 de dez. de 2021.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A Convenção de Budapeste e as leis Brasileiras.** João Pessoa: UFPB, 2009. E-book. Disponível em: https://www.charlieoscartango.com.br/Images/A%20convencao%20de%20Budapeste%20e%20as%20leis%20brasileiras.pdf. Acesso em: 06 de abril de 2022.

SYDOW, SPENCER TOTH. **Curso de Direito Penal Informático**. 2. ed. rev. e. atual. Salvador: Editora JusPodivm, 2021.

SYDOW, SPENCER TOTH. **Curso de Direito Penal Informático**. 3. ed. rev. e. atual. Salvador: Editora JusPodivm, 2022.

TANENBAUM, Andrew S.; WETHERALL, David J.; **Rede de Computadores**. 5. ed. Person Education, 2017. E-book.

TOBARES CATALA, Gabriel H. **Delitos informáticos**. Cordoba: Advocatus, 2010.

VIANA, Gabriela. **O que é um Host**?. Disponível em: https://www.techtudo.com.br/noticias/2012/02/o-que-e-um-host.ghtml. Acesso em: 17 de nov. de 2021.